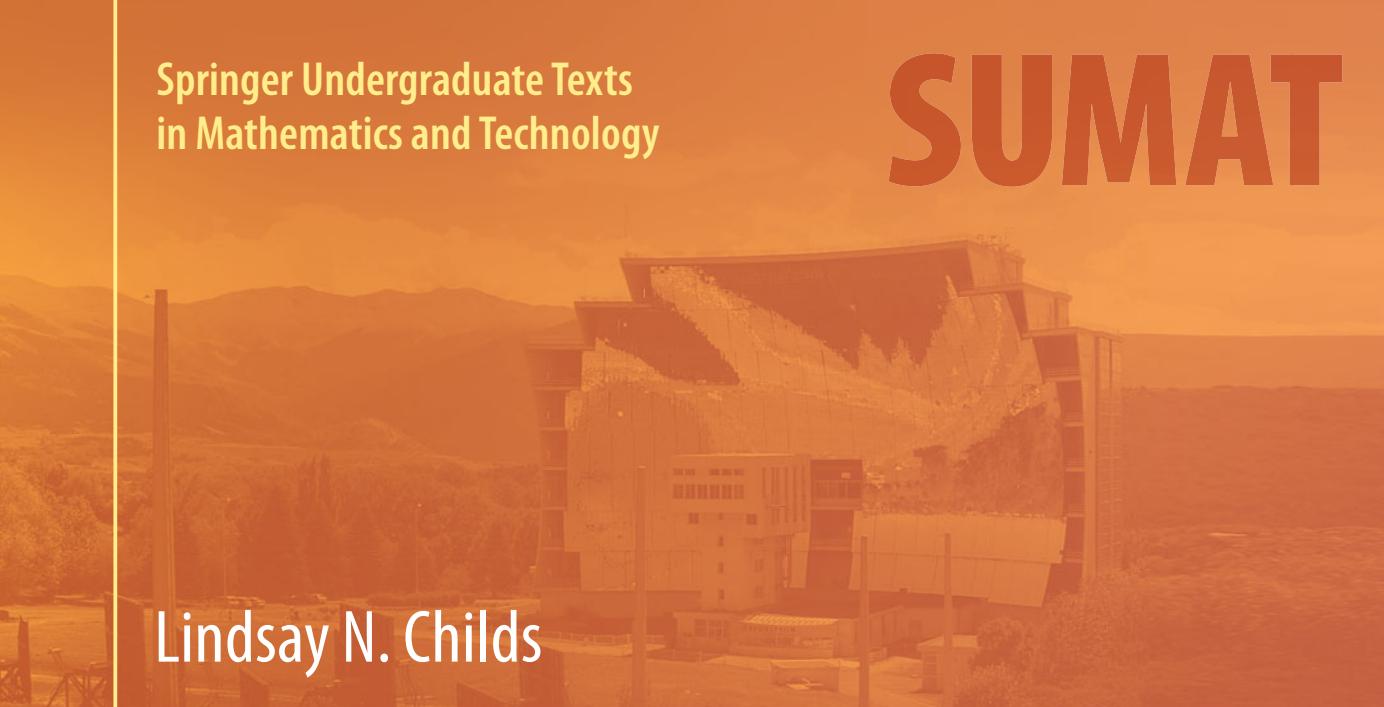


Springer Undergraduate Texts  
in Mathematics and Technology

SUMAT



Lindsay N. Childs

# Cryptology and Error Correction

An Algebraic Introduction and Real-World  
Applications

 Springer

# **Springer Undergraduate Texts in Mathematics and Technology**

## **Series Editors**

Helge Holden, Department of Mathematical Sciences, Norwegian University of Science and Technology, Trondheim, Norway

Keri A. Kornelson, Department of Mathematics, University of Oklahoma, Norman, OK, USA

## **Editorial Board Members**

Lisa Goldberg, Department of Statistics, University of California, Berkeley, Berkeley, CA, USA

Armin Iske, Department of Mathematics, University of Hamburg, Hamburg, Hamburg, Germany

Palle E.T. Jorgensen, Department of Mathematics, MLH 14, University of Iowa, Iowa, IA, USA

**Springer Undergraduate Texts in Mathematics and Technology** (SUMAT) publishes textbooks aimed primarily at the undergraduate. Each text is designed principally for students who are considering careers either in the mathematical sciences or in technology-based areas such as engineering, finance, information technology and computer science, bioscience and medicine, optimization or industry. Texts aim to be accessible introductions to a wide range of core mathematical disciplines and their practical, real-world applications; and are fashioned both for course use and for independent study.

More information about this series at <http://www.springer.com/series/7438>

Lindsay N. Childs

# Cryptology and Error Correction

An Algebraic Introduction and Real-World Applications



Springer

Lindsay N. Childs  
Department of Mathematics and Statistics  
University at Albany, State University of  
New York  
Albany, NY, USA

ISSN 1867-5506                   ISSN 1867-5514 (electronic)  
Springer Undergraduate Texts in Mathematics and Technology  
ISBN 978-3-030-15451-6       ISBN 978-3-030-15453-0 (eBook)  
<https://doi.org/10.1007/978-3-030-15453-0>

Library of Congress Control Number: 2019933907

Mathematics Subject Classification (2010): 12-01, 11T71, 68P25, 68P30, 94A60

© Springer Nature Switzerland AG 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

This book has two objectives.

One is to carefully present the RSA, Diffie–Hellman and Blum–Goldwasser cryptosystems and Hamming and Reed–Solomon error correction.

The other is to provide an introduction to concepts of abstract algebra and number theory.

The two objectives complement each other. On the one hand, to fully understand the cryptology and error correction requires the algebra and number theory. On the other hand, to appreciate the significance of the algebra and number theory, no application of the ideas is more immediately relevant than their application to methods of maintaining the integrity of information. So the book presents the requisite results from elementary number theory, and some basic concepts of abstract algebra—fields, commutative rings, ideals, abelian groups, subgroups and cosets, vector spaces and subspaces, homomorphisms and isomorphisms, products of rings—ideas and results needed to understand how and why those applications work. It does so in far more detail than most introductory books on cryptography or error correction.

The intended audience is a student who has had a year or two of college-level mathematics (typically calculus) and either has had or is taking concurrently a course in elementary matrix theory or linear algebra.

A student who completes this book will have gained a good mathematical understanding of some methods of cryptology and error correction that are widely used in the “real world” for the security and reliability of information. The student should also be well prepared for further study of both mathematics and cryptology and error correction, in two respects.

For students interested in applications, the mathematics presented in this book is part of the toolkit of researchers working on the next generations of mathematical methods to protect information. So even if (when) the methods presented in this book are supplanted by newer methods, the underlying mathematical ideas in this book should remain useful. Those ideas ultimately involve understanding the natural numbers and polynomials, and these timeless concepts, together with geometry, lie at the core of mathematics, pure and applied. For example, the second generation of public key cryptography involves elliptic curves, and while elliptic curves themselves are beyond the scope of this book, every mathematical idea in the book will help prepare a student to learn elliptic curve cryptography.

For mathematics students, an overall message of the book is that ideas of abstract algebra play an immediate and central role in understanding applications of great importance. That message should provide motivation for further study of abstract algebra and other advanced mathematics.

In detail, here is what is in the book.

**Concepts of Algebra.** This book introduces abelian groups, commutative rings and fields. The vector spaces  $F^n$  of column (or row) vectors arise for  $n = 3$  in Chapter 3 and for general  $n$  in Chapter 7, and are occasionally referred to in later chapters, but the theory of vector spaces is left for an elementary

linear algebra course. For a commutative ring  $R$ , in Chapter 5 we derive elementary properties of addition and multiplication from the axioms. We introduce ideals, classify the ideals of the ring of integers  $\mathbb{Z}$  and of the ring  $F[x]$  of polynomials with coefficients in a field  $F$  and construct the quotient ring  $R/J$ , made up of the cosets of an ideal  $J$  of a commutative ring  $R$ : this is how we formally construct, in Chapter 5, the ring of integers modulo  $m$ , in particular the prime fields  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ , and, in Chapter 18, all finite fields. We introduce ring homomorphisms and direct products of rings in Chapter 12 and give a proof of the Chinese remainder theorem from the fundamental homomorphism theorem for rings.

Some elementary properties of groups appear in Chapter 5. The order of an element of the group of units modulo  $m$ , and theorems about the order of an element, such as Fermat's and Euler's theorems, is the focus of Chapter 8. Chapter 8 contains mathematics that is fundamental for everything that follows. Subgroups show up in Chapter 10, constructed either by a set of generators or as the kernel of a group homomorphism. Cosets are introduced and illustrated for groups of small order by using group tables. Using cosets, we prove Lagrange's theorem and derive from it Fermat's and Euler's theorems. Non-abelian groups appear only in brief remarks at the end of Chapter 10, and normal subgroups and quotient groups other than  $\mathbb{Z}/m\mathbb{Z}$  are hardly mentioned because they are not needed for any of the applications. The three main examples of groups and subgroups appearing in the book are  $(\mathbb{Z}, +)$  and its subgroups, and groups of units of  $\mathbb{Z}/m\mathbb{Z}$ , both in Chapter 10, and vector spaces over  $\mathbb{F}_2$ , arising in Chapter 14 in connection with further exploration of a Hamming code. In Chapter 13 is a proof that the multiplicative group of a finite field is cyclic: the proof involves the concept of the exponent of an abelian group. Cyclic groups are examined in Chapters 10 and 13. The description of the groups  $U_m$  leads in Chapter 12 to a proof of the multiplicative property of Euler's phi function, essential for understanding RSA.

Subgroups of  $e$ -th roots of unity in  $U_m$  are introduced in Chapter 10, show up in connection with primality testing and are used to form the discrete Fourier transform in Chapter 19.

Cosets, and their use in the proof of Lagrange's theorem in Chapter 10, are useful in many subsequent places in the book: for constructing finite fields, to better understand Hamming codes, in proofs of the security of the Blum–Goldwasser cryptosystem and of RSA, in understanding sets of solutions of non-homogeneous linear equations and in primality testing. The idea of cosets is sometimes viewed as a difficult concept in an elementary abstract algebra course. Chapter 14 is wholly devoted to applications of cosets. Among other results, Section 14.1 views a linear transformation  $T$  of finite vector spaces over  $\mathbb{F}_p$  as a group homomorphism and derives from ideas involved in Lagrange's theorem the result that the rank of  $T$  plus the nullity of  $T$  is equal to the dimension of the domain of  $T$  (half of the so-called Fundamental Theorem of Linear Algebra [St06]).

Chapter 12 introduces the fundamental homomorphism theorem for ring homomorphisms, useful for both understanding the Chinese remainder theorem and Euler's phi function, and for constructing finite non-prime fields in Chapter 18. Chapter 12 also introduces direct products of rings, all of which leads to the decomposition of groups of units modulo  $m$  into the direct product of groups of units modulo the prime power factors of  $m$ . The ideas of Chapter 12 reappear in Section 16.7, where we introduce commutative diagrams to help describe two equivalent ways to decrypt in a Blum–Goldwasser cryptosystem.

The book includes the basic theory of the ring of integers in Chapters 3 and 4, and of polynomials in one variable over a field in Chapters 6 and 18. In elementary number theory, Chapter 2 introduces modular arithmetic and congruence, and Chapter 3 derives Bezout's identity and derives from it a complete description of how to solve a linear congruence, or equivalently, a linear diophantine equations in two variables. Chapter 3 also contains the highly useful consequence of Bezout's identity that we call the Coprime Divisibility Lemma in  $\mathbb{Z}$ : if a number  $a$  divides  $bc$  and  $a$  is coprime to  $b$ , then  $a$  divides  $c$ . It plays a key role in factoring methods. Chapter 6 includes a proof of D'Alembert's theorem on the number of roots in a field of a polynomial of degree  $n$ : it plays a key role in

understanding Reed–Solomon decoding. Two proofs of Fermat’s theorem and of Euler’s theorem appear, one derived from Lagrange’s theorem in Chapter 10, one each independent of Lagrange (in Chapters 8 and 14, respectively). Chapter 11 is devoted to the Chinese remainder theorem and its extension to general systems of linear congruences. The presentation of the CRT using Bezout’s identity was chosen because of its usefulness for decrypting, but that approach also becomes useful in Chapter 14 and Section 16.7.

**Applications.** Chapter 1 introduces several classical ideas in error detection and cryptography, both to introduce the two areas of application to be studied later in the book and to lay the groundwork for modular arithmetic. Cryptographic methods discussed are the Caesar cipher and Vigenère and Vernam (one-time pad) systems. Error detection is illustrated by Luhn’s formula for checking credit card numbers, and error correction by repetition coding. In Chapter 2, a multiplicative Caesar cipher is presented to help motivate the question in modular arithmetic: which numbers are units modulo  $m$ ? A multiplicative Caesar cipher is a one-dimensional Hill cipher. Hill ciphers are briefly discussed in the exercises of Chapter 7.

Modern applications begin in Chapter 7 with examples of Hamming codes, a class of single-error correcting codes. After Chapter 8, which contains Fermat’s and Euler’s theorems and a description of the XS binary algorithm for finding modular powers, the RSA cryptosystem is presented at the beginning of Chapter 9. RSA poses the problem of finding large primes, so much of Chapter 9 addresses questions such as: are there many large primes for use as factors of moduli in RSA? how do we find large primes?

Chapter 13 presents Diffie–Hellman key exchange and the closely related ElGamal cryptosystem, whose security depends on the difficulty of the discrete logarithm problem. Since Diffie–Hellman uses cyclic groups, this chapter includes a proof of the primitive root theorem: the multiplicative group of a finite field is cyclic. Chapter 13 concludes with a description of the Pohlig–Hellman algorithm, which uses the Chinese remainder theorem to reduce the discrete logarithm problem in a cyclic group of units modulo  $p$  whose order is composite, to finding discrete logarithms in subgroups of prime power order. Chapter 13 also includes a description and illustration of the baby-step giant-step algorithm for finding a discrete logarithm.

Chapter 14 contains results that shed further light on Hamming codes, on the security of RSA and on primality testing.

Chapter 15 introduces Reed–Solomon codes, used for multiple error correction and especially suited for “burst” errors. In this chapter, the codes are defined over a prime field. Decoding is done by the Welch–Berlekamp algorithm, which reduces the problem to solving a system of homogeneous linear equations. Assumed in Chapter 15, and also in Chapters 17 and 19, is some knowledge of the standard solution method, Gaussian elimination, typically learned early in a first course on linear algebra.

Chapter 16 introduces pseudorandom sequences of numbers and the Blum–Goldwasser cryptosystem, a clever public key analogue of a Vernam cryptosystem. In a Vernam system, the private key is a truly random sequence of numbers. A Blum–Goldwasser system uses a Blum–Blum–Shub pseudorandom sequence.

Since both the RSA and Blum–Goldwasser cryptosystems rely on their security on the difficulty of factoring large numbers, it seemed appropriate in Chapter 17 to introduce Fermat’s factorization and its generalization, the quadratic sieve method of factoring large numbers. The current factoring method of choice is the number field sieve, but the overall strategy of the two methods is similar and the NFS requires too many prerequisites in algebraic number theory to include in this book. The chapter concludes with a brief description of the index calculus method for finding discrete logarithms in the units group  $U_p$  of the field  $\mathbb{F}_p$  of  $p$  elements,  $p$  prime. The parallels between the baby-step giant-Step/index calculus algorithms and the Fermat/quadratic sieve algorithms are very strong.

After Chapter 18 on constructing finite fields, Chapter 19 returns to Reed–Solomon multiple error correcting codes. Using a complete set of  $n$ -th roots of unity as the numbers at which a plaintext message polynomial is evaluated, the decoding effort can be significantly reduced by use of the inverse of the discrete Fourier transform.

The book presents algorithms that in practice are implemented on a computer. Students who want to compute examples should be able to find sources online to help them do so, or may have access to MAPLE or other computer algebra systems. Or perhaps they can construct their own programs to do the computations. There are resources online for finding modular powers, for factoring and primality testing, for doing row operations on small matrices. The scientific calculator available with Windows 10 does modular arithmetic, including modular powers. Microsoft Excel can be used for small computations, such as finding greatest common divisors or solving Bezout’s identity, or finding modular powers, or constructing BBS sequences, or to assist on sieving numbers. Since Excel is so widely available on personal computers, the book includes in a few places descriptions of how to do computations using Excel.

Students who have not had elementary linear algebra may find Hamming codes (Chapter 7) and Reed–Solomon codes (Chapters 15 and 19) difficult. A course focusing on cryptography can omit those chapters and Section 14.2, and skip the linear algebra examples in Chapters 12 and 14. Some linear algebra is part of the quadratic sieve algorithm in Chapter 17, but a reader should be able to grasp the method without an understanding of linear algebra.

## Origin of This Book

The ultimate origin of this book was a set of class notes written in the 1970s for an introductory abstract algebra course at the University at Albany (State University of New York), entitled Classical Algebra. The course sought to motivate the basic concepts of groups, rings and fields by connecting them to elementary number theory and polynomials, subjects that we hoped second- and third-year undergraduate math majors could relate to. Those notes became a book, “A Concrete Introduction to Higher Algebra”. That book (1979) and its subsequent two editions (2nd edition, 1995; 3rd, 2009 [Ch09]) contain a broad array variety of applications and continues to be used for the Classical Algebra course at UAlbany.

In 2011, I began teaching Classical Algebra for UAlbany as a summer course, entirely online. For the course, I created a sequence of modules, adapted from the third edition of [CIHA], in which the focus of the applications was cryptology. Teaching the material wholly online, without lectures but with daily one-on-one interaction with the students, provided a great deal of feedback on how well the students understood the written modules, and forced me to think about how to present the material more clearly and make it easier to understand outside of a traditional classroom setting.

In April 2013, Ann Kostant of Springer urged me to consider writing a “Topics in Algebra for Information” book for the SUMAT series. With her invitation in mind, I taught the summer course five more times, rethinking the modules each year, and also used the modules in a classroom setting for a course, “Applied Abstract Algebra”, at Virginia Commonwealth University. With each revision, the course (and the modules) became more sharply focused. Instead of the algebraic topics being the main point, motivated by a diverse array of applications, the applications to cryptography and error correction became a dominant partner with the algebra, and everything that did not contribute to a better understanding of those applications was omitted. (But at the same time, the algebraic topics that survived were treated more thoughtfully—for example, the extended Euclidean algorithm in Chapter 3 is done with vectors; an explicit connection is shown between the XS binary algorithm and the strong  $a$ -pseudoprime test in Chapter 9; understanding the security of B-G cryptography in Chapter 16 is

facilitated by a study of the cosets of the kernel of a certain group homomorphism; the two ways to decrypt in B-G cryptography can be described visually by a commutative diagram of maps.) Other material was added, such as a sequence of exercises that explain why the cyclic group of units modulo  $p^e$  for small odd primes  $p$  and large  $e$  is not suitable for DH cryptography, a new exposition of Reed–Solomon codes, and a presentation of the Fermat and quadratic sieve factoring algorithms and the baby-step giant-step and index calculus discrete logarithm algorithms in Chapter 17 that hopefully brings out the parallels between the two pairs of methods.

The present book is the output of this multi-year revision process.

Given its evolution, the book should be suitable for use in a traditional classroom setting, for Web-based courses and for self-study.

## Acknowledgements

Writing this book has been a 40-year experience. I am grateful to Professors Ed Davis, Malcolm Smiley and David Drasin for their input and advice on the first edition of CIHA, and to so many people—students and colleagues at the University at Albany, and numerous users of CIHA elsewhere—for their comments over the years. Most of them are cited in one or more of the three editions of that book. For this book, I wish to thank the University at Albany and its Mathematics Department for enabling me to continue to teach the summer online course for them remotely. I especially thank the students in the online course who have provided invaluable feedback on the course content. My thanks also to the Mathematics Department at VCU for the opportunity to teach their Applied Abstract Algebra course. My thanks to Ann Kostant for suggesting the project and for her valuable guidance on the orientation of the book, and to Elizabeth Loew of Springer for her support and encouragement. And most importantly, heartfelt thanks to my wife, Rhonda, for her support and understanding, for this project and everything else.

Albany, USA  
November 2018

Lindsay N. Childs

# Contents

<b>1</b>	<b>Secure, Reliable Information</b>	1
1.1	Introduction	1
1.2	Least Non-negative Residues and Clock Arithmetic	2
1.3	Cryptography	3
1.4	Error Detection and Correction	7
	Exercises	9
<b>2</b>	<b>Modular Arithmetic</b>	13
2.1	Arithmetic Modulo $m$	13
2.2	Modular Arithmetic and Encryption	17
2.3	Congruence Modulo $m$	19
2.4	Letters to Numbers	22
	Exercises	24
<b>3</b>	<b>Linear Equations Modulo <math>m</math></b>	27
3.1	The Greatest Common Divisor	28
3.2	Finding the Greatest Common Divisor	30
3.3	Bezout's Identity	33
3.4	Finding Bezout's Identity	35
3.5	The Coprime Divisibility Lemma	41
3.6	Solutions of Linear Diophantine Equations	42
3.7	Manipulating and Solving Linear Congruences	45
	Exercises	47
<b>4</b>	<b>Unique Factorization in <math>\mathbb{Z}</math></b>	51
4.1	Unique Factorization into Products of Prime Numbers	51
4.2	Induction	56
4.3	The Fundamental Theorem of Arithmetic	58
4.4	The Division Theorem	60
4.5	Well-Ordering	61
	Exercises	62
<b>5</b>	<b>Rings and Fields</b>	65
5.1	Groups, Commutative Rings, Fields, Units	66
5.2	Basic Properties of Groups and Rings	67
5.3	Units and Fields	69
5.4	Ideals	70

5.5	Cosets and Integers Modulo $m$ . . . . .	73
5.6	$\mathbb{Z}_m$ is a Commutative Ring . . . . .	76
5.7	Complete Sets of Representatives for $\mathbb{Z}/m\mathbb{Z}$ . . . . .	78
5.8	When is $\mathbb{Z}/m\mathbb{Z}$ a Field? . . . . .	79
	Exercises . . . . .	80
<b>6</b>	<b>Polynomials</b> . . . . .	83
6.1	Basic Concepts . . . . .	83
6.2	Division Theorem . . . . .	86
6.3	D'Alembert's Theorem . . . . .	88
	Exercises . . . . .	90
<b>7</b>	<b>Matrices and Hamming Codes</b> . . . . .	93
7.1	Matrices and Vectors . . . . .	93
7.2	Error Correcting and Detecting Codes . . . . .	101
7.3	The Hamming (7, 4) Code: A Single Error Correcting Code . . . . .	102
7.4	The Hamming (8, 4) Code . . . . .	108
7.5	Why Do These Codes Work? . . . . .	110
	Exercises . . . . .	112
<b>8</b>	<b>Orders and Euler's Theorem</b> . . . . .	117
8.1	Orders of Elements . . . . .	117
8.2	Fermat's Theorem . . . . .	121
8.3	Euler's Theorem . . . . .	123
8.4	The Binomial Theorem and Fermat's Theorem . . . . .	125
8.5	Finding High Powers Modulo $m$ . . . . .	127
	Exercises . . . . .	131
<b>9</b>	<b>RSA Cryptography and Prime Numbers</b> . . . . .	135
9.1	RSA Cryptography . . . . .	135
9.2	Why Is RSA Effective? . . . . .	138
9.3	Signatures . . . . .	140
9.4	Symmetric Versus Asymmetric Cryptosystems . . . . .	141
9.5	There are Many Large Primes . . . . .	141
9.6	Finding Large Primes . . . . .	143
9.7	The $a$ -Pseudoprime Test . . . . .	144
9.8	The Strong $a$ -Pseudoprime Test . . . . .	146
	Exercises . . . . .	150
<b>10</b>	<b>Groups, Cosets and Lagrange's Theorem</b> . . . . .	153
10.1	Groups . . . . .	153
10.2	Subgroups . . . . .	154
10.3	Subgroups of Finite Cyclic Subgroups . . . . .	160
10.4	Cosets . . . . .	160
10.5	Lagrange's Theorem . . . . .	165
10.6	Non-abelian Groups . . . . .	167
	Exercises . . . . .	168
<b>11</b>	<b>Solving Systems of Congruences</b> . . . . .	171
11.1	Two Congruences: The "Linear Combination" Method . . . . .	172
11.2	More Than Two Congruences . . . . .	176
11.3	Some Applications to RSA Cryptography . . . . .	177

11.4	Solving General Systems of Congruences . . . . .	181
11.5	Solving Two Congruences . . . . .	182
11.6	Three or More Congruences . . . . .	186
11.7	Systems of Non-monic Linear Congruences . . . . .	187
	Exercises . . . . .	188
<b>12</b>	<b>Homomorphisms and Euler's Phi Function</b> . . . . .	195
12.1	The Formulas for Euler's Phi Function . . . . .	195
12.2	On Functions . . . . .	196
12.3	Ring Homomorphisms . . . . .	197
12.4	Fundamental Homomorphism Theorem . . . . .	200
12.5	Group Homomorphisms . . . . .	201
12.6	The Product of Rings and the Chinese Remainder Theorem . . . . .	204
12.7	Units and Euler's Formula . . . . .	208
	Exercises . . . . .	211
<b>13</b>	<b>Cyclic Groups and Cryptography</b> . . . . .	215
13.1	Cyclic Groups . . . . .	215
13.2	The Discrete Logarithm . . . . .	217
13.3	Diffie–Hellman Key Exchange . . . . .	220
13.4	ElGamal Cryptography . . . . .	221
13.5	Diffie–Hellman in Practice . . . . .	222
13.6	The Exponent of an Abelian Group . . . . .	224
13.7	The Primitive Root Theorem . . . . .	228
13.8	The Exponent of $U_m$ . . . . .	230
13.9	The Pohlig–Hellman Algorithm . . . . .	231
13.10	Shanks' Baby Step–Giant Step Algorithm . . . . .	233
	Exercises . . . . .	236
<b>14</b>	<b>Applications of Cosets</b> . . . . .	241
14.1	Group Homomorphisms, Cosets and Non-homogeneous Equations . . . . .	241
14.2	On Hamming Codes . . . . .	246
14.3	Euler's Theorem . . . . .	248
14.4	A Probabilistic Compositeness Test . . . . .	250
14.5	There Are No Strong Carmichael Numbers . . . . .	251
14.6	Boneh's Theorem . . . . .	253
	Exercises . . . . .	255
<b>15</b>	<b>An Introduction to Reed–Solomon Codes</b> . . . . .	259
15.1	The Setting . . . . .	259
15.2	Encoding a Reed–Solomon Code . . . . .	260
15.3	Decoding . . . . .	263
15.4	An Example . . . . .	266
	Exercises . . . . .	271
<b>16</b>	<b>Blum–Goldwasser Cryptography</b> . . . . .	273
16.1	Vernam Cryptosystems . . . . .	273
16.2	Blum, Blum and Shub's Pseudorandom Number Generator . . . . .	275
16.3	Blum–Goldwasser Cryptography . . . . .	276
16.4	The Period of a BBS Sequence . . . . .	278

16.5	Recreating a BBS Sequence from the Last Term . . . . .	282
16.6	Security of the B-G Cryptosystem . . . . .	283
16.7	Implementation of the Blum-Goldwasser Cryptosystem . . . . .	286
	Exercises . . . . .	291
<b>17</b>	<b>Factoring by the Quadratic Sieve . . . . .</b>	<b>293</b>
17.1	Trial Division . . . . .	293
17.2	The Basic Idea Behind the Quadratic Sieve Method . . . . .	294
17.3	Fermat's Method of Factoring . . . . .	296
17.4	The Quadratic Sieve Method . . . . .	297
17.5	The Index Calculus Method for Discrete Logarithms . . . . .	306
	Exercises . . . . .	309
	Appendix: Fermat's Method Versus Trial Division . . . . .	310
<b>18</b>	<b>Polynomials and Finite Fields . . . . .</b>	<b>313</b>
18.1	Greatest Common Divisors . . . . .	313
18.2	Factorization into Irreducible Polynomials . . . . .	317
18.3	Ideals of $F[x]$ . . . . .	320
18.4	Cosets and Quotient Rings . . . . .	321
18.5	Constructing Many Finite Fields . . . . .	326
	Exercises . . . . .	328
<b>19</b>	<b>Reed-Solomon Codes II . . . . .</b>	<b>331</b>
19.1	Roots of Unity and the Discrete Fourier Transform . . . . .	331
19.2	A Field with 8 Elements . . . . .	333
19.3	A Reed-Solomon Code Using $\mathbb{F}_8$ . . . . .	334
19.4	An Example Using $\mathbb{F}_{13}$ . . . . .	337
	Exercises . . . . .	342
	<b>References . . . . .</b>	<b>343</b>
	<b>Index . . . . .</b>	<b>347</b>

# Chapter 1

## Secure, Reliable Information



### 1.1 Introduction

Most of us create and send information across the internet to friends and relatives, financial institutions, retail websites, cloud backup, etc. (One estimate is that in 2015 some 205 billion emails were sent each day worldwide.) All of this information ends up as numerical, usually binary, data of some form, e.g., sequences of 0's and 1's. Once sent, the information is out of our control, and can be compromised in two ways: by the introduction of errors caused by humans, static, computer glitches, sunspots, defective memory storage, etc., and by misuse of the information by eavesdroppers, identity thieves, stalkers, hackers, government agencies, etc. among the two billion internet users worldwide who may be on the internet at the same time we send out our information.

So there are two issues to consider when trying to protect our information.

One is security. How can we help safeguard our messages from being read by eavesdroppers? How can others be certain that messages we send are in fact from us?

The other is reliability. How can we help safeguard the content of our messages from errors that may arise?

Study of the first issue has led to cryptology. The basic strategy is to transform messages to try to make them unreadable by anyone other than the desired recipient, or to add a “signature” so that a recipient can be sure that a message really came from us.

Study of the second issue has led to coding theory. The basic strategy is to take a message and encode it by adding redundancy, in such a way that with high probability, a receiver will at least know if the encoded message contains errors, and perhaps also be able to correct errors to determine the original message.

Both subjects have long histories, dating back to (at least) the ancient Romans. Both areas have grown vigorously since the 1940s, spurred by the maturation of computers, to become important areas of modern applied mathematics and computer science.

Our aim in this book is to present some modern methods of cryptology and coding in wide use throughout the world and to carefully present the basic number theory and concepts of abstract algebra needed to understand these methods.

In this chapter we will look at some simple examples of efforts to create security in the transmission of information, and to deal with errors.

But we begin with some ideas that will make describing those examples easier.

## 1.2 Least Non-negative Residues and Clock Arithmetic

Let  $\mathbb{N}$  be the set of natural (or counting) numbers: 1, 2, 3, .... Let  $\mathbb{Z}$  be the set of integers. Then  $\mathbb{Z}$  contains the natural numbers, 0 (zero), and the negatives of the natural numbers.

The reader is assumed to know long division, used to divide a number by a non-zero number. For numbers  $m$  and  $a$ , the objective of dividing  $a$  by  $m$  is to get a *quotient*  $q$  and a *remainder*  $r \geq 0$  so that

$$a = mq + r$$

where  $r < m$ . Terminology:  $m$  is the *divisor*,  $a$  the *dividend*.

The outcome of long division can be extended to the case where the dividend  $a$  is any integer, positive, negative or zero. The generalization is:

**Theorem 1.1** (Division Theorem) *Let  $m$  be a positive integer and let  $a$  be any integer. Then there is a unique integer  $q$  and a unique number  $r$  with  $0 \leq r < m$  so that  $a = mq + r$ .*

For example, if  $m = 9$  and  $a = -25$ , then

$$-25 = 9 \cdot (-3) + 2.$$

If  $m = 360$  and  $a = -1020$ , then

$$-1020 = 360 \cdot (-3) + 60.$$

The Division Theorem will be proven in Chapter 4.

For the case where the dividend can be any integer, positive or negative (or 0), we introduce some new terminology.

**Definition** Let  $m$  be a natural number and let  $a$  be any integer  $\geq 0$ . The *least non-negative residue* of  $a$  modulo  $m$ , denoted by  $(a \bmod m)$ , is the unique number  $r$  with  $0 \leq r < m$  so that

$$a = mq + r.$$

The least non-negative residue of  $-25$  modulo  $9$ , denoted  $(-25 \bmod 9)$ , is  $2$ . The least non-negative residue of  $-1020$  modulo  $360$ , denoted  $(-1020 \bmod 360)$ , is  $60$ . For  $a \geq 0$ ,  $(a \bmod m)$  is just the remainder when  $a$  is divided by  $m$ .

*Example 1.2* The least non-negative residue of  $20$  modulo  $8$  is  $4$ , because  $8$  divides into  $20$  two times with remainder  $4$ . So  $(20 \bmod 8) = 4$ .

$(365 \bmod 7) = 1$ , because when we divide  $7$  into  $365$ , we find that  $365 = 7 \cdot 52 + 1$ . (Interpretation: a non-leap year of  $365$  days consists of  $52$  weeks plus one day.)

The improper fraction approximation to  $\pi$  is

$$\frac{22}{7} = 3 + \frac{1}{7}.$$

So

$$22 = 7 \cdot 3 + 1;$$

the numerator  $1$  of the proper part  $\frac{1}{7}$  of  $\frac{22}{7}$  is the least non-negative residue  $(22 \bmod 7)$ .

The least non-negative residue  $(72 \bmod 8)$  is  $0$ , because  $72/8 = 9$ , an integer.

The idea of the least non-negative residue lies behind what is sometimes called “clock arithmetic”. For an introduction, consider the following questions:

I. I fly from La Paz, Bolivia to New York City. The trip begins at 8 am on Tuesday in La Paz and (with two changes of planes) ends in New York 38 hour later. What does my watch show at the time I land in NYC? (La Paz and New York are in the same time zone).

II. If April 1 is a Tuesday, what day of the week is April 25?

III. What is the sine of  $-1020$  degrees?

Question I involves the idea that hours on a watch repeat every 12 hours. If my watch shows 8 o’clock when I left, then when I arrive 38 hour later the watch will show  $((8 + 38) \bmod 12) = (46 \bmod 12) = 10$  o’clock.

Question II involves the fact that names of days repeat every seven days. Since April 25 is 24 days after a Tuesday, the day is  $(24 \bmod 7) = 3$  days after a Tuesday, hence a Friday.

Question III involves knowing that  $\sin(x) = \sin(x + 360k)$  for every integer  $k$ . So

$$\begin{aligned}\sin(-1020) &= \sin(-1020 \bmod 360) = \sin(-1020 + 1080) \\ &= \sin(60) = \sqrt{3}/2.\end{aligned}$$

We’ll discuss these ideas much more in Chapters 2 and 5. But having the idea of the least non-negative residue  $(a \bmod m)$  is helpful for describing examples in the remainder of this chapter.

## 1.3 Cryptography

Encrypting messages has a history that goes back at least 2500 years. We look at very old examples and one newer example.

First, some terminology. A *cipher* is a method of transforming a *plaintext* message into an *encrypted* message, called the *ciphertext*, which must be *decrypted* back to the plaintext in order to be read.

**Caesar ciphers.** The oldest method we will consider to alter a text message to make it unreadable to an uninitiated reader is the Caesar cipher, used by Julius Caesar around 40 B.C. to communicate with his friends ([Kah67], p. 84). In the Caesar cipher a message is encrypted by replacing each letter by the letter three places to the right in the alphabet. Thus

STAY THERE

would be encrypted as

*VWDB WKHUH,*

where if moving three places to the right puts you past Z, just start over with A: (...WXYZABC...). Thus three places to the right from Y is B.

To view a Caesar cipher numerically, replace each letter of the alphabet by its position number. So A becomes 1, B becomes 2, etc.:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Then

SAXONY

becomes

19, 1, 24, 15, 14, 25.

The Caesar cipher encrypts letters by adding 3, the key, to each position number, modulo 26. Thus

- 19 is encrypted as  $((19 + 3) \bmod 26) = 22$ , or *U*
- 1 is encrypted as  $((1 + 3) \bmod 26) = 4$ , or *D*
- 24 is encrypted as  $((24 + 3) \bmod 26) = 1$ , or *A*
- 15 is encrypted as  $((15 + 3) \bmod 26) = 18$ , or *R*
- 14 is encrypted as  $((14 + 3) \bmod 26) = 17$ , or *Q*
- 25 is encrypted as  $((25 + 3) \bmod 26) = 2$ , or *B*.

So SAXONY is encrypted as UDARQB.

To decrypt, we subtract the key 3 from the position number of each encrypted letter. In particular,

- 1 is decrypted as  $((1 - 3) \bmod 26) = 24$ , or *X*
- 2 is decrypted as  $((2 - 3) \bmod 26)$ , or *Y*.

It is then easy to see how to generalize the Caesar cipher by replacing the key  $\kappa = 3$  by any key  $\kappa$  with  $2 \leq \kappa \leq 25$ . For example, to encrypt SAXONY with  $\kappa = 17$ , we would transform the position numbers (19, 1, 24, 15, 14, 25) by adding 17 modulo 26 to each number, to get

$$\begin{aligned} & ((19 + 17) \bmod 26), ((1 + 17) \bmod 26), ((24 + 17) \bmod 26), \\ & ((15 + 17) \bmod 26), ((14 + 17) \bmod 26), ((25 + 17) \bmod 26) \\ & = ((36 \bmod 26), (18 \bmod 26), (41 \bmod 26), \\ & (32 \bmod 26), (31 \bmod 26), (42 \bmod 26) \\ & = (10, 18, 15, 6, 5, 16) = JROFEP. \end{aligned}$$

In a society with a high literacy rate, Caesar ciphers are very easy to crack, so they have not been used for many centuries. But our next examples have a higher level of security.

At this point we introduce Alice and Bob. We could envision one as a newspaper editor, the other a reporter assigned overseas in a hostile environment. They send messages to each other (usually Alice is the sender, Bob the receiver), and want their messages to be private and accurate. For the remainder of our discussions in this book, when discussing a new method of treating messages, we'll typically describe what Alice and Bob need to do to implement the method.

**Vigenère ciphers.** These cryptosystems were popularized by Blaise de Vigenère in 1585 [Kah67, p. 145ff]. Let's assign the numbers 0 through 28 to letters and ?, ! and “space” according to the table:

A	B	C	...	Z	?	!	(sp)
1	2	3	...	26	27	28	0.

Then a message becomes a sequence of numbers. For example,

I LOVE YOU SO MUCH!

becomes the numerical plaintext message

9, 0, 12, 15, 22, 5, 0, 25, 15, 21, 0, 19, 15, 0, 13, 21, 3, 8, 28.

The modulus here is 29, not 26.

A Vigenère cipher works like a Caesar cipher, except that the key is no longer a single number, but rather a sequence of numbers, often derived from a piece of text that Alice (the sender) and Bob (the recipient) share.

Suppose, for example, that Alice and Bob agree that their shared key is the word ENCRYPT. Then when Alice sends Bob the message “I LOVE YOU SO MUCH!”, she would turn both the key and the plaintext message into position numbers, as above (ENCRYPT becomes 5, 14, 3, 18, 25, 16, 20), and then encrypt by adding as follows:

$$\begin{array}{r}
 & 9 & 0 & 12 & 15 & 22 & 5 & 0 & | 25 & 15 & 21 & 0 & 19 & 15 & 0 & | 13 & 21 & 3 & 8 & 28 \\
 + & 5 & 14 & 3 & 18 & 25 & 16 & 20 & | 5 & 14 & 3 & 18 & 25 & 16 & 20 & | 5 & 14 & 3 & 18 & 25 \\
 \hline
 = & 14 & 14 & 15 & 4 & 18 & 21 & 20 & | 1 & 0 & 24 & 18 & 15 & 2 & 20 & | 18 & 6 & 6 & 26 & 24
 \end{array}$$

where encryption of each number is done by adding to it the corresponding key number modulo 29. Thus if a sum, such as  $15 + 18 = 33$ , or  $22 + 25 = 47$ , is  $\geq 29$ , then we subtract 29 to get a number  $< 29$ . So we find  $((15 + 18) \bmod 29) = (33 \bmod 29) = 4$  and  $((22 + 25) \bmod 29) = (47 \bmod 29) = 18$ , etc. After translating the bottom line of numbers back into their corresponding letters, the resulting ciphertext (in letters) is

NNODRUTA(sp)XROBTRFFZD.

Bob would decrypt by subtracting the numbers 5, 14, 3, 18, 25, 16, 20, 5, 14, 3, 18, 25, ... of the repeated key ENCRYPT from the encrypted sequence of numbers, then finding the least non-negative residue modulo 29 of the result. What comes out is the sequence of numbers corresponding to the original plaintext.

If the message is longer than the length of the key, then the key is repeated, as done above, until we reach the end of the plaintext.

The Vigenère cryptosystem was used in the 17th century and was believed to be secure. But it is not so secure when the message is much longer than the key, because of the cyclical pattern of the key. In our example, the key was repeated every seven letters. Also, as used in historical practice, the key was often an easily remembered short piece of Latin text, such as AMOR VINCIT OMNIA (“Love conquers all”) or IN PRINCIPIO ERAT VERBUM (“In the beginning was the Word”, recited at the conclusion of the Roman Catholic mass in the 16th century), so cryptanalysts could try to guess the key text. If the key is short compared to the message, then an analysis can often determine the length of the key, and then the message itself, based on the fact that different letters in English (or French or Latin in the 16th century) have greatly different frequencies of use (in English, compare E and Q, for example). There are websites that demonstrate the insecurity by decrypting ciphertexts encrypted by a Vigenère cryptosystem with a short key.

Nonetheless, the idea of using a key that encrypts successive letters differently is the basis of a secure cryptosystem, which we look at next.

**Vernam ciphers.** Alice and Bob want to be able to send messages to each other privately while one of them is on a trip abroad. To do so, they meet before the trip and construct a long list of random (base 10) digits (for example, obtained from measurements of cosmic rays, or by choosing random digits of the volume of stock shares traded on the New York Stock Exchange each day over many years). Then they depart from each other, each with an identical copy of the list of random digits.

When Alice wants to send a message to Bob, such as “HUG YOU”, she turns the message into a sequence of two-digit (base 10) numbers:

08, 21, 07, 00, 25, 15, 21

where 08 is H, 00 is space, 21 is U, etc. She starts at a point agreed to with Bob on their shared list of random digits. Suppose the next 14 random digits on the list are

29378568401172.

She adds her digits to the list of random digits one at a time, modulo 10 (that is, subtracting 10 if the sum of the digits is  $> 9$ ): Thus she computes

$$\begin{array}{r} |0 & 8 & 2 & 1 & 0 & 7 & 0 & 0 & 2 & 5 & 1 & 5 & 2 & 1 \\ + |2 & 9 & 3 & 7 & 8 & 5 & 6 & 8 & 4 & 0 & 1 & 1 & 7 & 2 \\ = |2 & 7 & 5 & 8 & 8 & 2 & 6 & 8 & 6 & 5 & 2 & 6 & 9 & 3 \end{array}$$

and sends the message 27588268652693 to Bob. Bob receives this message, and subtracts from each digit in order, the same digits 29378568401172 that Alice used, and then obtains the digits modulo 10 that will give the original number and hence the message. (He smiles.)

Let us introduce Eve. Eve is a malevolent eavesdropper: let’s assume she was Bob’s girl friend until Alice came on the scene (“Heav’n has no Rage, like Love to Hatred turn’d, Nor Hell a Fury, like a Woman scorn’d”—William Congreve, *The Mourning Bride*, 1697). Eve would like to know what is going on between Alice and Bob.

But if Eve intercepts Alice’s message somewhere between Alice and Bob, Eve has no chance of reading it. The cipher is unbreakable. If you add a truly random sequence to any sequence, the resulting cipher sequence is random: the cipher sequence has an equal probability of being any given 14-digit number. Frequency analysis of English letters will be futile.

The only way for Eve to learn the message is to steal the list of random digits, or gain access to either Alice’s or Bob’s computer to read the message before it is encrypted or after it is decrypted.

The Vernam cipher was discovered in 1917, and was quickly recognized as an unbreakable code [Kah67, pp. 394ff].

But implementation has always been difficult.

The problem is that Alice and Bob must have identical copies of a random digit sequence as long as the message. If Eve is able to gain access to that sequence of random digits, then she can read the messages. So for high volumes of messages to be encrypted, the length of the needed keys becomes impossible to deal with. Even nowadays, where huge shared random keys could be stored on a computer, the extent to which computers seem to be “hacked” means that almost any data stored on a computer attached to the internet is at risk.

The Caesar cipher, the Vigenère cipher, and the Vernam cipher are symmetric, private key cryptosystems.

A *key* is a piece of information that enables Alice to encrypt a message and Bob to decrypt a message. For the Caesar cipher, the key  $\kappa$  is the shift number. For the Vigenère cipher, the key is a shared piece of text. For the Vernam cipher, the key is the shared sequence of random digits.

The three ciphers are *symmetric*, because both Alice and Bob use the same key, Alice to encrypt, Bob to decrypt a message.

The ciphers are *private key ciphers*, because the security of the cryptosystem depends on the secrecy of the key. If Eve obtains the key, she can read messages encrypted with the key as easily as Bob can.

The ciphers we study later in the book are of a different character. They are asymmetric and public key, and date from 1976 or later. As we'll see, their security does not depend on the privacy of a shared key, but rather depends on the fact that a particular mathematics problem, such as factoring a large number into a product of prime numbers, is very hard.

One aim of this book is to understand several public key cryptosystems. To do so requires knowing some algebra and number theory. So the next few chapters are devoted to introducing the ideas needed.

## 1.4 Error Detection and Correction

To illustrate the basic idea of error detection and correction, we start with a method of error detection used in online shopping.

**Check digits.** Not so long ago I tried to buy something online with a credit card. I keyed in the credit card number, and instantly got an error message, “invalid credit card number, please retype the number”. Apparently I had mistyped the card number, and the retail website recognized the error.

The website was likely using a formula for checking the validity of credit card numbers that was patented in 1960 by H. P. Luhn of IBM. (It is now in the public domain; see Wikipedia, “Luhn Algorithm”.)

We introduce Alice and Bob again. In this setting, Alice is a shopper, and wants to buy something online with a credit card. Bob, the merchant, wants to be confident that the credit card number is valid. Suppose Alice keys in the following number and sends it to Bob:

$$M = 4567\ 8901\ 2345\ 6789.$$

This looks like a credit card number. But not every sixteen digit number beginning with 45 can be a valid credit card number, because the last digit is a “check digit”, determined by the previous 15 digits, as follows:

Define a function  $p(x)$  on the digits 0, 1, 2, ..., 8, 9 by

$$\begin{aligned} p(0) &= 0 \\ p(9) &= 9 \\ p(n) &= (2n \bmod 9) \text{ for } 1 \leq n \leq 8. \end{aligned}$$

In tabular form, here are the values of  $p(x)$ :

$n$	0	1	2	3	4	5	6	7	8	9
$p(n)$	0	2	4	6	8	1	3	5	7	9

Given a credit card number of  $n$  digits, number the digits starting from the right (here  $n = 16$ ):

$$a_{16}a_{15}a_{14}a_{13} \ a_{12}a_{11}a_{10}a_9 \ a_8a_7a_6a_5 \ a_4a_3a_2a_1.$$

Starting from the right end of the card number, apply the function  $p(x)$  to every second digit, that is, to  $a_2, a_4, a_6, \dots$ . Then sum all of the modified and unmodified digits to get the *check sum*:

$$S = a_1 + p(a_2) + a_3 + p(a_4) + a_5 + \dots + a_{15} + p(a_{16}).$$

Then  $M$  is an invalid credit card number if the sum is not a multiple of 10, or equivalently, if  $(S \bmod 10) \neq 0$ .

For Alice's 16 digit example  $M = 4567\ 8901\ 2345\ 6789$ , Bob applies  $p(x)$  to every other digit, then the check sum is:

$$\begin{aligned} S &= 9 + p(8) + 7 + p(6) + 5 + p(4) + 3 + p(2) \\ &\quad + 1 + p(0) + 9 + p(8) + 7 + p(6) + 5 + p(4) \\ &= 9 + 7 + 7 + 3 + 5 + 8 + 3 + 4 \\ &\quad + 1 + 0 + 9 + 7 + 7 + 3 + 5 + 8 \\ &= 86. \end{aligned}$$

Since  $(86 \bmod 10) = 6$ , not 0,  $M$  is not a valid credit card number. Bob writes Alice back and asks her to reenter the card number.

If the last digit were 3, not 9, then  $(S \bmod 10) = 0$ , and the online merchant would not reject the number as an invalid credit card number.

Luhn's formula detects a single instance of two of the most common errors in typing numbers: mistyping a single digit, or (with one exception) transposing two adjacent digits. See Exercises 1.5 and 1.6.

Luhn's formula is a quick computation that an online retailer's website software can perform automatically before submitting a credit card number to a central agency for validation. The retailer can instantly detect if the customer made a simple error when keying in the card number, and ask the customer to reenter the number immediately, rather than processing a sale with an invalid number and perhaps losing the sale as a result.

Exercises 1.7 and 1.8 describe two other check digit schemes.

**A simple error correction scheme.** The most obvious way to send a message so that errors may be not just detected, but also corrected by the receiver, is to send the message several times—a repetition code.

For convenience, suppose the message is a string of zeros and ones. Alice wants to send Bob the message BUY. She replaces the letters B, U and Y by their numbering in the alphabet: 2, 21, 25, and then writes the three numbers in base 2, that is, as a sum of decreasing powers of 2:

$$2 \leftrightarrow 00010 \quad (2 = 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0),$$

$$21 \leftrightarrow 10101 \quad (21 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1),$$

$$25 \leftrightarrow 11001 \quad (25 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1).$$

Then, instead of sending 00010, 10101, 11001, Alice sends it with each bit repeated three times:

00010 becomes 000, 000, 000, 111, 000

10101 becomes 111, 000, 111, 000, 111

11001 becomes 111, 111, 000, 000, 111.

Bob looks at the message he received. Suppose it is

100, 001, 001, 111, 000

101, 000, 111, 000, 111

011, 111, 000, 000, 101.

Bob decides to determine each digit of Alice's message by choosing the most frequent digit in each position, i.e., the majority digit. For example, the digits in the first position in the three copies are 1, 0, 0. Bob chooses 0. Doing this for all fifteen positions yields 00010, 10101, 11001, the correct message that Alice sent.

This error correcting scheme works as long as there aren't two or more errors in the three copies of each bit.

Historically, this form of error correction was used in navigation in the late 18th and 19th centuries. In order to accurately determine the longitude of the location of a ship, Greenwich mean time was needed. Marine clocks, called chronometers, that would usually keep accurate time on board a ship at sea, were invented in the 1750s, but were not entirely reliable. So there was a saying among navigators, "Never go to sea with two chronometers; take one or three."

This form of error correction is called triple modular redundancy. (See "Triple modular redundancy" and "Marine chronometer" in Wikipedia.)

When using a less reliable communication channel, one could send four copies of each bit (which would correct one error and detect two errors), five copies of each bit (which would correct up to two errors), or seven copies (which would correct up to three errors), or more.

But to correct even a single error, one needs three copies of the message. So the uncoded message would be one-third of the length of the coded message. Two thirds of the transmission of the coded message is redundant. That redundancy can be costly. (The 18th century version of the cost of redundancy was the very high cost of a reliable chronometer.)

The modern science of error correcting codes involves trying to construct coding strategies that correct some errors, but without adding so much redundancy. The idea is to transform each plain message word, so that the resulting encoded word is not much larger than the plain word, but has a pattern in it. If errors occur in the transmission, the pattern will be violated. The receiver will be able to find the "nearest" message word that has the pattern. That nearest message word will be the original message word unless more errors occurred than the code is designed for.

We'll see some modern examples of error correcting codes beginning in Chapter 7.

## Exercises

- 1.1. For some moduli  $m$ , it is easy to find  $(a \bmod m)$  for any number  $a$  because of the way a number is written in base 10 notation, for example,  $365 = 300 + 60 + 5$ , and by making observations such as  $(10 \bmod 9) = 1$  and  $(10 \bmod 5) = 0$ . Try to find, without dividing:

$$\begin{aligned}(33487 \bmod 9) \\ (33487 \bmod 3) \\ (33487 \bmod 5) \\ (33487 \bmod 2).\end{aligned}$$

- 1.2. The following English language message was found, using a Caesar cipher as in Section 1.3 with an unknown key  $\kappa$ . Find the key and decrypt the message: WHH KB CWQH EO ZEREZAZ EJPK PDNAA LWNPO.
- 1.3. You and Bob use a Vigenère cipher using the numbers  $0, \dots, 28$  modulo 29, as in Section 1.3. The key word is

“ALICEROBERT”.

Encrypt the message

CALL ME AT NOON

to send to Bob.

- 1.4. Check the validity of the following card numbers by computing the Luhn check sum. If either of the card numbers is shown to be invalid, change the rightmost digit so that the resulting card number satisfies Luhn’s formula:
- (i) 4354 6172 8596 3728
  - (ii) 6011 8666 5885 1279.
- 1.5. Show that if you try to type in a valid 16-digit credit card number, but mistype one of the 16 digits, the resulting number will be shown to be invalid by Luhn’s formula.
- 1.6. Let  $S$  be the Luhn check sum for a 16-digit card number. Suppose two adjacent digits  $a_i$  and  $a_{i+1}$  of the card number are transposed, and let  $S'$  be the Luhn check sum for the resulting number.
- (i) Describe  $S - S'$  in terms of the digits  $a_i$  and  $a_{i+1}$ .
  - (ii) For which choices of the digits  $a_i$  and  $a_{i+1}$  is  $(S - S' \bmod 10) = 0$ ?
  - (iii) If  $S$  is the check sum for a valid credit card, and two adjacent digits  $a_i$  and  $a_{i+1}$  are transposed, under what conditions on the pair  $(a_i, a_{i+1})$  will  $S'$  be shown by Luhn’s formula to be an invalid credit card number?
- 1.7. The U.S. Federal Bureau of Investigation has a large database of fingerprints of individuals. In 2015 each individual in the database was given a nine-character Universal Control Number, using as characters the usual digits  $0, 1, 2, \dots, 9$  together with 17 letters of the alphabet. The letters used were chosen to be unlikely to be mistaken for any digit 0 through 9; thus letters such as I, O, B, Q, S, Z were omitted because they could be mistaken for 1, 0, 8, 0, 5 and 2. Each character was assigned a number, as follows: the characters 0 through 9 were assigned their numerical values, and A, C, D, E, F, H, J, K, L, M, N, P, R, T, V, W, X were assigned the numerical values 10 through 26, in order.
- The first eight characters of the UCN form the identifier, and the ninth character is a check digit, defined by multiplying the successive values of the identifier by 2, 4, 5, 7, 8, 10, 11 and 13, respectively, and then taking the result modulo 27. For example, the identifier EDM08TA9 corresponds to the 8-tuple  $(13, 12, 19, 0, 8, 23, 10, 9)$ , so the check digit is

$$(13 \cdot 2 + 12 \cdot 4 + 19 \cdot 5 + 0 \cdot 7 + 8 \cdot 8 + 23 \cdot 10 + 10 \cdot 11 + 9 \cdot 13 \bmod 27) \\ = (26 + 48 + 95 + 0 + 64 + 230 + 110 + 117 \bmod 27) = 15,$$

which corresponds to H. So the UCN for the identifier EDM08TA9 is EDM08TA9H.

(i) Find the check character for the identifiers

- (a) MAT13FVN,
- (b) P1EKWL83,
- (c) N01T8N0T.

(ii) Show that the FBI scheme detects all single position errors.

(iii) Show that the FBI scheme detects all transpositions of adjacent characters unless one of the characters is the check character.

(iv) Will the FBI scheme detect transpositions of any two non-check characters (such as switching E and W in P1EKWL83 to get P1WKEL83)?

- 1.8. Decades before 2015, R. W. Hamming proposed a check digit scheme similar to the FBI scheme of the last problem. Items in a large inventory are given eight-digit identifiers that are a mix of letters and numbers, where all 26 letters of the alphabet are used. If we assign the numbers 1, 2, ..., 36, 37 to the symbols 1, 2, ..., 9, 0, A, B, ..., Z, space, then each symbol is replaced by one of the numbers 1, ..., 37 (so the alphabet starts with A  $\longleftrightarrow$  11).

To add a check digit, take an identifier, say

$$X84G9P2D,$$

write down the number for each symbol:

$$34, 8, 4, 17, 9, 26, 2, 14,$$

then multiply each number by its location in the identifier:

$$1 \cdot 34 + 2 \cdot 8 + 3 \cdot 4 + 4 \cdot 17 + 5 \cdot 9 + 6 \cdot 26 + 7 \cdot 2 + 8 \cdot 14 = 457.$$

Then compute  $(457 \bmod 37) = 13$ . The check digit is the symbol corresponding to 13, namely C. Then the identifier with the check digit appended is the universal control number (UCN)

$$X84G9P2DC.$$

In general, if the symbol numbers are

$$s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8,$$

then the symbol number  $s_9$  for the check digit should satisfy the formula

$$(s_1 + 2s_2 + 3s_3 + 4s_4 + 5s_5 + 6s_6 + 7s_7 + 8s_8 \bmod 37) = s_9.$$

Hamming proposed this method for a check digit because this check digit formula will detect an error if

- a single symbol of the identifier is miscopied, such as zero by O or B by 8;
- any two symbols of the identifier are switched, such as 8 and P in the example: X84G9P2DC by XP4G982DC, unless one of the symbols is the check digit.

Justify Hamming's claims.

# Chapter 2

## Modular Arithmetic



The additive Caesar cipher in the last chapter involved addition and subtraction modulo 26 or 29. The Vernam cipher involved addition and subtraction modulo 10, as did the check digit for the Luhn formula. The FBI check character and Hamming's check digit scheme (in the exercises of Chapter 1) involved addition modulo 27 and 37. So it should be evident that modular arithmetic is useful in error correction and cryptography.

In this chapter we develop the idea of modular arithmetic in general. In Chapter 5 we'll revisit the subject.

### 2.1 Arithmetic Modulo $m$

In the last chapter we stated:

**Theorem 2.1** (Division Theorem) *Let  $m$  be a natural number. For every integer  $a$ , there are unique integers  $q$  and  $r$  so that  $a = qm + r$  and  $0 \leq r = a - mq < m$ .*

We'll prove the Division Theorem in two ways in Chapter 4, once we have introduced induction.

The number  $r$  in the Division Theorem for  $a$  and  $m$  is called the *least non-negative residue* of  $a$  modulo  $m$ , and is denoted by  $(a \bmod m)$ . (The notation is from the computer algebra language MAPLE. In Excel, the least non-negative residue of  $a$  is denoted by  $\text{MOD}(a, m)$ ).

The Division Theorem can then be restated as follows:

For every integer  $a$ , and every natural number  $m$ , there is a unique integer  $q$  so that

$$a = qm + (a \bmod m).$$

Using this notation we can describe arithmetic modulo  $m$  where the modulus  $m$  can be any natural number.

**Definition** Let  $\mathbb{Z}_m$  denote the set of numbers  $\{0, 1, 2, \dots, m - 1\}$ . Define the operations of addition  $+_m$ , subtraction  $-_m$ , and multiplication  $\cdot_m$  in  $\mathbb{Z}_m$  by

$$\begin{aligned} a +_m b &= ((a + b) \bmod m) \\ a -_m b &= ((a - b) \bmod m) \\ a \cdot_m b &= ((a \cdot b) \bmod m). \end{aligned}$$

Here the addition, subtraction, and multiplication on the right side of the equal signs are the addition, subtraction and multiplication in  $\mathbb{Z}$ .

For example, let  $m = 7$ . Then

$$5 +_7 6 = ((5 + 6) \text{ mod } 7) = (11 \text{ mod } 7) = 4$$

$$5 -_7 6 = ((5 - 6) \text{ mod } 7) = (-1 \text{ mod } 7) = 6$$

$$5 \cdot_7 6 = ((5 \cdot 6) \text{ mod } 7) = (30 \text{ mod } 7) = 2.$$

Let  $m = 43$ . Then

$$25 +_{43} 38 = ((25 + 38) \text{ mod } 43) = (63 \text{ mod } 43) = 20$$

because  $63 = 43 + 20$ , and

$$25 \cdot_{43} 38 = ((25 \cdot 38) \text{ mod } 43) = (950 \text{ mod } 43) = 4$$

because  $950 = 43 \cdot 22 + 4$ .

For  $m$  very small, we can write down tables to describe addition and multiplication mod  $m$  for all elements of  $\mathbb{Z}_m$ . Here are the tables for  $m = 3$ :

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Only a few entries are different from ordinary addition and multiplication:  $((1 + 2) \text{ mod } 3) = 0$  because the remainder on dividing  $1 + 2 = 3$  by 3 is 0. Similarly,  $(2 \cdot_3 2) = (4 \text{ mod } 3) = 1$ .

Here are the addition and multiplication tables for arithmetic mod 6:

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

For example, the barred entry  $\bar{2}$  in the addition table means that  $4 +_6 4 = 2$ . In the multiplication table the barred entry  $\bar{2}$  means that  $4 \cdot_6 5 = 2$ .

**Definition** A number  $a$  has an inverse modulo  $m$  if there is a number  $b$  so that  $a \cdot_m b = (ab \text{ mod } m) = 1$ .

A unit of  $\mathbb{Z}_m$  is a number  $a$  that has an inverse modulo  $m$ .

For example, the multiplication table for  $\mathbb{Z}_6$  shows that  $5 \cdot_6 5 = 1$ , so 5 is the inverse of itself. This means that 5 has a multiplicative inverse in  $\mathbb{Z}_6$ : 5 is a unit of  $\mathbb{Z}_6$ .

On the other hand, 4 is not a unit of  $\mathbb{Z}_6$ , because 4 does not have a multiplicative inverse in  $\mathbb{Z}_6$  (as can be seen from the table above).

Looking at multiplication modulo 7, we notice that  $3 \cdot_7 5 = 1$ , so 3 has a multiplicative inverse in  $\mathbb{Z}_7$ , namely 5 (and also that 5 has a multiplicative inverse in  $\mathbb{Z}_7$ , namely 3). Also,  $2 \cdot_7 4 = 1$ , so 2 and 4 are inverses of each other in  $\mathbb{Z}_7$ .

We will be working with units of  $\mathbb{Z}_m$  for various moduli  $m$  everywhere in the rest of this book. So we need to know: given a modulus  $m$  and a number  $a$ , how do we decide whether or not  $a$  is a unit modulo  $m$ . And if  $a$  is a unit, how do we find the inverse of  $a$ ? We'll answer both questions completely by the end of Chapter 3.

One warning. When looking for the inverse of an element  $a$  of  $\mathbb{Z}_m$ , we almost always need to do some work to find it, and if  $a$  is not a unit, the inverse of  $a$  won't even exist. So we shouldn't just write the inverse as a fraction (such as  $1/5$ ) because most fractions are not integers, and modular arithmetic involves only integers. We will never use fractional notation in modular arithmetic unless we know that the fraction is an integer.

*Example 2.2* Let's look for units of  $\mathbb{Z}_{27}$ .

How about 2? Is there some integer  $r$  so that  $2 \cdot_{27} r = 1$ ? A little thought shows that  $2 \cdot 14 = 28$  and  $(28 \bmod 27) = 1$ . So  $r = 14$  is a multiplicative inverse for 2 in  $\mathbb{Z}_{27}$ . Then also 2 is a multiplicative inverse for 14 in  $\mathbb{Z}_{27}$ . The numbers 2 and 14 are inverses of each other in  $\mathbb{Z}_{27}$ . So they are both units of  $\mathbb{Z}_{27}$ . Also, if  $ab \equiv 1 \pmod{m}$ , then  $(-a)(-b) \equiv 1 \pmod{m}$ . So  $(-2) \cdot (-14) \equiv 1 \pmod{27}$ , and so 25 and 13 are inverses of each other modulo 27.

Since  $(55 \bmod 27) = 1$  and 55 factors as  $55 = 11 \cdot 5$ , therefore 11 and 5 are multiplicative inverses of each other in  $\mathbb{Z}_{27}$ . So are 16 and 22.

Since 28 factors as  $4 \cdot 7$ , therefore 4 and 7 are multiplicative inverses of each other in  $\mathbb{Z}_{27}$ . So are 23 and 20.

Since  $27 \cdot 5 + 1 = 136 = 17 \cdot 8$ , then 17 and 8 are multiplicative inverses of each other in  $\mathbb{Z}_{27}$ . So are 10 and 19.

Of course, since  $1 \cdot 1 = 1$ , then 1 is a multiplicative inverse of itself in  $\mathbb{Z}_{27}$ . And 26 is a multiplicative inverse of itself, because  $(-1 \bmod 27) = 26$  and  $(-1) \cdot (-1) = 1$ .

Can you find other pairs?

The idea we just used to find pairs of inverses modulo  $m$  was to factor numbers of the form  $mk + 1$ . That idea is not very efficient. The idea is especially inefficient when we have a large modulus  $m$  and we want to find the inverse of a particular number  $a$  modulo  $m$ . So we'll find a better method in Chapter 3.

For some moduli  $m$  there is another set of special numbers in  $\mathbb{Z}_m$ .

**Definition** A *zero divisor* of  $\mathbb{Z}_m$  is a number  $a$  with  $0 < a < m$  for which there is a number  $b$  with  $0 < b < m$ , so that  $a \cdot_m b = 0$ .

Looking at the multiplication table for  $\mathbb{Z}_6$ , you can see that  $2 \cdot_6 3 = 0$  and  $4 \cdot_6 3 = 0$ . So 2, 3 and 4 are zero divisors in  $\mathbb{Z}_6$ .

Zero divisors may seem a bit weird. Integers under ordinary multiplication are never zero divisors. Integers satisfy the property that if  $a \neq 0$  and  $b \neq 0$ , then  $ab \neq 0$ . That fact is also true for rational numbers (fractions of integers) and real numbers, and complex numbers.

You may have seen zero divisors for the first time with matrices:

$$\begin{pmatrix} 2 & 3 \\ 4 & 6 \end{pmatrix} \begin{pmatrix} 9 & -12 \\ -6 & 8 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(If this makes no sense, you could look ahead to Chapter 7.)

The existence of zero divisors in  $\mathbb{Z}_m$  for many  $m$  is part of the fun of working with  $\mathbb{Z}_m$ . Can you guess for which  $m$  is it true that  $\mathbb{Z}_m$  has zero divisors?

**Arithmetic properties of modular arithmetic.** Addition and multiplication of integers satisfy various properties that are so natural that we don't usually think of them:

- Associativity of addition:  $a + (b + c) = (a + b) + c$  for all  $a, b, c$  in  $\mathbb{Z}$ ;
- Commutativity of addition:  $a + b = b + a$  for all  $a, b$  in  $\mathbb{Z}$ .

These two properties imply that when we have a collection of numbers we wish to add, we can do the addition in any order we wish. Thus if we want to add

$$3, 5, 8, 7, 2, 5, 3, 1, 6, 3, 4,$$

we can rearrange them as

$$3, 7, 8, 2, 5, 5, 6, 4, 3, 3, 1$$

and then observe quickly that the sum is 47.

- Existence of zero : The integer 0 satisfies  $a + 0 = a$  for all  $a$  in  $\mathbb{Z}$ ;
- Existence of negatives: for every  $a$  in  $\mathbb{Z}$  there is an integer  $b$  in  $\mathbb{Z}$  so that  $a + b = 0$ . The number  $b$  is unique (see Chapter 5), and is usually called  $-a$ .
- Associativity of multiplication:  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  for all  $a, b, c$  in  $\mathbb{Z}$ ;
- Commutativity of multiplication:  $a \cdot b = b \cdot a$  for all  $a, b$  in  $\mathbb{Z}$ ;
- Existence of one: the integer 1 satisfies  $a \cdot 1 = a$  for all  $a$  in  $\mathbb{Z}$ ;
- Distributivity:  $a \cdot (b + c) = a \cdot b + a \cdot c$  for all  $a, b, c$  in  $\mathbb{Z}$ ;

It will turn out to be true that addition and multiplication in  $\mathbb{Z}_m$  satisfies all of the properties of addition and multiplication in  $\mathbb{Z}$ . Therefore, we can work with integers modulo  $m$  almost as we do with ordinary integers. We'll explain why this is so in Chapter 5.

The one difference between working with integers and working with integers modulo  $m$  involves canceling. Because of the possible existence of zero divisors in  $\mathbb{Z}_m$ , if we have an equation involving elements of  $\mathbb{Z}_m$ , we cannot always cancel a common factor. For example, in  $\mathbb{Z}_6$ ,

$$3 \cdot_6 5 = 3 \cdot_6 1,$$

but  $5 \neq 1$ . We'll determine when we can cancel in Chapter 3.

Using the multiplication properties of  $\mathbb{Z}_m$ , we can sometimes find units in another way than by factoring  $rm + 1$  for various  $r$ . For example, in  $\mathbb{Z}_{27}$ , we know that

$$2 \cdot_{27} 14 = 1,$$

$$4 \cdot_{27} 7 = 1.$$

So multiplying the left and right sides together gives

$$(2 \cdot_{27} 14) \cdot_{27} (4 \cdot_{27} 7) = 1 \cdot_{27} 1.$$

Rearranging by associativity and commutativity of multiplication gives

$$(2 \cdot_{27} 4) \cdot_{27} (14 \cdot_{27} 7) = 1 \cdot_{27} 1,$$

which simplifies to

$$8 \cdot_{27} (98 \bmod 27) = 1.$$

So the inverse of 8 is  $(98 \bmod 27)$ , and since  $98 = 81 + 17$ , we have  $(98 \bmod 27) = 17$ .

## 2.2 Modular Arithmetic and Encryption

Modular arithmetic can help us understand and generalize the Caesar ciphers of Chapter 1.

To encrypt messages using mathematics, we first translate messages into sequences of numbers. For this section, we'll replace letters of the alphabet by position numbers in the usual way:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

and let (space) correspond to the number 0. Then a message such as “SELL THE STOCK TODAY” becomes the sequence of numbers

$$19, 5, 12, 12, 0, 20, 8, 5, 0, 19, 20, 15, 3, 11, 0, 20, 15, 4, 1, 25.$$

Since we've included (space), we will use arithmetic modulo 27 instead of modulo 26, as we did in Chapter 1.

**Additive Caesar cipher.** In Chapter 1 we constructed an additive Caesar cipher with any non-zero key  $\kappa$  in  $\mathbb{Z}_{27}$ . With the 27 symbols A ... Z and (space), encryption is done by replacing the position number  $w$  of a plaintext letter by  $c = w +_{27} \kappa$ . Decrypting is done by replacing the position number of an encrypted letter  $c$  by  $w = c -_{27} \kappa$ . There are 26 possible non-zero keys  $\kappa$  modulo 27, so there are 26 non-trivial Caesar ciphers.

**Multiplicative Caesar cipher.** Another way to encrypt the numerical message is to *multiply* each number by a fixed key  $\kappa$  in  $\mathbb{Z}_{27}$ . To illustrate, we'll choose  $\kappa = 5$ . Thus starting from the plaintext sequence of numbers arising from the message SELL THE STOCK TODAY:

$$19, 5, 12, 12, 0, 20, 8, 5, 0, 19, 20, 15, 3, 11, 0, 20, 15, 4, 1, 25,$$

we encrypt by multiplying each number by 5 in  $\mathbb{Z}_{27}$ :  $19 \cdot_{27} 5 = 14$ ,  $5 \cdot_{27} 5 = 25$ , etc. To do the encrypting, we can multiply each of the numbers by 5 in  $\mathbb{Z}$ :

$$95, 25, 60, 60, 0, 100, 40, 25, 0, 95, 100, 75, 15, 55, 0, 100, 75, 20, 5, 125$$

and then reduce each number modulo 27: thus

$$(95 \bmod 27) = 14, (25 \bmod 27) = 25, \text{ etc.}$$

We get the encrypted sequence:

$$14, 25, 6, 6, 0, 19, 13, 25, 0, 14, 19, 21, 15, 1, 0, 19, 21, 20, 5, 17.$$

Translating back to letters yields

$$NYFF\ SMY\ NSUOA\ SUTEQ.$$

We'll call this a *multiplicative Caesar cipher*.

But with the multiplicative Caesar cipher, we want to be certain that what we encrypt can be decrypted. Decrypting isn't an issue with the additive Caesar cipher. If we encrypt by adding the key  $\kappa$ , we can always decrypt by subtracting the same  $\kappa$ , both modulo 27. To undo adding  $\kappa$ , we just add  $27 - \kappa$ .

But to undo multiplication is not so easy. If we encrypt by multiplying by 5 modulo 27, can we undo that operation? Can we find a number  $d$  that solves the equation

$$5 \cdot_{27} d = 1$$

in  $\mathbb{Z}_{27}$ ? If so, then we can decrypt by multiplying by  $d$  modulo 27. This is because in  $\mathbb{Z}_{27}$ , for every number  $w$ ,

$$\begin{aligned}(w \cdot_{27} 5) \cdot_{27} d &= w \cdot_{27} (5 \cdot_{27} d) \\ &= w \cdot_{27} 1 \\ &= w,\end{aligned}$$

using the fact that in  $\mathbb{Z}_{27}$ , multiplication is associative, and 1 is a multiplicative identity.

So is there an inverse to 5 in  $\mathbb{Z}_{27}$ ?

We noticed in Example 2.2 that 11 is the multiplicative inverse of 5 in  $\mathbb{Z}_{27}$ :

$$5 \cdot_{27} 11 = 1.$$

So we can decrypt, using  $d = 11$ . We take the list of encrypted numbers

$$14, 25, 6, 6, 0, 20, 8, 5, 0, 14, 19, 21, 15, 1, 0, 19, 21, 20, 5, 17$$

and multiply each number by 11,

$$154, 275, 66, 66, 0, 209, 143, 275, 0, \dots$$

then reduce modulo 27:

$$19, 5, 12, 12, 0, 20, 8, 5, 0, \dots$$

to recover the original plaintext message.

The key  $\kappa = 5$  gives a good cipher.

But suppose we were to encrypt the same original message

$$\text{SELL THE STOCK TODAY,}$$

or, in numbers,

$$19, 5, 12, 12, 0, 20, 8, 5, 0, 19, 20, 15, 3, 11, 020, 15, 4, 1, 25,$$

by using the key  $\kappa = 6 \bmod 27$ . To do so, we multiply each plaintext number by 6:

$$114, 30, 72, 72, 0, 120, 48, 30, 0, 114, 120, 90, 18, 66, 0, 120, 90, 24, 6, 150,$$

then reduce modulo 27 to get

$$6, 3, 18, 18, 0, 12, 21, 3, 0, 6, 12, 9, 18, 12, 0, 12, 9, 24, 6, 15,$$

or, in letters,

$$FCRR \ LUC \ FLIRL \ LIXFO.$$

Let's compare the original message with the encrypted message:

$$\begin{aligned} &\text{SELL THE STOCK TODAY,} \\ &FCRR LUC FLIRL LIXFO. \end{aligned}$$

Notice that the letter K of STOCK and the letter T of TODAY both become L. Also, L and C become R, and A and S become F.

In fact, it is not hard to see that every message will be transformed into an encrypted message involving only the letters

$$C, F, I, L, O, R, U, X, (\text{space}).$$

If someone receiving the message tries to decrypt it, he would have several (in fact, three) choices for each encrypted letter. So finding the correct plaintext message would not be automatic, and could be difficult or ambiguous. (See Exercise 2.11.)

Unlike multiplying by 5, multiplying by 6 modulo 27 is not a one-to-one function, and hence there is no well-defined decrypting function. That's because 6 has no multiplicative inverse in  $\mathbb{Z}_{27}$ .

We will need to study the arithmetic of integers modulo  $m$  enough to know how to avoid encrypting with numbers like 6 modulo 27.

## 2.3 Congruence Modulo $m$

To work with integers modulo  $m$ , there is an extraordinarily convenient notation called congruence modulo  $m$ , invented by Gauss (1777–1855).

**Definition** Let  $m$  be an integer  $> 0$ . Two integers  $a$  and  $b$  are *congruent modulo  $m$* , written

$$a \equiv b \pmod{m}$$

if

$$a = b + (\text{multiple of } m),$$

or more precisely,

$$a = b + mt$$

for some integer  $t$ . The number  $m$  is called the *modulus*.

Examples:

$$55 \equiv 1 \pmod{27}$$

$$1 \equiv 55 \pmod{27}$$

$$154 \equiv 19 \pmod{27}.$$

Every multiple of 27 is congruent to 0 modulo 27, because for every integer  $t$ ,

$$27t \equiv 0 + (\text{multiple of } 27).$$

Before working with congruence, we write down some of its basic properties.

The congruence notation looks a lot like equality. In essence, congruence is an equality, but we can't show that for a while. But it's easy to show that congruence satisfies many of the standard properties of equality. Fix a modulus  $m > 0$ . We have:

**Proposition 2.3** *Congruence modulo  $m$  is an equivalence relation. That means: for all integers  $a, b, c$  and every modulus  $m > 0$ , congruence is:*

- *Reflexive:  $a \equiv a \pmod{m}$ ;*
- *Symmetric: if  $a \equiv b \pmod{m}$ , then  $b \equiv a \pmod{m}$ ;*
- *Transitive: if  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ , then  $a \equiv c \pmod{m}$ .*

All three can be proved easily and directly from the definition that  $a \equiv b \pmod{m}$  if and only if  $a = b + (\text{multiple of } m)$ .

Also, we need to see that congruence modulo  $m$  “gets along” with addition and multiplication:

**Proposition 2.4** *If*

$$a \equiv b \pmod{m} \text{ and } a' \equiv b' \pmod{m},$$

*then*

$$\begin{aligned} a + a' &\equiv b + b' \pmod{m} \\ aa' &\equiv bb' \pmod{m}. \end{aligned}$$

We prove only the multiplication rule, and leave the addition rule for congruences for you to prove (Exercise 2.20).

*Proof* The hypothesis means that  $a = b + ms$  for some integer  $k$ , and  $a' = b' + mt$  for some integer  $t$ . Then, using distributivity,

$$aa' = (b + ms)(b' + mt) = bb' + (bmt + msb' + msmt) = bb' + (\text{multiple of } m).$$

So  $aa' \equiv bb' \pmod{m}$ . □

Propositions 2 and 3 mean that we can treat a congruence modulo  $m$  just like an equality, except for canceling. (See Exercise 2.13.) In particular, we can substitute in a congruence, that is, replace a term in a congruence modulo  $m$  by another term if the two terms are congruent modulo  $m$ .

These properties of congruence can help in solving problems involving  $\mathbb{Z}_m$ .

*Example 2.5* Suppose we look at a multiplicative Caesar cipher using  $\mathbb{Z}_{29}$  and we decide to use the key  $\kappa = 16$ . Can we find its inverse?

We need to solve the equation

$$16 \cdot_{29} x = 1.$$

This is the same as the congruence

$$16x \equiv 1 \pmod{29}.$$

Let's "mess around". First, let's multiply both sides by 2:

$$32x \equiv 2 \pmod{29}.$$

Now  $32 \equiv 3 \pmod{29}$ , so we can replace 32 by 3 in the last congruence to get

$$3x \equiv 2 \pmod{29}.$$

Now  $-27 = 2 - 29 \equiv 2 \pmod{29}$ . So let's replace 2 by  $-27$  in our congruence to get

$$3x \equiv -27 \pmod{29}.$$

This has an obvious solution:  $x = -9$ . And  $-9 \equiv 20 \pmod{29}$ .

Is 20 the answer? To check, let's try  $x = 20$  in the original congruence:

$$16 \cdot 20 \equiv 1 \pmod{29}.$$

Is it true? Yes. Because  $16 \cdot 20 = 320 = 1 + 319 = 1 + 29 \cdot 11$ .

Thus  $x = 20$  is a solution of  $16 \cdot_{29} x = 1$ . In other words, 20 is the inverse of 16 in  $\mathbb{Z}_{29}$ .

What did we do? Two things: starting from  $ax = b \pmod{m}$ , we multiplied both sides of the congruence by a number  $c$  so that

$$acx \equiv bc \pmod{m}$$

and then replaced  $ac$  by  $a'$  and  $bc$  by  $b'$  where  $ac \equiv a' \pmod{m}$  and  $bc \equiv b' \pmod{m}$ , and  $a'$  divides  $b'$ . Then we can solve  $a'x \equiv b' \pmod{m}$  because we can solve  $a'x = b$  in the integers.

Solving a congruence by multiplying by some number  $c$  to make the numbers nicer can yield incorrect solutions if  $c$  is not a unit modulo  $m$ . There may be no solutions at all. See Exercise 2.17 and Section 3.7.

We'll find out in the next chapter how to decide if there is or is not a solution.

But the point of the example is that using properties of congruence, and, in particular, replacing numbers by other numbers to which they are congruent, can make the solution easier to find.

**On notation.** Earlier we introduced the notation  $(a \bmod m)$ , the least non-negative residue of  $a$  modulo  $m$ . It arose in connection with the Division Theorem. For any integer  $a$ , there is an integer  $q$  and a unique number  $r$  with  $0 \leq r < m$  so that  $a = qm + r$ . We called  $r = (a \bmod m)$ .

Now we have the notation  $a \equiv b \pmod{m}$ , which is a statement about a relationship between two numbers  $a$  and  $b$ .

There could be some confusion between the number  $(a \bmod m)$ , and the statement  $a \equiv b \pmod{m}$ . To be precise about the relationship between the two notations, we have:

**Proposition 2.6** *For all integers  $a$  and  $b$  and any modulus  $m$ :*

- $(a \bmod m) \equiv a \pmod{m}$ .
- $a \equiv b \pmod{m}$  if and only if  $(a \bmod m) = (b \bmod m)$ .

*Proof* The first statement follows immediately from the Division Theorem, which says: for every integer  $a$ , there are numbers  $q$  and  $r$  with  $0 \leq r < m$  so that

$$a = mq + r.$$

For the second statement, apply the Division Theorem to  $a$  and  $b$ :

$$\begin{aligned} a &= mq + r \\ b &= mq' + r' \end{aligned}$$

where  $0 \leq r, r' < m$ . Then  $r = (a \bmod m)$  and  $r' = (b \bmod m)$ .

If  $r = r'$ , then  $a - mq = b - mq'$ , so  $a = b + m(q' - q)$ . That means  $a \equiv b \pmod{m}$ .

On the other hand, if  $a \equiv b \pmod{m}$ , then

$$mq + r \equiv mq' + r' \pmod{m}$$

and since

$$mq \equiv mq' \equiv 0 \pmod{m}$$

(directly from the definition of congruence), it follows by substitution that

$$r \equiv r' \pmod{m}.$$

The proof is completed by showing that if  $0 \leq r, r' < m$  and  $r \equiv r' \pmod{m}$ , then  $r = r'$ . So suppose  $r \equiv r' \pmod{m}$ . Then  $r' - r = mt$  for some integer  $t$ . If  $0 \leq r \leq r' \leq m$ , then

$$m > r' \geq r' - r = mt \geq 0.$$

Dividing by  $m$  gives  $1 > t \geq 0$ . Since  $t$  is an integer,  $t = 0$  and  $r = r'$ .  $\square$

## 2.4 Letters to Numbers

Humans usually communicate in some natural language, like English. When natural language is encoded for error detection/correction or encrypted for maintaining secrecy, it is typically first translated into a sequence of natural numbers, then into “words”, sequences of elements of whatever system of “numbers” is used for the encoding/decoding or encrypting/decrypting algorithms being applied.

Perhaps the most naive way of translating English into a sequence of numbers is to observe that English is made up of words, which in turn are made up of sequences of letters. So we can translate an English sentence into a sequence of numbers by replacing each letter by its location number in the alphabet: A becomes 1, B becomes 2, ..., Z becomes 26. If we want to also include (space) and basic punctuation, we can attach a number to each of those: (space) becomes 0, (period) becomes 27, (comma): 28, (exclamation point): 29; (question mark): 30; (apostrophe): 31. In the examples in Chapters 1 and 2 we settled for just A through Z, or A through Z and (space). We will generally limit our examples to variations of this enumeration of letters.

But it is worth observing that translating written language into numbers has been of significant interest in the evolution of computers for over half a century, and has led to standardized ways of assigning numbers to symbols.

An early effort occurred in the 1960s with the development of ASCII, the American Standard Code for Information Interchange. This is a standardized way to assign numbers 0 through 127 to printable characters, such as those on a standard American keyboard, and control characters, such as (delete). Printable characters begin with (space)  $\leftrightarrow$  32, (exclamation point)  $\leftrightarrow$  33, (double quotes)  $\leftrightarrow$  34, etc.

The numerals 0, 1, 2, . . . , 9 correspond to 48, 49, . . . , 57. The English alphabet, in upper case, begins with A  $\leftrightarrow$  65, B  $\leftrightarrow$  66, . . . , Z  $\leftrightarrow$  90, and after the assignments

$$[ \leftrightarrow 91, " \leftrightarrow 92, ] \leftrightarrow 93, ^ \leftrightarrow 94, \cdot \leftrightarrow 95, ' \leftrightarrow 96,$$

the lower case alphabet begins with a  $\leftrightarrow$  97, . . . , z  $\leftrightarrow$  122. The highest number, 127, was assigned to the control character (delete).

ASCII was subsequently extended to the numbers  $\leq 255$  to include letters in other Roman-based European languages, as well as some of the Greek alphabet and some mathematical symbols. (For example,  $\alpha \leftrightarrow 224$ ,  $\infty \leftrightarrow 236$ ,  $\checkmark \leftrightarrow 251$ .)

By the 1980s the need to deal with characters used in non-western languages (for example, Chinese, Japanese, Korean, Arabic, Hindi and many others) led to the development of Unicode, a system of “unique, universal and uniform character encoding”. By 2016, Unicode included more than 100,000 characters that cover over 100 scripts and symbol sets. Unicode remains an ongoing project. (See [Unicode].)

The point is that there is now a standardized way to translate messages in almost every written language into a sequence of numbers.

So in the remainder of the book, we will assume that every message under consideration is a sequence of numbers.

**Numbers to sequences of bits.** In turn, every number can be written as a sequence of bits (0’s and 1’s). A standard way to do this is to write the number in base, or radix 2, that is, “in binary form”. Since we will need to know how to do this for a useful algorithm found in Chapter 8, here is how it can be done.

The idea is to take a number  $n$ , divide it by 2, then divide the quotient by 2, etc., until we get a quotient of 0.

*Example 2.7* Let  $n = 27$ .

$$\begin{aligned} 29 &= 14 \cdot 2 + 1 \\ 14 &= 7 \cdot 2 + 0 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 2 + 1 \\ 1 &= 0 \cdot 2 + 1. \end{aligned}$$

Then the remainders, from bottom to top, represent the number in “base 2”, or binary form. Thus

$$29 = (11101)_2.$$

This means:

$$29 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 2^4 + 2^3 + 2^2 + 1.$$

To see this, successively substitute for the quotients from bottom to top, using the equation immediately below. For example, with 29:

$$1 = 1 = (1),$$

$$3 = 2 + 1 = (11),$$

$$7 = 2 \cdot 3 + 1 = 2(2 + 1) + 1 = 2^2 + 2 + 1 = (111),$$

$$14 = 2 \cdot 7 = 2(2^2 + 2 + 1) = 2^3 + 2^2 + 2 = (1110),$$

$$29 = 2 \cdot 14 + 1 = 2(2^3 + 2^2 + 2) + 1 = 2^4 + 2^3 + 2^2 + 1 = (11101).$$

This method works because it is very easy to divide by 2 a large number written in base 10, that is, in the usual decimal notation. (Is it as easy to divide by 10 a large number written in binary form?)

A less efficient way to do the same thing is to find the highest power of 2 that is  $\leq n$ , subtract that power from  $n$ , and then repeat until you get 0. For example,

$$\begin{aligned} 29 &= 16 + 13 \\ 13 &= 8 + 5 \\ 5 &= 4 + 1 \\ 1 &= 1 + 0. \end{aligned}$$

Then successively substituting for the remainders from top to bottom gives

$$29 = 16 + 8 + 4 + 1 = (11101).$$

This is less efficient because we would continually need to consult a table of powers of 2 in order to know which is the largest power of 2  $\leq$  a given number.

## Exercises

- 2.1. (i) What is the condition on the remainder  $r$  in the Division Theorem (Theorem 2.1)  
(ii) Find the quotient  $q$  and the remainder  $r$  in the Division Theorem when the divisor  $m$  and dividend  $b$  are:  
(a)  $m = 18, b = 80$ ;  
(b)  $m = 98, b = 80$ ;  
(c)  $m = 18, b = 90$ ;  
(d)  $m = 18, b = -80$ .
- 2.2. (i) Find the units and the zero divisors for  $\mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}_6$ .  
(ii) Then guess: for which moduli  $m \geq 3$  is every non-zero number a unit? for which  $m$  does  $\mathbb{Z}_m$  have zero divisors?
- 2.3. Find the zero divisors and the units of  $\mathbb{Z}_{10}$ .
- 2.4. Knowing that  $2 \cdot_{27} 14 = 1$  and  $5 \cdot_{27} 11 = 1$  in  $\mathbb{Z}_{27}$ , find the inverse in  $\mathbb{Z}_{27}$  of  
(i) 10;  
(ii) 22;  
(iii) 25.
- 2.5. Find some of the 20 units of  $\mathbb{Z}_{33}$ .
- 2.6. Suppose we use a multiplicative Caesar cipher modulo 37. (Using modulo 37, we can encrypt words in an alphabet containing the symbols 0 through 9, A through Z and *space*.) Suppose we encrypt a message using the multiplier 18 (so that if  $a$  is the number of a plaintext letter, then  $18 \cdot_{37} a$  is the number of the encrypted letter). What is the decrypting multiplier  $d$  (so that  $(18 \cdot_{37} d = 1)$ ?
- 2.7. Observe that  $4 \cdot_{27} 7 = 1$ , or equivalently,

$$4 \cdot 7 \equiv 1 \pmod{27}.$$

Use the multiplication rule for congruences to find  $x$  satisfying

$$16x \equiv 1 \pmod{27}.$$

- 2.8. Encrypt the message COME BACK using a multiplicative Caesar cipher modulo 27 with encrypting multiplier 16.  
Then find the decrypting multiplier.
- 2.9. In the example in the text, using mod 27, the encrypting multiplier 5 for a multiplicative Caesar cipher had a corresponding decrypting multiplier 11 mod 27, because  $5 \cdot_{27} 11 = 1$ .
- (i) For each of the numbers  $e$  for  $2 \leq e \leq 13$ , decide whether or not  $e$  is a suitable encrypting multiplier, and if so, find the corresponding decrypting multiplier  $d$ . (Save your work for an exercise in the next chapter.)
  - (ii) For each number  $e$  with  $1 \leq e \leq 27$ , find a simple property of  $e$  that determines whether or not  $e$  is suitable as an encrypting multiplier modulo 27?
- 2.10. Suppose we use a multiplicative Caesar cipher modulo 26 (with  $A \leftrightarrow 1, \dots, Z \leftrightarrow 26 \equiv 0$ ), and use the encrypting multiplier 13. Which letters can occur in an encrypted message?
- 2.11. You received the subject of a message of some sensitivity using the multiplicative Caesar cipher modulo 27 with the encrypting multiplier 6. You received:

$$FRLFCRL\_RIX\_CO.$$

The first seven letters can be decrypted as SUBJECT and the remainder of the encryption is what the subject is. Find a plausible decryption of the subject. (There are at least two possibilities.)

- 2.12. Give an example of numbers  $a, b, c$  with  $0 < a, b, c < 10$  and  $a \cdot_{10} b = a \cdot_{10} c$  but  $b \neq c$ .
- 2.13. Let  $a, b, c, d$  be numbers.

(i) Show that if

$$ab \equiv ac \pmod{m}$$

and  $b \not\equiv c \pmod{m}$ , then  $a$  and  $d = b - c$  are complementary zero divisors in  $\mathbb{Z}_m$ .  
(ii) Let  $a$  and  $d$  be complementary zero divisors in  $\mathbb{Z}_m$  (so that  $a$  and  $d$  are non-zero modulo  $m$ ). Let  $c$  be any element of  $\mathbb{Z}_m$  and let  $b = c + d \pmod{m}$ . Show that

$$ab \equiv ac \pmod{m}$$

but  $b \not\equiv c \pmod{m}$ .

- 2.14. (i) Solve the congruence

$$20x \equiv 1 \pmod{37}.$$

(ii) For a multiplicative Caesar cipher modulo 37, suppose we encrypt a message using the multiplier 20 (so that if  $a$  is the number of a plaintext letter, then  $20 \cdot_{37} a$  is the number of the encrypted letter). What is the decrypting multiplier  $d$  (so that  $(20 \cdot_{37} d = 1)$ )?

- 2.15. Solve the congruence  $9x \equiv 1 \pmod{31}$ .
- 2.16. Solve the equation  $13 \cdot_{37} x = 1$  by turning it into a congruence modulo 37.
- 2.17. Try to solve the congruence

$$16x \equiv 1 \pmod{30}$$

by first multiplying both sides of the congruence by 2. Is the resulting solution correct? What went wrong?

- 2.18. Prove that congruence modulo  $m$  is transitive: if  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ , then  $a \equiv c \pmod{m}$ .
- 2.19. Explain why it is so that for all numbers  $e > 0$ , if  $a \equiv b \pmod{m}$ , then  $a^e \equiv b^e \pmod{m}$ .
- 2.20. Prove the addition rule for congruence: if  $a \equiv b \pmod{m}$ , then for all integers  $c$ ,  $a + c \equiv b + c \pmod{m}$ .
- 2.21. Suppose  $a \cdot b \equiv d \pmod{m}$  and  $b \equiv e \pmod{m}$ . Using properties of congruence listed in the text, carefully explain why substituting  $b$  by  $e$  to get  $a \cdot e \equiv d \pmod{m}$  gives a correct congruence.
- 2.22. (i) Is it true that for each number  $a$  with  $1 \leq a \leq 10$ , there is a number  $r$  so that  $(2^r \bmod 11) = a$ ? (Explain.)  
(ii) Is it true that for each number  $a$  with  $1 \leq a \leq 10$ , there is a number  $r$  so that  $(3^r \bmod 11) = a$ ? (Explain.)
- 2.23. Using properties of congruence modulo 9, explain why every number is congruent modulo 9 to the sum of its digits.
- 2.24. Write in base 2:
  - (i) 113
  - (ii) 240
  - (iii) 751.
- 2.25. Write 271,234 in base 2.
- 2.26. For a number  $n$  lying between  $2^r$  and  $2^{r+1}$ , what is the maximum number of divisions that would be required to find  $n$  in base 2?

# Chapter 3

## Linear Equations Modulo $m$



In Chapter 2 we introduced  $\mathbb{Z}_m$ , the set of numbers

$$\{0, 1, 2, \dots, m - 1\}$$

with addition and multiplication modulo  $m$ . We were interested in solving equations involving elements of  $\mathbb{Z}_m$ , equations of the form

$$a \cdot_m x = b.$$

We introduced congruence modulo  $m$ , and showed that we can translate the question,

- Is there an integer  $x$  so that

$$a \cdot_m x = b?$$

into several other forms:

- Is there an integer  $x$  so that

$$(ax \bmod m) = b?$$

- Is there an integer  $x$  that satisfies the congruence

$$ax \equiv b \pmod{m}?$$

- Are there integers  $x, y$  so that

$$ax + my = b?$$

If we can find integers  $x$  and  $y$  that solve this last equation, then that integer  $x$  will also be a solution to the other three problems.

In this chapter, for any linear equation  $ax + my = b$  with  $a, m$  and  $b$  integers, we determine whether or not the equation has a solution with  $x, y$  integers. If so, we show how to find all solutions efficiently. The method, Euclid's Algorithm, has been known for 2300 years, which means it predates the use of 0 or negative numbers, and is also older than the usual algorithms for multiplication and division of integers.

Modular arithmetic is used in all of the cryptography and error correction methods found in this book. So the results in this chapter are essential for nearly everything that follows.

### 3.1 The Greatest Common Divisor

The Division Theorem, proved in Chapter 4, says that if  $a > 0$  and  $b$  are non-negative integers, then there are unique non-negative integers  $q$  and  $r$  so that

$$b = aq + r$$

and  $0 \leq r < a$ .

The Division Theorem describes what comes out of doing long division, dividing  $b$  by  $a$ . Recall the terminology:  $a$  is the *divisor*,  $b$  is the *dividend*,  $q$  is the *quotient*,  $r$  is the *remainder*.

**Definition** A non-zero integer  $a$  *divides* an integer  $b$ , if  $b = aq$  for some integer  $q$ .

Other terminology for the same thing:  $a$  is a divisor of  $b$ , or  $a$  is a factor of  $b$ , or  $b$  is a multiple of  $a$ .

If  $b > a > 0$  and we do long division with  $a$  as the divisor and  $b$  the dividend, then  $a$  divides  $b$  if the remainder  $r = 0$ .

Examples: The number 3 divides 15 because  $15 = 3 \cdot 5$ , but 3 does not divide 16 because  $16 = 3 \cdot 5 + 1$ .

The number 100 divides all and only those integers whose last two digits end in 00 (such as 300 or 2300, but not 3550 or 678).

The number 2 divides every number whose last digit is 0 or 2 or 4 or 6 or 8, but no other numbers.

The number 9 divides a number  $a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$  if and only if 9 divides  $a_n + a_{n-1} + \dots + a_1 + a_0$ . (See Exercise 3.2.)

The number 1 divides every number. Every number divides itself.

Finding negative divisors is essentially the same as finding positive divisors. For if  $a$  divides  $b$ , then  $ac = b$  for some integer  $c$ , and then  $(-a)(-c) = b$ , so  $-a$  also divides  $b$ . So in looking for divisors of a number  $b$ , we usually restrict attention to positive divisors.

For small numbers, we can write down all the positive divisors. For example:

The number 48 has the divisors 1, 2, 3, 4, 6, 8, 12, 16, 24 and 48.

The number 210 has the divisors 1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105 and 210.

Given two numbers  $a$  and  $b$ , we will be interested in the *common divisors* of  $a$  and  $b$ , that is, all the numbers that divide both  $a$  and  $b$ .

The common divisors of the numbers 48 and 210 can be obtained by comparing the two lists of divisors of each number. Doing so, we find that the common divisors of 48 and 210 are 1, 2, 3, and 6.

Of particular interest to us for modular arithmetic is the largest number among the common divisors of the two numbers. For 48 and 210, that largest common divisor is 6.

**Definition** Let  $a, b$  be two natural numbers. The *greatest common divisor* of  $a$  and  $b$  is the largest number  $d$  which is both a divisor of  $a$  and a divisor of  $b$ .

The greatest common divisor of two numbers  $a$  and  $b$  is denoted by  $(a, b)$ .

*Example 3.1* The greatest common divisor of 8 and 6 is  $(8, 6) = 2$ , as is easily checked. Also,  $(9, 6) = 3$ ,  $(12, 6) = 6$ ,  $(15, 6) = 3$  and  $(19, 6) = 1$ .

A special case: If  $a$  and  $b$  are two numbers and  $a$  divides  $b$ , then  $(a, b) = a$ . So  $(3, 15) = 3$ , and  $(34, 3468) = 34$  (because  $3468 = 34 \cdot 102$ ).

Here is the opposite extreme:

**Definition** Two non-zero integers whose greatest common divisor is 1 are called *coprime* or *relatively prime*.

For example, 8 and 15 are coprime, as are 6 and 19. Every number is coprime to 1. But 6 and 15 are not coprime.

We'll see soon that knowing the greatest common divisor of two numbers  $a$  and  $m$  tells us a great deal about whether we can solve the equation  $a \cdot_m x = b$  in  $\mathbb{Z}_m$ .

But finding the greatest common divisor of two numbers by finding all the divisors of each number separately and comparing the lists of divisors is usually not an efficient way to proceed.

One mathematical objective of this chapter is to find a better way.

**The greatest common divisor and multiplicative Caesar ciphers.** Why is the greatest common divisor of two numbers of interest in modular arithmetic?

When we looked at the multiplicative Caesar cipher, we found that encrypting a number  $a < 27$  by multiplying  $a$  by the encrypting multiplier  $5 \bmod 27$  is a useable encryption function, because the receiver can decrypt by multiplying the encrypted number by a decrypting multiplier,  $11 \bmod 27$ . The reason 11 works is that

$$5 \cdot_{27} 11 = 1,$$

so when we multiply the encrypted letter  $a \cdot_{27} 5$  by 11, we obtain

$$\begin{aligned}(a \cdot_{27} 5) \cdot_{27} 11 &= a \cdot_{27} (5 \cdot_{27} 11) \\ &= a \cdot_{27} 1 = a\end{aligned}$$

by associativity of multiplication mod 11.

On the other hand, multiplying  $a$  by 6 mod 27 did not give a useful cipher, because there is no decrypting multiplier for 6. There is no number  $c$  so that

$$6 \cdot_{27} c = 1.$$

In general, given a modulus  $m$  (such as  $m = 26$  or 27), and given a possible encrypting multiplier  $e$  (such as  $e = 5$  or 6), then  $d$  is a decrypting multiplier for  $e$  if and only if  $e \cdot_m d = 1$ . Among the equivalent ways to express this condition is that there is an integer  $t$  so that

$$ed = 1 + mt \text{ for some integer } t.$$

In particular, to solve  $6 \cdot_{27} d = 1$  is the same as to find integers  $d$  and  $t$  so that

$$6d = 1 + 27t$$

or, rewriting slightly,

$$6d - 27t = 1.$$

In this form it is easy to see why there is no solution in  $\mathbb{Z}$ . The numbers 6 and 27 have a common divisor  $> 1$ , namely, 3. So

$$6d - 27t = 3(2d - 9t),$$

and the equation we want to solve is

$$3(2d - 9t) = 1.$$

If there were integers  $d$  and  $t$  satisfying  $3(2d - 9t) = 1$ , then 3 would be a divisor of 1. But the only divisors of 1 in  $\mathbb{Z}$  are 1 and  $-1$ .

Generalizing the situation for  $m = 27$  and  $e = 6$ , we see easily the following fact.

**Proposition 3.2** Suppose  $e$  and  $m$  have a common divisor  $> 1$ . Then there is no number  $d$  so that  $e \cdot_m d = 1$ .

Thus if  $(e, m) > 1$ , then  $e$  cannot be used as an encrypting multiplier for a multiplicative Caesar cipher in  $\mathbb{Z}_m$ .

On the other hand, suppose  $e$  is coprime to  $m$  (such as 5 and 27). Can we then be sure we can use  $e$  as an encrypting multiplier in  $\mathbb{Z}_m$ ? As we'll see, the answer is "yes".

## 3.2 Finding the Greatest Common Divisor

Evidently, knowing the greatest common divisor of two numbers is useful. So how do we find the greatest common divisor efficiently?

It turns out (fortunately!) that we can find the greatest common divisor of two numbers without knowing ahead of time any divisors of either number.

The key is the following fact:

**Lemma 3.3** Suppose  $a, b, c$  are numbers and  $b = aq + c$  for some integer  $q$ . Then every number  $s$  that divides both  $b$  and  $a$ , also divides  $c$ , and every number  $t$  that divides both  $c$  and  $a$ , also divides  $b$ .

*Proof* All we need to do is substitute: if  $s$  divides  $a$ , then  $a = sa'$  for some integer  $a'$ . If  $s$  divides  $b$ , then  $b = sb'$  for some integer  $b'$ . Then

$$c = b - aq = sb' - (sa')q = s(b' - a'q),$$

and  $(b' - a'q)$  is an integer. So  $s$  divides  $c = b - aq$ .

The same argument shows that if  $t$  divides  $c$  and  $t$  divides  $a$ , then  $t$  divides  $c + aq = b$ .  $\square$

Lemma 3.3 yields immediately:

**Corollary 3.4** If  $b = aq + c$ , then the common divisors of  $b$  and  $a$  are the same as the common divisors of  $c$  and  $a$ . Hence the greatest common divisor of  $b$  and  $a$  is equal to the greatest common divisor of  $c$  and  $a$ . In symbols,

$$\text{if } b = aq + c, \text{ then } (a, b) = (a, c).$$

We can apply this to find the greatest common divisor of two numbers  $a$  and  $b > a$  by using the Division Theorem, repeatedly if necessary.

*Example 3.5* To find the greatest common divisor of 12345 and 24693, we apply Corollary 3.4. We divide the smaller number, 12345, into the larger number, 24693:

$$24693 = 12345 \cdot 2 + 3.$$

So by Corollary 3.4, the greatest common divisor of 12345 and 24693 is equal to the greatest common divisor of 12345 and 3. Since 3 divides  $12345 = 4115 \cdot 3$ , therefore the greatest common divisor of 12345 and 3 is 3.

*Example 3.6* Suppose we want to find the greatest common divisor of 429 and 923. We apply Corollary 3.4. Write

$$923 = 429 \cdot 2 + 65.$$

Then  $(923, 429) = (429, 65)$ .

To find  $(429, 65)$  we can factor 65, to get  $65 = 13 \cdot 5$ . So 65 has divisors 1, 5, 13 and 65. Which of these divide 429? That's easy to check: 1 does, 5 doesn't, and so 65 doesn't, but 13 does:  $429 = 13 \cdot 33$ . So 13 is the greatest common divisor of 65 and 429. So by Corollary 3.4, 13 is the greatest common divisor of 429 and 923.

But why use Corollary 3.4 just once?

If  $a < b$  and we use the Division Theorem to divide  $a$  into  $b$  to get  $b = aq + r$ , then  $(b, a) = (a, r)$ . Since  $r < a < b$ , we've replaced the problem, “find  $(b, a)$ ” with “find  $(a, r)$ ”, the same problem with smaller numbers. So if we repeatedly divide the smaller number into the larger number, we'll make the original problem of finding  $(b, a)$  very easy.

*Example 3.7* We use Corollary 3.4 to find the greatest common divisor of 22911 and 9856. To begin, we divide the smaller number, 9856, into the larger number, 22911:

$$22911 = 9856 \cdot 2 + 3199.$$

Then the greatest common divisor of 22911 and 9856 is equal to the greatest common divisor of 9856 and 3199. Now divide the remainder, 3199, into the divisor, 9856:

$$9856 = 3199 \cdot 3 + 259.$$

The greatest common divisor of 9856 and 3199 is equal to the greatest common divisor of 3199 and 259. Let's divide again:

$$3199 = 259 \cdot 12 + 91.$$

And again:

$$259 = 91 \cdot 25 + 77.$$

And again, three more times:

$$91 = 77 + 14,$$

$$77 = 14 \cdot 5 + 7,$$

and

$$14 = 7 \cdot 2 + 0.$$

Then  $(22911, 9856) = (14, 7) = 7$ . With repeated dividing, we never need to look at any factors of any numbers.

Let us write down all these equations in a list:

$$\begin{aligned} 22911 &= 9856 \cdot 2 + 3199 \\ 9856 &= 3199 \cdot 3 + 259 \\ 3199 &= 259 \cdot 12 + 91 \\ 259 &= 91 \cdot 25 + 77 \\ 91 &= 77 + 14 \\ 77 &= 14 \cdot 5 + 7 \\ 14 &= 7 \cdot 2 + 0. \end{aligned}$$

Each line is the result of dividing the remainder of the previous line into the divisor of the previous line.

The last line implies that the greatest common divisor of 7 and 14 is 7. By Corollary 3.4, 7 is then the greatest common divisor of 22911 and 9865.

Notice that the greatest common divisor, 7, is the last non-zero remainder in our list. So the last non-zero remainder in our list of divisions is the greatest common divisor of 22911 and 9865, our original two numbers.

The list of divisions we just wrote down is called Euclid's Algorithm for 9856 and 22911. Euclid's Algorithm is a method to find the greatest common divisor of any two numbers  $a$  and  $b$ .

**Euclid's Algorithm.** In Euclid's Algorithm for finding the greatest common divisor of two numbers, we divide the smaller number (the divisor) into the larger number (the dividend). We get a remainder. Then we repeat, with the divisor becoming the new dividend, and the remainder becoming the new divisor. Then we repeat, again and again, until we get a remainder of 0. Then the last non-zero remainder is the greatest common divisor of the two original numbers.

Here is a description of Euclid's Algorithm in general notation:

**Definition** Let  $b > a > 0$  be natural numbers. The sequence of instances of the Division Theorem:

$$\begin{aligned} b &= q_1 a + r_1 \quad 0 < r_1 < a \\ a &= q_2 r_1 + r_2 \quad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \quad 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

is called Euclid's Algorithm.

Note that Euclid's Algorithm stops for any two starting numbers  $a$  and  $b \geq a$ . For we have

$$a > r_1 > r_2 > \dots > r_{n-1} > r_n > \dots \geq 0.$$

Since there are  $a - 1$  numbers  $< a$ , there can be at most  $a - 1$  non-zero remainders. (But in fact, Euclid's Algorithm is much faster than this last argument suggests. The number of steps in Euclid's Algorithm is  $\leq$  five times the number of decimal digits of the smaller number  $a$ . The number of decimal digits of  $a$  is approximately  $\log_{10}(a)$ , which is far smaller than  $a - 1$ . See the exercises at the end of this chapter.)

The point of Euclid's Algorithm is:

**Theorem 3.8** *Let  $r_n$  be the last non-zero remainder in Euclid's Algorithm. Then  $r_n = (a, b)$ , the greatest common divisor of  $a$  and  $b$ .*

*Proof* This follows by  $n$  applications of Corollary 3.4, which, working down the lines of Euclid's Algorithm, says that

$$(b, a) = (a, r_1) = (r_1, r_2) = \dots = (r_{n-1}, r_n),$$

and  $(r_{n-1}, r_n) = r_n$  because  $r_n$  divides  $r_{n-1}$ . □

But Euclid's Algorithm is not only an efficient way to find the greatest common divisor of two numbers. It also provides us with a tool for solving equations in  $\mathbb{Z}_m$ , as we'll see.

### 3.3 Bezout's Identity

The key to solving linear equations in  $\mathbb{Z}_m$  is

**Theorem 3.9** (Bezout's Identity) *Let  $d = (a, m)$  be the greatest common divisor of the natural numbers  $a$  and  $m$ . Then there are integers  $s, t$  so that*

$$d = as + mt.$$

*Example 3.10* We see easily that  $(24, 14) = 2$ , and see somewhat less easily that Bezout's Identity,  $24s + 14t = 2$ , has a solution  $s = 3, t = -5$ :

$$24 \cdot 3 + 14 \cdot (-5) = 2.$$

Also,  $(21, 13) = 1$  and  $13 \cdot 13 + 21 \cdot (-8) = 169 - 168 = 1$ . We also have  $13 \cdot (-8) + 21 \cdot 5 = -104 + 105 = 1$ , which illustrates that there is more than one possible solution of Bezout's Identity,  $ax + my = d$ .

Also,  $(5, 10) = 5$  and  $5 = 5 \cdot 1 + 10 \cdot 0 = 5 \cdot 3 + 10 \cdot (-1)$ .

Bezout's Identity tells us exactly when an equation  $ax + by = e$  is solvable for  $x, y$  in  $\mathbb{Z}$ .

We'll show how to find Bezout's Identity in the next section. But here, let's assume that Bezout's Identity is true, and derive some consequences.

The first is to tell us exactly when a linear equation with integer coefficients has an integer solution.

**Theorem 3.11** *Let  $a, m, e$  be natural numbers. The equation  $ax + my = e$  has a solution with  $x, y$  integers if and only if  $d = (a, m)$  is a divisor of  $e$ .*

*Proof* Let  $d$  be the greatest common divisor of  $a$  and  $b$ . By Bezout's Identity, there are integers  $s, t$  so that

$$d = as + mt.$$

Suppose that  $e = dq$  for some number  $q$ . Then

$$e = dq = (as + mt)q = a(sq) + m(tq),$$

so  $ax + my = e$  has a solution  $x = sq, y = tq$  with  $x, y$  integers.

Conversely, if  $d$  is the greatest common divisor of  $a$  and  $m$ , then  $d$  divides  $a$  and  $m$ , so  $a = dz, m = dw$  for some integers  $z, w$ . If

$$as + bt = e$$

for some integers  $s$  and  $t$ , then substituting for  $a$  and  $b$  gives

$$dzs + dwt = e,$$

so

$$d(zs + wt) = e.$$

Thus  $e$  is a multiple of  $d$ . □

*Example 3.12* We saw that  $(24, 14) = 2$  and that

$$2 = -70 + 72 = 14 \cdot (-5) + 24 \cdot 3.$$

To solve  $14x + 24y = 8$  (that is, find integers  $x$  and  $y$  satisfying the equation), multiply the equation

$$14 \cdot (-5) + 24 \cdot 3 = 2$$

by 4, to get

$$14 \cdot (-5) \cdot 4 + 24 \cdot 3 \cdot 4 = 2 \cdot 4 = 8$$

or

$$14 \cdot (-20) + 24 \cdot 12 = 8.$$

Thus  $x = -20$ ,  $y = 12$ .

Theorem 3.11 immediately yields:

**Corollary 3.13** *If  $d = (a, m)$ , then there is a solution to the congruence*

$$ax \equiv e \pmod{m}$$

and a solution in  $\mathbb{Z}_m$  to the equation

$$a \cdot_m x = e$$

if and only if  $d$  divides  $e$ .

Corollary 3.13 implies that if  $(a, m) = 1$ , then the equation  $a \cdot_m x = 1$  is solvable in  $\mathbb{Z}_m$ . Corollary 3.13 and Proposition 3.2 confirm that for a multiplicative Caesar cipher modulo  $m$ , the number  $e$  is a valid encrypting multiplier if and only if  $e$  is coprime to  $m$ .

More generally, we now know whether or not it is possible to solve equations  $a \cdot_m x = b$  in  $\mathbb{Z}_m$ :

*Example 3.14* Suppose we know that  $(111, 81) = 3$  and find that Bezout's Identity is  $3 = 81 \cdot 11 - 111 \cdot 8$ . If we want to solve

$$81 \cdot_{111} x = 42,$$

or, equivalently, the congruence

$$81 \cdot x \equiv 42 \pmod{111},$$

we observe that

$$81 \cdot 11 \equiv 3 \pmod{111},$$

and  $42 = 3 \cdot 14$ . So we just multiply both sides of this last congruence by 14 to get

$$81 \cdot 11 \cdot 14 \equiv 3 \cdot 14 = 42 \pmod{111}.$$

So

$$x \equiv 11 \cdot 14 = 154 \equiv 43 \pmod{111}.$$

If we want to solve

$$81 \cdot_{111} x = 47,$$

we observe that  $3 = (81, 111)$  does not divide 47, so there is no solution.

### 3.4 Finding Bezout's Identity

How do we find Bezout's Identity for two numbers  $a$  and  $b$ ?

For example, how do we solve  $13x + 28y = 1$ ?

One naive way might be to write the equation as  $13x = -28y + 1$ . Then write down multiples of 28 in one list, add 1 to each, and also write down multiples of 13.

$$28, 56, 84, 112, 140, 168, 196, 224, 252, 280, \dots$$

$$29, 57, 85, 113, 141, 169, 197, 225, 253, 281, \dots$$

$$13, 26, 39, 52, 65, 78, 91, 104, 117, 130, 143, 156, 169, 182, 195, 208, 221, \dots$$

Then we look for a number common to the second and third lists: we find that

$$169 = 13 \cdot 13 = 28 \cdot 6 + 1,$$

so  $x = 13, y = -6$  is a solution:

$$13 \cdot 13 + 28 \cdot (-6) = 1.$$

But in practice this method is rather inefficient, if not impossible, if  $a$  and  $b$  have many digits.

Fortunately, there is a better way.

**EEA.** The most efficient way to find Bezout's Identity, that is, solve the equation  $ax + by = (a, b)$ , is to work from Euclid's Algorithm. Here is the key idea:

**Lemma 3.15** *Given two fixed numbers  $a, b$ , suppose  $e$  and  $f$  are integers and*

$$e = s_1a + s_2b$$

and

$$f = t_1a + t_2b$$

for some integers  $s_1, s_2, t_1, t_2$ . If  $e = qf + r$ , then

$$\begin{aligned} r &= e - fq \\ &= (s_1a + s_2b) - q(t_1a + t_2b) \\ &= w_1a + w_2b \end{aligned}$$

where

$$w_1 = s_1 - qt_1$$

$$w_2 = s_2 - qt_2.$$

*Example 3.16* Let  $a = 23, b = 13$ . Suppose we notice that

$$23 \cdot 4 + 13 \cdot (-6) = 92 - 78 = 14$$

$$23 \cdot (-1) + 13 \cdot 2 = -23 + 26 = 3.$$

Suppose we also observe that  $1 = 3 \cdot 5 - 14$ . Then to solve the equation

$$1 = 13x + 23y,$$

we substitute for 14 and 3 in the equation  $1 = 3 \cdot 5 - 14$ , and then collect coefficients of 23 and 13, as follows. Writing 23 and 13 in boldface type, we obtain

$$\begin{aligned} 1 &= 3 \cdot 5 - 14 \\ &= (\mathbf{23} \cdot (-1) + \mathbf{13} \cdot 2) \cdot 5 - (\mathbf{23} \cdot 4 + \mathbf{13} \cdot (-6)). \end{aligned}$$

Collecting coefficients of **13** and **23** gives:

$$\begin{aligned} 1 &= \mathbf{23} \cdot (-5 - 4) + \mathbf{13} \cdot (2 \cdot 5 + 6) \\ &= \mathbf{23} \cdot (-9) + \mathbf{13} \cdot 16, \end{aligned}$$

(which is true:  $1 = -207 + 208$ ).

Some terminology. Given numbers  $a$  and  $b$ , if  $e = ra + sb$  for some integers  $r$  and  $s$ , we say that  $e$  is an *integer linear combination* of  $a$  and  $b$ . (The terminology is from elementary linear algebra.) Lemma 3.15 says that if  $e$  and  $f$  are integer linear combinations of  $a$  and  $b$ , and  $e = fq + r$ , then  $r$  is an integer linear combination of  $a$  and  $b$ .

If we know how  $e$  and  $f$  are integer linear combinations of  $a$  and  $b$ , we want to efficiently find  $r$  as an integer linear combination of  $a$  and  $b$ . The method of the last example shows how to do it. But following that example in practice often leads to errors, because in the equations it is hard to keep track of which numbers are coefficients of  $a$  and  $b$  and which numbers are  $a$  and  $b$ . We tried to reduce confusion in the example by writing  $a = 23$  and  $b = 13$  in boldface.

But the method of vectors we now introduce eliminates confusion, because it isolates and only works with the coefficients.

For that purpose, we introduce (or recall from analytic geometry) vectors and the operations of addition and scalar multiplication of vectors.

**Definition** Let  $s_1, s_2, s_3$  be integers. A vector with three components is an ordered 3-tuple of integers, of the form  $(s_1, s_2, s_3)$ .

We add vectors by

$$(s_1, s_2, s_3) + (t_1, t_2, t_3) = (s_1 + t_1, s_2 + t_2, s_3 + t_3).$$

We subtract one vector from another by

$$(s_1, s_2, s_3) - (t_1, t_2, t_3) = (s_1 - t_1, s_2 - t_2, s_3 - t_3).$$

We multiply a vector by a scalar (an integer)  $k$ , by

$$k(s_1, s_2, s_3) = (ks_1, ks_2, ks_3).$$

The operations are done component-by-component.

We'll see many examples shortly.

**Definition** Given two fixed numbers  $a$  and  $b$ , a vector  $(e, s_1, s_2)$  of integers is *an EEA vector for  $a$  and  $b$*  if  $e = s_1a + s_2b$ .

These are the vectors we will use to find Bezout's identity for  $a$  and  $b$ .

For example, with  $a = 23$ ,  $b = 13$ , we have

$(14, 4, -6)$  is an EEA vector for 23 and 13, because  $14 = 4 \cdot 23 + (-6) \cdot 13$ . (Check:  $92 - 78 = 14$ .)

$(3, -1, 2)$  is an EEA vector for 23 and 13, because  $3 = (-1) \cdot 23 + 2 \cdot 13$ .

With this notation, Lemma 3.15 can be rewritten using EEA vectors:

**Lemma 3.17** *Given two fixed numbers  $a, b$ , suppose  $e$  and  $f$  are integers and*

$$e = s_1a + s_2b$$

*and*

$$f = t_1a + t_2b$$

*for some integers  $s_1, s_2, t_1, t_2$ . Then*

$$(e, s_1, s_2) \text{ and } (f, t_1, t_2)$$

*are EEA vectors for  $a$  and  $b$ . If  $e = qf + r$ , then*

$$(e, s_1, s_2) - q(f, t_1, t_2) = (e - qf, s_1 - qt_1, s_2 - qt_2) = (r, s_1 - qt_1, s_2 - qt_2)$$

*is an EEA vector for  $a$  and  $b$ , because*

$$r = (s_1 - qt_1)a + (s_2 - qt_2)b.$$

Using EEA vectors, we can find Bezout's identity for two numbers  $a$  and  $b$  by manipulating EEA vectors. We illustrate with some examples.

*Example 3.18* Suppose  $a = 87, b = 38$ , and we find that

$$11 = 1 \cdot 87 + (-2) \cdot 38$$

and

$$5 = (-3) \cdot 87 + 7 \cdot 38.$$

Then  $(11, 1, -2)$  and  $(5, -3, 7)$  are EEA vectors for 87 and 38. If we divide 5 into 11, we find that  $11 = 2 \cdot 5 + 1$ , so

$$1 = 11 - 2 \cdot 5.$$

Using this last equation we can find an EEA vector for 1 by vector addition and scalar multiplication:

$$\begin{aligned} (11, 1, -2) - 2(5, -3, 7) &= (11, 1, -2) + (-10, 6, -14) \\ &= (11 + (-10), 1 + 6, (-2) + (-14)) \\ &= (1, 7, -16). \end{aligned}$$

This last vector corresponds to the equation

$$1 = 7 \cdot 87 - 16 \cdot 38$$

(which is true:  $1 = 609 - 608$ ).

We can apply Lemma 3.17 to find a solution of Bezout's Identity by using EEA vectors and working our way down Euclid's Algorithm. The resulting algorithm is called the Extended Euclidean Algorithm, or EEA.

*Example 3.19* Here is Euclid's Algorithm for 35 and 24:

$$\begin{aligned} 35 &= 24 + 11 \\ 24 &= 2 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + 1. \end{aligned}$$

Solve for the remainders:

$$\begin{aligned} 35 - 24 &= 11 \\ 24 - 2 \cdot 11 &= 2 \\ 11 - 5 \cdot 2 &= 1. \end{aligned}$$

We use this to get Bezout's Identity, which will express the greatest common divisor, 1, in terms of 35 and 24. Begin with the two obvious equations

$$\begin{aligned} 35 &= 1 \cdot 35 + 0 \cdot 24, \\ 24 &= 0 \cdot 35 + 1 \cdot 24. \end{aligned}$$

Write the corresponding EEA vectors:

$$\begin{aligned} (35, 1, 0) \\ (24, 0, 1). \end{aligned}$$

Using the EEA vectors for 35 and 24, we apply the relation  $35 - 24 = 11$  to find an EEA vector for 11:

$$(35, 1, 0) - (24, 0, 1) = (11, 1, -1).$$

This last vector says that  $11 = 1 \cdot 35 + (-1) \cdot 24$  (which is clearly true).

The next line of Euclid's algorithm yields the equation for the next remainder:

$$24 - 2 \cdot 11 = 2.$$

Take the EEA vectors for 24 and 11 and apply the relation  $24 - 2 \cdot 11 = 2$  to find an EEA vector for 2:

$$(24, 0, 1) - 2(11, 1, -1) = (2, -2, 3).$$

This last vector says that

$$2 = (-2) \cdot 35 + 3 \cdot 24,$$

which is true:  $2 = -70 + 72$ .

The last line of Euclid's algorithm yields the equation for the last remainder:

$$11 - 5 \cdot 2 = 1.$$

Take the EEA vectors for 11 and 2 and apply the relation  $11 - 5 \cdot 2 = 1$  to find an EEA vector for 1:

$$(11, 1, -1) - 5(2, -2, 3) = (1, 11, -16).$$

This last vector says that

$$1 = 11 \cdot 35 + (-16) \cdot 24,$$

which is true:  $1 = 385 - 384$ . We have found the coefficients in Bezout's Identity for 35 and 24.

Some more examples:

*Example 3.20* Here is Euclid's algorithm for 85 and 37:

$$\begin{aligned} 85 &= 2 \cdot 37 + 11 \\ 37 &= 3 \cdot 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0. \end{aligned}$$

Isolate the non-zero remainders:

$$\begin{aligned} 85 - 2 \cdot 37 &= 11 \\ 37 - 3 \cdot 11 &= 4 \\ 11 - 2 \cdot 4 &= 3 \\ 4 - 1 \cdot 3 &= 1. \end{aligned}$$

To find the coefficients  $s$  and  $t$  in Bezout's Identity:  $1 = s \cdot 85 + t \cdot 37$ , we perform the EEA: begin with the vectors

$$\begin{aligned} (85, 1, 0) \\ (37, 0, 1), \end{aligned}$$

and then for each of the remainders 11, 4, 3 and 1 in Euclid's algorithm, we find the EEA vectors that describe how to write that remainder as an integer linear combination of 85 and 37. Beside each step is the corresponding equation.

$$\begin{aligned} (85, 1, 0) &\longleftrightarrow 85 = 1 \cdot 85 + 0 \cdot 37 \\ (37, 0, 1) &\longleftrightarrow 37 = 0 \cdot 85 + 1 \cdot 37 \\ (85, 1, 0) - 2(37, 0, 1) = (11, 1, -2) &\longleftrightarrow 11 = 1 \cdot 85 + (-2) \cdot 37 \\ (37, 0, 1) - 3(11, 1, -2) = (4, -3, 7) &\longleftrightarrow 4 = (-3) \cdot 85 + 7 \cdot 37 \\ (11, 1, -2) - 2(4, -3, 7) = (3, 7, -16) &\longleftrightarrow 3 = 7 \cdot 85 + (-16) \cdot 37 \\ (4, -3, 7) - (3, 7, -16) = (1, -10, 23) &\longleftrightarrow 1 = -10 \cdot 85 + 23 \cdot 37 \end{aligned}$$

Thus Bezout's Identity for 85 and 37 is

$$1 = (-10) \cdot 85 + 23 \cdot 37.$$

*Example 3.21* Let us find  $d = (63008, 60504)$  and write  $d$  as an integer linear combination of 63008 and 60504. We start with Euclid's algorithm.

$$\begin{aligned} 63008 &= 60504 + 2504 \\ 60504 &= 24 \cdot 2504 + 408 \\ 2504 &= 6 \cdot 408 + 56 \\ 408 &= 56 + 16 \\ 56 &= 3 \cdot 16 + 8 \\ 16 &= 2 \cdot 8 + 0. \end{aligned}$$

So  $(63008, 60504) = 8$ . The corresponding sequence of vectors in the EEA (as you can check) is

$$\begin{aligned} & (63008, 1, 0) \\ & (60504, 0, 1) \\ & (63008, 1, 0) - (60504, 0, 1) = (2504, 1, -1) \\ & (60504, 0, 1) - 24(2504, 1, -1) = (408, -24, 25) \\ & (2504, 1, -1) - 6(408, -24, 25) = (56, 145, -151) \\ & (408, -24, 25) - 7(56, 145, -151) = (16, -1039, 1082) \\ & (56, 145, -151) - 3(16, -1039, 1082) = (8, 3262, -3397). \end{aligned}$$

So Bezout's Identity for 63008 and 60504 is

$$3262 \cdot 63008 - 3397 \cdot 60504 = 8.$$

As can be seen, the EEA to find Bezout's identity is as efficient as Euclid's Algorithm itself.

*Example 3.22* Find the decrypting multiplier for the multiplicative Caesar cipher modulo 37 where the multiplier is 24.

We do Euclid's algorithm with 37 and 24:

$$\begin{aligned} 37 &= 24 + 13 \\ 24 &= 13 + 11 \\ 13 &= 11 + 2 \\ 11 &= 5 \cdot 2 + 1. \end{aligned}$$

To do the EEA, we construct the sequence of EEA vectors corresponding to 37, 24 and the four remainders, 13, 11, 2 and 1.

$$\begin{aligned} & (37, 1, 0) \\ & (24, 0, 1) \\ & (37, 1, 0) - (24, 0, 1) = (13, 1, -1) \\ & (24, 0, 1) - (13, 1, -1) = (11, -1, 2) \\ & (13, 1, -1) - (11, -1, 2) = (2, 2, -3) \\ & (11, -1, 2) - 5(2, 2, -3) = (1, -11, 17). \end{aligned}$$

So  $24 \cdot 17 = 408 = 37 \cdot 11 + 1$ . Therefore,  $24 \cdot_{37} 17 = 1$ .

(For this problem we're only interested in the coefficient of 24, so we could have omitted the components that are the coefficients of 37 in the vectors.)

**EEA in Excel.** Here is how to do the vector version of the Extended Euclidean Algorithm in Excel. Given numbers  $b > a > 0$ , to write  $(b, a) = xb + ya$  for some integers  $x, y$ , start with

row #	Col. A	Col. B	Col. C
1	remainders	coeff. of $b$	coeff. of $a$
2	$b$	1	0
3	$a$	0	1

In cell A4, put

$$=A2 - \text{Int}(\$A2/\$A3)*A3.$$

Copy (Ctrl-C) the contents of cell A4.

Highlight cells B4 and C4, then paste (Ctrl-V) the contents of cell A4 in cells B4 and C4.

Highlight the first three cells of the next ten or so rows beneath row 4, and paste (Ctrl-V) the contents of cell A4.

The cells ( $A_k$ ,  $B_k$ ,  $C_k$ ) should give the successive vectors of the EEA for  $b$  and  $a$ . (If you didn't paste the contents of cell A4 into enough rows below, just paste it into some more rows.)

*Example 3.23* We find the EEA for 21 and 8:

row #	Col. A	Col. B	Col. C
1	remainders	coeff. of $b$	coeff. of $a$
2	21	1	0
3	8	0	1
4	5	1	-2
5	3	-1	3
6	2	2	-5
7	1	-3	8
8	0	8	-21
9	#DIV/0!	#DIV/0!	#DIV/0!

Then 1 is the greatest common divisor of 21 and 8, the remainders in Euclid's Algorithm are 5, 3, 2 and 1, and  $1 = 21 \cdot (-3) + 8 \cdot 8$ .

*Example 3.24* We find the EEA for 4536 and 3228:

row #	Col. A	Col. B	Col. C
1	remainders	coeff. of $b$	coeff. of $a$
2	4536	1	0
3	3228	0	1
4	1308	1	-1
5	612	-2	3
6	84	5	-7
7	24	-37	52
8	12	116	-163
9	0	-269	378
10	#DIV/0!	#DIV/0!	#DIV/0!

The remainders in Euclid's algorithm are 1308, 612, 84, 24 and 12; the greatest common divisor of 4536 and 3228 is 12, and Bezout's Identity is

$$12 = 116 \cdot 4536 - 163 \cdot 3228.$$

## 3.5 The Coprime Divisibility Lemma

Bezout's Identity has an important theoretical consequence that we will need to know in several situations.

**Lemma 3.25** (Coprime Divisibility Lemma) *For natural numbers  $a, b, c$ , if  $a$  divides  $bc$  and  $(a, b) = 1$ , then  $a$  divides  $c$ .*

*Proof* Suppose  $(a, b) = 1$ . Then by Bezout's Identity there are integers  $s, t$  so that  $1 = as + bt$ . Multiply both sides of this equation by  $c$  to get

$$c = acs + bct.$$

If  $a$  divides  $bc$ , then  $a$  divides  $acs + bct = c$ . □

*Example 3.26* We have  $17 \cdot 1666 = 28322 = 49 \cdot 578$ . Since 17 and 49 are coprime, the Coprime Divisibility Lemma implies that 17 must divide 578 and 49 must divide 1666.

In the Coprime Divisibility Lemma, Lemma 3.25, the hypothesis that  $a$  and  $b$  are coprime is important.

Some students like to believe that if  $a$  divides  $bc$  and  $a$  doesn't divide  $b$ , then  $a$  divides  $c$ . This is often false.

For example, 6 divides  $2 \cdot 3$  and 6 does not divide 2. But 6 also doesn't divide 3. The Coprime Divisibility Lemma does not apply, because 6 and 2 are not coprime.

The condition “ $a$  does not divide  $b$ ” is not the same as the condition “ $a$  and  $b$  are coprime”.

The following consequence of the Coprime Divisibility Lemma is a starting point for methods for factoring large numbers.

**Proposition 3.27** *Given a number  $m$ , suppose  $m$  divides  $a^2 - b^2$  for some numbers  $a$  and  $b$ . If  $m$  does not divide  $a + b$  and  $m$  does not divide  $a - b$ , then the greatest common divisor  $(m, a + b)$  is a non-trivial factor of  $m$ .*

*Proof* Since  $m$  divides  $a^2 - b^2$ ,  $m$  divides  $(a + b)(a - b)$ . If  $m$  does not divide  $a + b$ , then  $(m, a + b) < m$ . If  $(m, a + b) = 1$ , then by the Coprime Divisibility Lemma,  $m$  would divide  $a - b$ . So if  $m$  doesn't divide  $a - b$ , then  $1 < (m, a + b) < m$ , and so  $(m, a + b)$  must be a non-trivial factor of  $m$ . □

The Coprime Divisibility Lemma has implications for canceling in congruences. See Section 3.7, below.

## 3.6 Solutions of Linear Diophantine Equations

Given the equation  $ax + by = c$ , suppose we have found some solution  $x = x_0, y = y_0$  of the equation, so that

$$ax_0 + by_0 = c.$$

Then, setting  $d = (a, b)$ , we must have that  $d$  divides  $c$ .

Having found one solution of  $ax + by = c$ , we can find all solutions. To show how, we first observe:

**Proposition 3.28** *Let  $d$  be the greatest common divisor of  $a$  and  $b$ , and let  $a', b'$  be integers so that  $a'd = a, b'd = b$ . Then  $(a', b') = 1$ .*

*Proof* This follows from Bezout's Identity: for  $d = (a, b)$ , let  $r, s$  be integers so that  $ar + bs = d$ . Dividing both sides by  $d$  gives  $a'r + b's = 1$ . Then every common divisor of  $a'$  and  $b'$  is a divisor of the left side, hence divides 1. So the greatest common divisor of  $a'$  and  $b'$  is 1. □

Now, for  $(a, b) = d$ , look at the corresponding “homogeneous” equation

$$az + bw = 0.$$

Dividing by  $d$  gives  $a'z + b'w = 0$ , or

$$a'z = -b'w.$$

Since  $(a', b') = 1$ , the Coprime Divisibility Lemma says that  $b'$  divides  $z$ . Write  $z = b't$  for some integer  $t$ . Then substituting and canceling  $b'$  gives  $w = -a't$ . Since  $z = b't$ ,  $w = -a't$  is clearly a solution of  $az + bw = 0$  for every integer  $t$ , we conclude:

**Proposition 3.29** *If  $(a, b) = d$  and  $a'd = a$ ,  $b'd = b$ , then the integer solutions of  $az + bw = 0$  are the integers  $z = b't$ ,  $w = -a't$  for all integers  $t$ .*

(The terminology “homogeneous” is from linear algebra or differential equations: given an equation of the form  $\mathbf{Ax} = \mathbf{b}$ , the corresponding homogeneous equation is  $\mathbf{Ax} = \mathbf{0}$ .)

Having found the solutions of the corresponding homogeneous equation, we can then find every solution of the original equation  $ax + by = c$  by adding to the solution  $x = x_0$ ,  $y = y_0$  a solution of the corresponding homogeneous equation  $az + bw = 0$ :

**Corollary 3.30** *Suppose  $x = x_0$ ,  $y = y_0$  is an integer solution of the equation  $ax + by = c$ . Then  $x = x_0 + b't$ ,  $y = y_0 - a't$  is a solution of the equation for all integers  $t$ , and every solution of  $ax + by = c$  has the form  $x = x_0 + b't$ ,  $y = y_0 - a't$  for some integer  $t$ .*

*Proof* The first claim can be shown by substituting  $x = x_0 + b't$ ,  $y = y_0 - a't$  into the equation. For the second, suppose  $ax_1 + by_1 = c$  and  $ax_2 + by_2 = c$ . Then  $a(x_2 - x_1) + b(y_2 - y_1) = 0$ , so  $x_2 - x_1 = z$  and  $y_2 - y_1 = w$  satisfies  $az + bw = 0$ . So Proposition 3.29 applies.  $\square$

*Example 3.31* The equation  $36x + 21y = 12$  has a solution  $x = 5$ ,  $y = -8$ . Since  $(36, 21) = 3$ , the solutions of  $36z + 21w = 0$  are the integers  $z = 7t$ ,  $w = -12t$  for all integers  $t$ . So the solutions of the equation  $36x + 21y = 12$  are the integers  $x = 5 + 7t$ ,  $y = -8 - 12t$  for all integers  $t$ . (For example, for  $t = -1$  we get  $36x + 21y = -72 + 84 = 12$ .)

**Finding all solutions.** We summarize how to find all integer solutions of  $ax + by = c$  for  $a, b, c$  integers.

I. Find the greatest common divisor  $d = (a, b)$  of  $a$  and  $b$ . If  $d$  doesn’t divide  $c$ , there is no solution of the equation. If  $d$  does divide  $c$ , use the EEA to find  $x_0$ ,  $y_0$  so that  $ax_0 + by_0 = c$ .

II. Find all solutions  $z = b't$ ,  $w = -a't$  of the corresponding homogeneous equation  $az + bw = 0$  as in Proposition 3.29.

III. The solutions of the equation  $ax + by = c$  are then of the form

$$\begin{aligned} x &= x_0 + z = x_0 + b't, \\ y &= y_0 + w = y_0 - a't \end{aligned}$$

for all integers  $t$ .

*Example 3.32* We find all solutions of

$$42x + 30y = 96.$$

I. Do Euclid's algorithm:

$$\begin{aligned} 42 &= 30 + 12 \\ 30 &= 12 \cdot 2 + 6 \\ 12 &= 6 \cdot 2 + 0. \end{aligned}$$

So  $6 = (42, 30)$  is the greatest common divisor of 42 and 30, and the right side of the equation, 96, is divisible by 6:

$$96 = 16 \cdot 6.$$

So there are solutions of the equation.

Then do the EEA to find a solution of Bezout's Identity

$$42z + 30w = 6 :$$

$$\begin{aligned} (42, 1, 0) \\ (30, 0, 1) \\ (42, 1, 0) - (30, 0, 1) &= (12, 1, -1) \\ (30, 0, 1) - 2(12, 1, -1) &= (6, -2, 3). \end{aligned}$$

So

$$6 = 42 \cdot (-2) + 30 \cdot 3.$$

Having found a solution  $z = -2, w = 3$  of Bezout's Identity for 42 and 30, multiply the solution by 16 to get a solution of the equation  $42x + 30y = 96$ , namely  $x_0 = 16z = -32, y_0 = 16w = 48$ . We check:

$$\begin{aligned} 42x_0 + 30y_0 &= 42 \cdot (-32) + 30 \cdot 48 \\ &= -1344 + 1440 = 96. \end{aligned}$$

II. Since  $(42, 30) = 6$  and  $42 = 6 \cdot 7, 30 = 6 \cdot 5$ , the solutions of the equation

$$42z + 30w = 0$$

are the same as the solutions of the equation  $7z + 5w = 0$ , namely,  $z = 5t, w = -7t$ .

III. Then the solutions to the original equation  $42x + 30y = 96$  are

$$\begin{aligned} x &= 32 + 5t, \\ y &= 48 - 7t, \end{aligned}$$

for all integers  $t$ . In particular, the solution with the smallest positive  $x$  corresponds to  $t = 7$ : then  $x = 3, y = -1$  and

$$42 \cdot 3 + 30 \cdot (-1) = 126 - 30 = 96.$$

The solution with the smallest positive  $y$  corresponds to  $t = 6$ : then  $x = -2, y = 6$  and

$$42 \cdot (-2) + 30 \cdot 6 = -84 + 180 = 96.$$

## 3.7 Manipulating and Solving Linear Congruences

To solve  $ax \equiv b \pmod{m}$ , we can solve

$$ax + my = b.$$

For this equation, if  $(a, m)$  does not divide  $b$ , there is no solution. But if  $(a, m) = d$  does divide  $b$ , then we can find a solution  $x = x_0, y = y_0$  by the EEA, as above. Then the integer solutions for  $x$  in the equation  $ax + my = b$  are the integer solutions for  $x$  in the congruence  $ax \equiv b \pmod{m}$ .

But we can also try working directly with congruences. To do so, knowing when we can cancel common factors from a congruence is critical. We have

**Proposition 3.33** *If  $ab \equiv ac \pmod{m}$  and  $(a, m) = 1$ , then  $b \equiv c \pmod{m}$ . That is, we can cancel the factor  $a$  in the congruence if  $a$  and  $m$  are coprime.*

*Proof* The congruence implies that  $m$  divides  $ab - ac = a(b - c)$ . Since  $a$  and  $m$  are coprime, the Coprime Divisibility Lemma tells us that  $m$  divides  $b - c$ . So  $b \equiv c \pmod{m}$ .  $\square$

Proposition 3.33 implies that if we are trying to solve a congruence

$$ax \equiv b \pmod{m},$$

and  $f$  is an integer coprime to  $m$ , then we can multiply both sides of the congruence by  $f$ , and the solutions of the congruence won't change. For if  $(f, m) = 1$ , then canceling  $f$  is a reversible action to multiplying by  $f$ .

On the other hand, if  $ab \equiv ac \pmod{m}$  and  $(a, m) > 1$ , then we cannot cancel  $a$  and expect to get a correct congruence. For example,

$$33 \equiv 3 \pmod{6}.$$

If we cancel the 3 from both sides we get

$$11 \equiv 1 \pmod{6},$$

which is false.

A consequence of this is that if you wish to solve a linear congruence

$$ax \equiv b \pmod{m},$$

and proceed by multiplying both sides by a number not coprime to  $m$ , you will end up with a congruence that can have more solutions than the original one did, because the multiplication is not reversible by cancellation.

*Example 3.34* The congruence

$$25x \equiv 10 \pmod{30}$$

has solutions  $x \equiv -2 \pmod{6}$ . But if we multiply both sides by 2 to get

$$50x \equiv 20 \pmod{30},$$

we also get the solution  $x = 1$ , which is not a solution of the original congruence.

The congruence

$$3x \equiv 1 \pmod{6}$$

has no solutions, but multiplying both sides by 3 gives

$$9x \equiv 3 \pmod{6},$$

which has the solution  $x = 1$ .

See Exercise 3.17 for more examples.

Given some integer  $x_0$  so that  $ax_0 \equiv b \pmod{m}$ , all solutions in  $\mathbb{Z}$  of the congruence  $ax \equiv b \pmod{m}$  have the form  $x = x_0 + z$ , where  $z$  satisfies the homogeneous congruence  $az \equiv 0 \pmod{m}$ .

**Proposition 3.35** *Given integers  $a$  and  $m$ , let  $(a, m) = d$  and let  $dm' = m$ . Then the integer solutions of the congruence*

$$az \equiv 0 \pmod{m}$$

*have the form  $z = m't$  for all integers  $t$ .*

*Proof* Let  $a'd = a$ . Then from Proposition 3.38

$$az \equiv 0 \pmod{m}$$

if and only if

$$a'z \equiv 0 \pmod{m'}.$$

Since  $(a', m') = 1$  (Proposition 3.28), we can cancel  $a'$  from both sides (Proposition 3.33) to get

$$z \equiv 0 \pmod{m'}.$$

So  $z$  is a multiple of  $m' = m/(a, m)$ . □

**Corollary 3.36** *Suppose  $x_0$  is a solution of the congruence  $ax \equiv b \pmod{m}$ . Then the set of all solutions of  $ax \equiv b \pmod{m}$  is the same as the set of all solutions modulo  $m$  of the congruence*

$$x \equiv x_0 \pmod{m/(a, m)}.$$

*Example 3.37* Consider the congruence

$$35x \equiv 49 \pmod{56}.$$

Since  $(35, 56) = 7$  divides 49, this congruence has the same solutions as

$$5x \equiv 7 \pmod{8}.$$

The inverse of 5 modulo 8 is 5, so multiplying this last congruence by 5 yields

$$5 \cdot 5x \equiv 7 \cdot 5 \pmod{8},$$

or

$$x \equiv 3 \pmod{8}.$$

So the solutions modulo 56 of the original congruence  $35x \equiv 49 \pmod{56}$  are the integers modulo 56 of the form  $x = 3 + 8t$  for all integers  $t$ . The seven distinct solutions modulo 56 are  $x = 3 + 8t$  for  $t = 0, 1, 2, 3, 4, 5, 6$ .

So the solutions of the original congruence modulo 56 are

$$x = 3, 11, 19, 27, 35, 43 \text{ and } 51 \pmod{56}.$$

The most general rule about canceling in congruences is:

**Proposition 3.38** *Given a congruence*

$$ax \equiv b \pmod{m},$$

let  $e$  be a common divisor of  $a, b$  and  $m$ , and let  $a'e = a, b'e = b, m'e = m$ . Then

$$a'x \equiv b' \pmod{m'}.$$

In words, you can cancel a common factor from the modulus and both sides of the congruence.

*Proof* Just write the first congruence as

$$ax = b + mt$$

and cancel  $e$  from both sides to get

$$a'x = b' + m't,$$

which yields the second congruence. □

For example, given the congruence

$$25x \equiv 10 \pmod{30},$$

when we cancel 5 to get

$$5x \equiv 2 \pmod{6},$$

both congruences have the same solutions in  $\mathbb{Z}$ . To find all solutions of the congruence modulo 30, we find all solutions in  $\mathbb{Z}$  of the second congruence, namely,  $x = 4 + 6t$  for all  $t$  in  $\mathbb{Z}$ , and then find all of these solutions that are distinct modulo 30, namely,  $x = 4 + 6t$  for  $t = 0, 1, 2, 3, 4$ .

## Exercises

- 3.1. Find a criterion involving the decimal digits of a number  $b$  for deciding whether or not  $b$  is divisible by
  - (i) 5; (ii) 20; (iii) 11.
- 3.2. (i) Show that  $10^n \equiv 1 \pmod{9}$  for all  $n \geq 1$ .  
 (ii) Show that if

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0,$$

then

$$a \equiv a_n + a_{n-1} + \dots + a_1 + a_0 \pmod{9}.$$

- 3.3. Among the numbers 1, 2, … 9, list those that are coprime to 10, and list those that are not coprime to 10. Then compare your lists with the lists of units and zero divisors of  $\mathbb{Z}_{10}$ .
- 3.4. Explain why every common divisor of 72 and 200 also divides 56.
- 3.5. Prove Proposition 3.2.
- 3.6. Find the greatest common divisor of 668 and 156 using Euclid's Algorithm.
- 3.7. Find the greatest common divisor of 216 and 300 in two ways:  
 (i) List the eighteen divisors of 300 and the sixteen divisors of 216, and compare the list;  
 (ii) Use Euclid's Algorithm.  
 Which method was faster?
- 3.8. Find the greatest common divisor of 1961 and 2279.
- 3.9. For 41 and 15, write down Euclid's algorithm to find the greatest common divisor (= 1). Then write down the EEA vector corresponding to each non-zero remainder. For each EEA vector  $(r, s, t)$  that you found, verify that  $r = 41s + 15t$ .
- 3.10. Find Euclid's algorithm, the greatest common divisor, the sequence of EEA vectors and Bezout's Identity for each of the following pairs of numbers:  
 (i) 86 and 37  
 (ii) 111 and 81  
 (iii) 22911 and 9856.
- 3.11. Find the smallest number  $x > 0$  so that  
 (i)  $81 \cdot_{111} x = 1$ ;  
 (ii)  $132 \cdot_{257} x = 1$ .
- 3.12. Find an integer solution, if any, of  
 (i)  $45x + 35y = 10$   
 (ii)  $85x + 37y = 12$ .
- 3.13. Decide for each equation whether or not the equation has an integer solution. If so, find one:  
 (i)  $221x + 143y = 176$   
 (ii)  $221x + 143y = 182$ .
- 3.14. Find all integer solutions of  
 $196x + 182y = 56$ .
- 3.15. For each composite number  $m$ , explain why there are numbers  $b$  and  $c$  so that  $m$  divides  $bc$  but  $m$  does not divide  $b$  and  $m$  does not divide  $c$ .
- 3.16. For each composite number  $m$ , explain why there are numbers  $a, b$  and  $c$  so that

$$ab \equiv ac \pmod{m}$$

but  $b \not\equiv c \pmod{m}$ .

- 3.17. Suppose  $(a, m) = 1$  and  $(s, m) = d$ . Show that the congruence

$$asx \equiv bs \pmod{m}$$

has  $d$  solutions modulo  $m$ .

- 3.18. Find all solutions of  
 (i)  $35x \equiv 25 \pmod{65}$ ;  
 (ii)  $8x \equiv 22 \pmod{30}$ .
- 3.19. Find all solutions of  
 (i)  $221x = 0 \pmod{260}$   
 (ii)  $221x = 299 \pmod{260}$ .
- 3.20. (i) Using  $\mathbb{Z}_{27}$  for multiplicative Caesar ciphers, write down the eighteen possible pairs  $(e, d)$  with  $1 \leq e < 27$ ,  $1 \leq d < 27$  where  $e$  is an encrypting multiplier and  $d$  is the corresponding decrypting multiplier.  
 (ii) Design a Vigenère cryptosystem (Chapter 1) using a multiplicative (not additive) Caesar cipher in  $\mathbb{Z}_{27}$  on each letter, where the key for each letter comes from an easily remembered piece of English text  $\kappa$  of at least six letters. (Note that the letters of the encrypting key text should have corresponding numbers that are possible encrypting multipliers! So  $\kappa = ENCRYPT$ , or  $(5, 14, 3, 18, 25, 16, 20)$ , doesn't work because  $(3, 27) > 1$ .)  
 (iii) Act like the receiver, and find the decrypting key text corresponding to your encrypting key text  $\kappa$ .
- 3.21. The Japanese Katakana alphabet has 71 characters. If we use  $\mathbb{Z}_{72}$  to encrypt a message in Katakana by a multiplicative Caesar cipher, how many encrypting multipliers are available to use?

The next four exercises relate to the speed of Euclid's Algorithm, and refer to the Fibonacci sequence

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \dots$$

The Fibonacci sequence is defined by  $a_1 = 1$ ,  $a_2 = 1$ ,  $a_3 = 2$ , and for all  $n \geq 1$ ,  $a_{n+1} = a_n + a_{n-1}$ .

- 3.22. (i) Show that Euclid's algorithm for  $a_5 = 5$  and  $a_4 = 3$  has two non-zero remainders.  
 (ii) How many non-zero remainders appear in Euclid's algorithm for  $a_{n+1}$  and  $a_n$ ?  
 (iii) Using Euclid's algorithm, show that consecutive Fibonacci numbers are coprime (that is,  $(a_n, a_{n+1}) = 1$  for all  $n \geq 0$ ). If you know how to write a proof by induction, write one for this exercise.
- 3.23. It is a fact, due to the 19th century mathematician Lamé, that Euclid's algorithm on  $a_n$  and  $a_{n+1}$  requires more divisions than it does on every pair  $(a, b)$  with  $a < b$  and  $a < a_n$ . Verify this fact for numbers  $a < b$  where  $a < 8 = a_6$ .
- 3.24. Show that  $a_{n+5} \geq 10a_n$  for all  $n \geq 5$ .
- 3.25. Use the information in the last two exercises to find an upper bound on the number of divisions needed for Euclid's algorithm for  $a$  and  $b > a$ , where  $a$  has  $d$  digits. (This exercise implies that finding the greatest common divisor of two 200 digit numbers can be done almost instantly on an ordinary PC. But we'll see that trying to factor a 200-digit number could take many hours using many computers.)

# Chapter 4

## Unique Factorization in $\mathbb{Z}$



From looking at the cryptographic examples of Chapters 1 and 2, it is evident that a very good understanding of the natural numbers and integers is useful for understanding cryptology. In fact, the cryptography presented in Chapters 9 and 16 is entirely based on the facts that, (1) there is a unique way to factor a number into a product of prime numbers, and, (2) in practice actually finding the factorization can be a hard problem. So in this chapter we prove uniqueness of factorization of numbers into products of primes. We also show how uniqueness of factorization relates to the greatest common divisor of two numbers.

The proof of uniqueness of factorization uses induction. So we devote some space to two versions of induction. Induction is part of the knowledge base of every mathematician.

One version of induction, the well-ordering principle, is useful both for proving facts about natural numbers and in telling us that certain numbers exist. For example, well-ordering implies the existence of the least common multiple of two numbers. It yields a new proof of Bezout's Identity. And in Chapter 8 well-ordering will be used to define the *order* of an invertible element of  $\mathbb{Z}_m$ , a concept that we will use throughout the rest of the book.

Most of the mathematics we've seen so far depends on the Division Theorem. So this chapter also includes in Section 4.4 the promised proof of that fundamental fact.

### 4.1 Unique Factorization into Products of Prime Numbers

The theorem that every natural number  $> 1$  factors uniquely into a product of prime numbers is called the Fundamental Theorem of Arithmetic. In this section we state the Fundamental Theorem, and apply it to understand divisibility, the greatest common divisor and the least common multiple.

We start with prime numbers.

**Definition** A number  $p > 1$  is a *prime number*, or for short, *prime*, if the only positive divisors of  $p$  are 1 and  $p$  itself. A number  $m > 1$  is *composite* if  $m$  is not prime.

Note that the number 1 is not prime, and not composite. (That's because 1 is the identity element of  $\mathbb{Z}$ : 1 is the only natural number that is a factor of every integer.)

*Example 4.1* Among the numbers  $n$  with  $1 < n \leq 50$ , the numbers 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 and 47 are prime. The others factor into a product of two or more primes. For example,

$$\begin{aligned}4 &= 2 \cdot 2 \\6 &= 2 \cdot 3 \\8 &= 2 \cdot 2 \cdot 2 \\10 &= 2 \cdot 5 \\12 &= 2 \cdot 2 \cdot 3 \\14 &= 2 \cdot 7 \\15 &= 3 \cdot 5 \\16 &= 2 \cdot 2 \cdot 2 \cdot 2 \\18 &= 2 \cdot 3 \cdot 3 \\20 &= 2 \cdot 2 \cdot 5.\end{aligned}$$

Here is the Fundamental Theorem:

**Theorem 4.2** *Let  $m$  be a number  $> 1$ . Then  $m$  factors into a product of prime numbers. If*

$$m = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t,$$

*where  $p_1, \dots, p_s$  and  $q_1, \dots, q_t$  are all primes, then  $s = t$  and the primes  $p_1, \dots, p_s$  and  $q_1, \dots, q_t$  are the same (only the order in which the primes are written down in the two factorizations might vary).*

The fact that every number factors into a product of primes, and that the factorization is unique, has been known for 2300 years.

To illustrate what is meant by the uniqueness of factorization, consider  $m = 60$ . We can write

$$60 = 2 \cdot 2 \cdot 3 \cdot 5 = 3 \cdot 5 \cdot 2 \cdot 2 = 5 \cdot 2 \cdot 3 \cdot 2.$$

but they are not different factorizations: each prime dividing 60 occurs the same number of times in each factorization. Only the order of the factors is different. And the order doesn't matter.

We'll prove the Fundamental Theorem later in this chapter. Here we will use the uniqueness of factorization to reinterpret divisibility and greatest common divisors, and to introduce the least common multiple.

**Exponential Notation.** In writing the prime factorization of a number  $a$ , it is convenient to arrange the prime factors in increasing order and use exponential notation. For example, 1050 factors as

$$1050 = 105 \cdot 10 = 3 \cdot 5 \cdot 2 \cdot 5.$$

We'll arrange the factorization as

$$1050 = 2 \cdot 3 \cdot 5^2 \cdot 7.$$

Similarly, we can write

$$720 = 2^4 \cdot 3^2 \cdot 5 \cdot 7^0.$$

The factorization of 720 illustrates that we can include in the factorization primes that do not actually divide the number  $a$ , as long as we give them the exponent zero.

In general, if the number  $a$  is divisible only by primes included in the list  $p_1, p_2, \dots, p_r$ , we can write the number  $a$  as

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

for some exponents  $e_1, \dots, e_r \geq 0$ . Uniqueness of factorization says that the exponents of the primes dividing a number are unique.

**Divisibility.** We can use exponential notation to describe when a number  $a$  divides a number  $b$ :

Suppose

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

and

$$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$$

where the list of primes  $p_1, \dots, p_r$  includes all primes that divide either  $a$  or  $b$ , and some of the exponents  $e_i$  or  $f_i$  may be zero.

**Proposition 4.3** *With  $a, b$  as above,  $a$  divides  $b$  if and only if  $e_i \leq f_i$  for all  $i = 1, \dots, r$ .*

*Example 4.4* The number 810 divides 87480. This can be seen because

$$810 = 2 \cdot 3^4 \cdot 5,$$

while

$$87480 = 2^3 \cdot 3^7 \cdot 5.$$

In fact,  $87480 = 810 \cdot q$  where

$$q = 2^2 \cdot 3^3 = 108.$$

On the other hand,

$$4050 = 2 \cdot 3^4 \cdot 5^2$$

does not divide 87480 because  $5^2 = 25$  divides 4050 but does not divide 87480.

*Proof* Given the factorizations of  $a$  and  $b$ , above, suppose  $a$  divides  $b$ , so that  $b = aq$  for some natural number  $q$ . Then every prime that divides  $q$  also divides  $b$ , so we can write  $q$  as a product

$$q = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$$

where  $c_i \geq 0$  for  $i = 1, \dots, r$ . In the equation  $aq = b$ , if we substitute the prime factorizations for  $a$ ,  $q$  and  $b$  and collect exponents of each prime on the left side, we find that

$$aq = p_1^{e_1+c_1} p_2^{e_2+c_2} \cdots p_r^{e_r+c_r}.$$

Since  $aq = b$  and

$$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r},$$

uniqueness of factorization implies that  $e_i + c_i = f_i$  for each  $i$ . Since all  $c_i \geq 0$ , we have  $e_i \leq f_i$ .

Conversely, for all  $i = 1, \dots, r$  we have  $e_i \leq f_i$ , let  $c_i = f_i - e_i$ . Then  $c_i \geq 0$  and so

$$q = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$$

is a natural number, and the prime factorizations of  $b$  and of  $aq$  are the same. So  $b = aq$ , and  $a$  divides  $b$ .  $\square$

This result yields a description of the greatest common divisor of two numbers.

**Corollary 4.5** *In the prime factorization of the greatest common divisor  $d$  of two numbers  $a$  and  $b$ , the exponent of each prime  $p$  in the factorization of  $d$  is the smaller of the exponents of  $p$  in  $a$  and in  $b$ .*

If  $e$  is a common divisor of  $a$  and  $b$ , then for each prime  $p$  dividing  $e$ , the exponent of  $p$  in  $e$  must be  $\leq$  the exponent of  $p$  in  $a$ , and also  $\leq$  the exponent of  $p$  in  $b$ . If  $d$  is the greatest common divisor, then the exponent of  $p$  in  $d$  must be as large as possible, hence must equal the smaller of the exponents of  $p$  in  $a$  and in  $b$ .

To restate the description of the greatest common divisor of two numbers, we introduce the notation  $p^e \parallel a$  to mean that  $p^e$  is the exact power of  $p$  in the prime factorization of  $a$ . Thus,  $p^e \parallel a$  if  $p^e$  divides  $a$  but  $p^{e+1}$  does not.

For example,  $2^3 \parallel 87480$ , because  $87480 = 8 \cdot 10935$  and 2 does not divide 10935.

Using this notation, we have:

- $a$  divides  $b$  if and only if for every prime  $p$ , if  $p^e \parallel a$  and  $p^f \parallel b$ , then  $e \leq f$ .
- Given numbers  $a$  and  $b$ , the greatest common divisor  $(a, b)$  has the property that for every prime  $p$ , if  $p^e \parallel a$  and  $p^f \parallel b$ , then  $p^{\min\{e, f\}} \parallel (a, b)$ . Here,  $\min\{e, f\}$  denotes the smaller of  $e$  and  $f$ .

*Example 4.6* We have

$$87480 = 2^3 \cdot 3^7 \cdot 5 \cdot 7^0, \quad 28350 = 2 \cdot 3^4 \cdot 5^2 \cdot 7.$$

So

$$(87480, 4050) = 2 \cdot 3^4 \cdot 5 \cdot 7^0 = 810$$

because  $\min\{3, 1\} = 1$ ,  $\min\{7, 4\} = 4$ ,  $\min\{1, 2\} = 1$  and  $\min\{0, 1\} = 0$ .

**The Least Common Multiple.** A common multiple of two natural numbers  $a, b$  is a number  $m > 0$  so that  $a$  divides  $m$  and  $b$  divides  $m$ . Every pair of numbers  $a$  and  $b$  has some common multiple, namely their product,  $ab$ . The *least common multiple* of  $a$  and  $b$  is the smallest number that is a common multiple of  $a$  and  $b$ . In Section 4.4 we'll see why the least common multiple of  $a$  and  $b$  always exists.

We denote the least common multiple of  $a$  and  $b$  by  $[a, b]$ .

*Example 4.7*  $[4, 10] = 20$ . Why? One way to see that is to first observe that  $4 \cdot 10 = 40$  is a common multiple of 4 and 10. So the least common multiple is  $\leq 40$ . To find it, we can just look at multiples of 10 that are  $\leq 40$ : 10, 20, 30, 40, and take the smallest one that is a multiple of 4.

Other examples:  $[35, 20] = 140$ ,  $[77, 91] = 1001$ . Particularly easy is the case where  $a$  divides  $b$ : then  $[a, b] = b$ . For example,  $[9, 18] = 18$ , and  $[91, 1001] = 1001$ .

You may have learned about the least common multiple of two numbers  $a$  and  $b$  when learning how to add fractions. Suppose you wish to add  $1/6$  and  $1/8$ . To do so, you need to find a common denominator. The least common multiple of the denominators is the same as the least common denominator of the two fractions.

In this example, the least common denominator is  $24 = [6, 8]$ , and

$$\frac{1}{6} + \frac{1}{8} = \frac{4}{24} + \frac{3}{24} = \frac{4+3}{24} = \frac{7}{24}.$$

As with the greatest common divisor, we can find the least common multiple of two numbers if we know the prime factorizations of the two numbers.

**Proposition 4.8** *Given two numbers  $a$  and  $b$ , with prime factorizations*

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

and

$$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}.$$

*Then the least common multiple of  $a$  and  $b$  has prime factorization:*

$$[a, b] = p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \cdots p_r^{\max\{e_r, f_r\}}.$$

*In words, for every prime  $p$  dividing  $a$  or  $b$ , if  $p^e \parallel a$  and  $p^f \parallel b$ , then the exponent of  $p$  in the prime factorization of the least common multiple  $[a, b]$  is the larger of  $e$  and  $f$ .*

**Example 4.9** Consider

$$1001 = 7 \cdot 11 \cdot 13 = 3^0 \cdot 7^1 \cdot 11^1 \cdot 13^1$$

$$1617 = 3 \cdot 7 \cdot 7 \cdot 11 = 3^1 \cdot 7^2 \cdot 11^1 \cdot 13^0.$$

Then the least common multiple

$$[1001, 1617] = 3^1 \cdot 7^2 \cdot 11^1 \cdot 13^1 = 21021.$$

Writing the least common multiple and greatest common divisor in terms of prime factorizations yields a useful description of the least common multiple:

**Proposition 4.10** *The least common multiple of  $a$  and  $b$  is the product  $ab$  divided by their greatest common divisor. In symbols:*

$$[a, b] = \frac{ab}{(a, b)}.$$

*Proof* Let  $p$  be a prime number that divides  $a$  or  $b$ . Let  $p^e \parallel a$ ,  $p^f \parallel b$ . Then by Proposition 4.8, we have

$$p^{\max\{e, f\}} \parallel [a, b] \text{ and } p^{\min\{e, f\}} \parallel (a, b).$$

The formula  $[a, b](a, b) = ab$  then follows from the easily verified relation

$$e + f = \max\{e, f\} + \min\{e, f\}.$$

□

Exercise 4.14 gives a prime-free proof of Proposition 4.10.

Why is this proposition useful? Think about it for a minute.

**Example 4.11** It is easy to check that  $(350, 600) = 50$ . So by Proposition 4.10, their least common multiple is

$$[350, 600] = 350 \cdot 600 / 50 = 4200.$$

We saw earlier that  $(87480, 4050) = 810$ . So

$$[87480, 4050] = 87480 \cdot 4050 / 810 = 437400.$$

A useful property of the least common multiple and the greatest common divisor:

**Proposition 4.12** (i) *The least common multiple of  $a$  and  $b$  divides every common multiple of  $a$  and  $b$ .*  
(ii) *Every common divisor of  $a$  and  $b$  divides the greatest common divisor of  $a$  and  $b$ .*

*Proof* (i) This can be seen using the idea that if  $n$  is a common multiple of  $a$  and  $b$ , then for every prime  $p$ , if  $p^r \parallel a$  and  $p^s \parallel b$ , then  $p^t$  divides  $n$  where  $t = \max\{r, s\}$ . So  $[a, b]$  divides  $n$ .

But we can also show (i) without looking at prime factors:

Let  $m$  be the least common multiple of  $a$  and  $b$ , and suppose  $n > 0$  is any common multiple of  $a$  and  $b$ . Write  $n = mq + r$  with  $0 \leq r < m$ , using the division theorem.

Since  $a$  divides  $m$  and  $a$  divides  $n$ , then  $a$  divides  $n - mq = r$ .

Since  $b$  divides  $m$  and  $b$  divides  $n$ , then  $b$  divides  $n - mq = r$ .

Thus  $r$  is a common multiple of  $a$  and  $b$ . But  $m$  is the least positive integer that is a common multiple of  $a$  and  $b$ , and  $r < m$ . Thus  $r$  must be 0. That means,  $m$  divides  $n$ .

The proof of (ii) is left as Exercise 4.6. [Use Bezout's identity.]  $\square$

Returning to the question: why is Proposition 4.10 useful?

The formula  $[a, b] = ab/(a, b)$  has the great virtue that we don't need to be able to factor  $a$  and  $b$  to find  $[a, b]$ —we just need to find the greatest common divisor  $(a, b)$ . (For example, we didn't need the prime factorizations of 87480 and 4050 to find their least common multiple.) And to find the greatest common divisor, we can use Euclid's Algorithm. That fact is very helpful in practice, because Euclid's algorithm is “lightning fast” compared to algorithms for factoring numbers into products of primes. [See the Fibonacci exercises in Chapters 3 and 17.]

*Example 4.13* Suppose we want to find  $[1794899, 1792471]$ .

First find  $(1794899, 1792471)$  by Euclid's algorithm:

$$\begin{aligned} 1794899 &= 1792471 + 2428 \\ 1792471 &= 2428 \cdot 738 + 607 \\ 2428 &= 607 \cdot 4 + 0. \end{aligned}$$

So  $(1794899, 1792471) = 607$ . Then

$$[1794899, 1792471] = (1794899 \cdot 1792471)/607 = 5300336747.$$

It would take a bit longer to discover the prime factorizations  $1794899 = 607 \cdot 2957$  and  $1792471 = 607 \cdot 2953$  of the two numbers.

## 4.2 Induction

To prove that every number factors uniquely into a product of primes, we need to use proof by induction.

Induction in its various forms is an essential tool for proving statements about natural numbers. It is a way of coping with the fact that the set of natural numbers is an infinite set. Thus, for example, the fact that we can explicitly factor every number  $< 1000$  into a product of prime numbers may give us confidence that every number can be factored into primes. But we can never prove that fact by looking at examples, because the number of examples is infinite.

Hopefully you have seen some form of induction already. The idea goes back to Euclid.

For us the most useful form of induction is the following:

**Definition (Complete Induction)** Let  $n_0$  be a fixed integer and let  $P(n)$  be a statement which makes sense for every integer  $n \geq n_0$ . Then  $P(n)$  is true for all integers  $n > n_0$ , if the following two statements are true:

- (a) (*base case*)  $P(n_0)$  is true, and
- (b) (*induction step*) For every  $m > n_0$ :  
if  $P(k)$  is true for all  $k$  with  $n_0 \leq k < m$ , then  $P(m)$  is true.

Let's use induction to prove:

**Theorem 4.14** *Every natural number  $n \geq 2$  is divisible by a prime.*

Every carefully written induction proof begins by identifying precisely what we want to prove about a given natural number. In this case we write the statement:

$P(n)$ : the number  $n$  is divisible by a prime number.

We want to prove that  $P(n)$  is true for every number  $n \geq 2$ .

It's easy to see that  $P(n)$  is true for small values of  $n$ . Some examples:

$P(2)$ : 2 is divisible by a prime. This is true because 2 is prime and 2 divides itself:  $2 = 2 \cdot 1$ .

$P(3)$ : 3 is divisible by a prime. This is true because 3 is prime and 3 divides itself:  $3 = 3 \cdot 1$ .

$P(4)$ : 4 is divisible by a prime. This is true because the prime 2 divides 4:  $4 = 2 \cdot 2$ .

$P(143)$ : 143 is divisible by a prime. This is true because 11 is prime and 11 divides 143:  $143 = 11 \cdot 13$ .

For every particular number  $n$ , we could try to show that  $n$  is divisible by a prime. But for large numbers  $n$ , it is often difficult to find a prime factor of  $n$ , and much worse, there are infinitely many numbers, and looking at them one at a time, we would never finish the proof.

Induction is a way around this problem.

An induction proof has two parts, a base case and an induction step. Here's how they work for this theorem.

*Proof Base case.*  $P(2)$  is true. We observed that already: it follows because 2 is prime and divides itself.

*Induction step.* For every number  $m > 2$ , we want to show that  $P(m)$  is true. We can assume that for every number  $k \geq 2$  where  $k$  is less than  $m$ , then  $P(k)$  is true.

More explicitly, we want to show that for a number  $m$ , if every number  $k > 1$  with  $k$  less than  $m$  is divisible by a prime number, then  $m$  itself is divisible by a prime number.

There are two cases.

If  $m$  is prime, then  $m$  is divisible by itself, so  $P(m)$  is true.

If  $m$  is not prime, then  $m = ab$  for some numbers  $a$  and  $b$  where  $a > 1$  and  $b > 1$ , and hence  $a = m/b < m$  and  $b = m/a < m$ . We've assumed that  $P(k)$  is true for all  $k$  with  $2 \leq k < m$ . So in particular,  $P(a)$  is true. So some prime  $p$  divides  $a$ : there is some integer  $c$  so that  $a = pc$ . Then  $m = ab$  and  $a = pc$ , so  $m = pbc$ . So  $m$  is divisible by the prime  $p$  that divides  $a$ . So  $P(m)$  is true.

A number  $m$  is either prime or not prime. We've dealt with both possibilities and found that in both cases,  $m$  is divisible by a prime.

So we've completed the induction step.

By complete induction, we conclude that  $P(n)$  is true for all numbers  $n \geq 2$ . The proof is complete.  $\square$

By the same argument, we can show part of the Fundamental Theorem:

**Theorem 4.15** *Every natural number  $n \geq 2$  is prime or factors into a product of primes.*

*Example 4.16* To illustrate what the proof generalizes, suppose we want to show that 1287 is prime or factors into a product of primes.

Suppose we know how to factor every number  $< 1287$  into a product of primes.

We look at 1287. Either 1287 is prime, or it's not prime. (We can try to decide which by the slow but simple algorithm: divide 1287 by every number  $d$  with  $2 \leq d \leq \sqrt{1287} = 35.8$ . In general, if a number  $n$  is not divisible by a number  $\leq \sqrt{n}$ , then it must be prime (See Exercise 4.17)).

If 1287 can't be factored into a product of smaller numbers, then 1287 must be prime.

If 1287 can be factored,  $1287 = ab$  where  $a$  and  $b$  are  $< 1287$ . We've assumed that  $a$  is a product of (one or more) primes, and also  $b$ . Then the product of the prime factorization of  $a$  and the prime factorization of  $b$  is a prime factorization of 1287.

Therefore, we know that 1287 factors into a product of primes.

In the case of 1287, I can easily find its prime factorization. I notice that 1287 is a multiple of 9. So we can write  $1287 = 9 \cdot 143$ . We then factor those two numbers:  $9 = 3 \cdot 3$  and  $143 = 13 \cdot 11$ . So

$$1287 = 9 \cdot 143 = (3 \cdot 3) \cdot (13 \cdot 11),$$

is a product of primes.

But I don't need to actually know *what is* the factorization of 1287 into a product of primes to know that *there is* a factorization of 1287 into a product of primes. We'll see later that the difficulty of factoring is at the heart of security for some modern cryptosystems.

The proof of Theorem 4.15 abstracts the example, and the form of the proof is identical to the proof of Theorem 4.14. In the proof we don't actually need to decide whether or not  $m$  is prime; we just know that either  $m$  is prime or it is not, and we can prove the theorem in either case.

We leave the proof by induction of Theorem 4.15 as Exercise 4.16.

### 4.3 The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic says that every natural number is prime or factors uniquely into a product of prime numbers. In this section we give a proof.

In this theorem we'll use the convention that a product of primes may consist of only one factor. So  $5 = 5$  is a factorization of 5 into prime numbers. With that convention, we can state the Fundamental Theorem as

**Theorem 4.17** (Fundamental Theorem of Arithmetic) *Every natural number  $n \geq 2$  factors uniquely into a product of primes.*

Theorem 4.15 says that there is a factorization. Here we prove uniqueness.

Before we get into the proof, we recall the Coprime Divisibility Lemma from the last chapter.

**Lemma 4.18** *For numbers  $a, b, c$ , if  $a$  divides  $bc$  and  $(a, b) = 1$ , then  $a$  divides  $c$ .*

We proved this using Bezout's identity.

**Corollary 4.19** *If  $p$  is a prime number and  $p$  divides  $bc$ , then  $p$  divides  $b$  or  $p$  divides  $c$ .*

*Proof* Suppose  $p$  divides  $bc$ . If  $p$  divides  $b$ , we're done. If  $p$  doesn't divide  $b$  then, since  $p$  is prime,  $(p, b) = 1$ . So  $p$  divides  $c$  by the Coprime Divisibility Lemma.  $\square$

It follows that if a prime  $p$  divides a product  $a_1 a_2 \cdots a_s$ , then  $p$  must divide one of the factors: write the product as  $(a_1 a_2 \cdots a_{s-1}) \cdot a_s$  and apply Corollary 4.19. If  $p$  divides  $a_s$ , we're done; if  $p$  divides  $a_1 a_2 \cdots a_{s-1}$ , repeat the argument, now with fewer factors in the product. After at most  $s - 1$  repetitions, we will have shown that  $p$  divides one of the factors.

We leave as Exercise 4.18 the problem of turning the argument in the last paragraph into a proper induction argument!

Now we can prove Theorem 4.17.

*Proof* We use complete induction. The statements we want to prove for all  $n \geq 2$  are:

$P(n)$  = “ $n$  factors uniquely into a product of primes”.

Suppose  $n \geq 2$ . To show that  $P(n)$  is true, we suppose that  $n$  has two factorizations into products of primes,  $n = p_1 \dots p_r$  and also  $n = q_1 \dots q_s$ . We want to show that the two factorizations are the same.

We first observe that if  $n = p$  is prime and also  $n = q_1 \dots q_s$ , then  $s = 1$  and  $p = q_1$ , because by definition a prime cannot factor into a product of two or more primes. So  $P(n)$  is true if  $n$  is prime. In particular it is true for  $n = 2$ , because 2 is a prime number. So  $P(2)$  is true. That completes the base case.

For the induction step, suppose that  $P(a)$  is true for all numbers  $a$  with  $2 \leq a < n$ . If  $n$  is prime, then  $P(n)$  is true, as we just observed. So assume that  $n$  is not prime. Then we have two factorizations

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

where both  $r$  and  $s$  are  $> 1$ . By the discussion below Corollary 4.19, the prime  $p_1$  must divide one of  $q_1, \dots, q_s$ . By reordering and renumbering the  $q_i$ , we can assume  $p_1$  divides  $q_1$ . Since  $p_1$  and  $q_1$  are primes and one divides the other, they are equal:  $p_1 = q_1$ .

Then dividing  $n$  by  $p_1$  gives us a natural number  $a = n/p_1 = n/q_1$  which is  $\geq 2$  and, of course,  $< n$  because a prime number is  $> 1$ .

We then have two factorizations of  $a$ , namely:

$$a = \frac{n}{p_1} = p_2 \cdot \dots \cdot p_r$$

and

$$a = \frac{n}{q_1} = q_2 \cdot \dots \cdot q_s.$$

Since  $2 \leq a < n$ , the induction assumption implies that  $P(a)$  is true: the two factorizations of  $a$  are the same. That is, the set of primes  $\{p_2, \dots, p_r\}$  is the same as the set of primes  $\{q_2, \dots, q_s\}$ . But since  $p_1 = q_1$ , the set of primes

$$\{p_1, p_2, \dots, p_r\}$$

is then the same as the set of primes

$$\{q_1, q_2, \dots, q_s\}.$$

These are the sets of primes in the two factorizations of  $n$ . So the two factorizations of  $n$  are the same. Thus  $P(n)$  is true. The theorem is true by complete induction.  $\square$

A note on the proof. The uniqueness really needs Corollary 4.19, and, in particular, the Coprime Divisibility Lemma. Corollary 4.19 is a consequence of Bezout's Identity, which we proved by Euclid's Algorithm and will prove again below using Well-Ordering. So the Fundamental Theorem of Arithmetic is really a special result. There are many sets of complex numbers that resemble the integers  $\mathbb{Z}$ , but do not have a Euclid's Algorithm and do not have uniqueness of factorization. One such set can be found in Exercise 4.24.

## 4.4 The Division Theorem

Here is a proof by complete induction of the Division Theorem.

**Theorem 4.20** *Let  $m$  be a natural number. For every integer  $a$  there are unique numbers  $q$  and  $r$  so that*

$$a = mq + r$$

and  $0 \leq r < m$ .

*Proof* We fix the divisor  $m$ , a positive integer. We first prove by complete induction the Division Theorem for  $a \geq 0$ , by proving for all  $a \geq 0$  the statements

$P(a)$ : “there are integers  $q$  and  $r$  so that  $a = mq + r$  and  $0 \leq r = a - mq < m$ .”

For  $a < m$  this is clear: let  $q = 0$  and  $r = a$ . So  $P(a)$  is true for  $0 \leq a < m$  and the base case is done.

For the induction step: Suppose  $P(c)$  is true for all  $c < a$ . We show that  $P(a)$  is true, where we can assume  $a \geq m$  because the base case is done.

Now  $a \geq m$ , so if  $a' = a - m$ , then  $a' \geq 0$ . So by the induction assumption,  $P(a')$  is true:

$$a' = mq' + r'$$

for some integer  $q'$  and some number  $r' \geq 0$ . Adding  $m$  to both sides of that equation gives

$$m + a' = m + mq' + r'$$

or

$$a = m(q' + 1) + r'.$$

Setting  $q = q' + 1$ ,  $r = r'$  shows that  $P(a)$  is true. By complete induction,  $P(a)$  is true for all  $a \geq 0$ .

For  $a < 0$ , let  $c = -a$ . Then  $c > 0$ , so there exist  $q', r'$  so that

$$c = mq' + r'$$

and  $0 \leq r' < m$ .

If  $r' = 0$ , then  $a = -c = m(-q')$ , so setting  $q = -q'$  and  $r = 0$  gives the Division Theorem for  $a$  and  $m$ .

If  $0 < r' < m$ , then, letting  $r = m - r'$ , we have  $0 < r < m$  and

$$c = mq' + m - r.$$

Multiplying both sides by  $-1$  gives

$$-c = m(-q') + r - m,$$

which is the same as

$$a = m(-q' - 1) + r.$$

Setting  $q = -q' - 1$  gives the Division Theorem for  $a$  and  $m$ .

Uniqueness is left as Exercise 4.28. □

## 4.5 Well-Ordering

The natural numbers have been a fundamental part of mathematics throughout its long history. Prime numbers and the unique factorization of a number into a product of prime numbers can be found in Euclid's Elements (300 B. C.). Proposition 31 of Book IX of Euclid's Elements proves that every number  $\geq 2$  is divisible by a prime number, by an argument known as the impossibility of infinite descent.

Complete Induction, as described in Section 4.2, was only formulated within the past 350 years. Two centuries later, Peano and others gave a formal, set-theoretic definition of the natural numbers, a definition that included the principle of induction as an axiom of the natural numbers.

But Euclid's argument uses a proof strategy that is equivalent to a seemingly different property of the natural numbers, called the

**Theorem 4.21** (Well-Ordering Principle) *Any non-empty set of natural numbers has a least element.*

It turns out that the Well-Ordering Principle is just a variation of induction, in the following sense. Any fact about natural numbers that can be proved by induction can be proved by well-ordering, and conversely, any fact that can be proved by well-ordering can be proved by induction.

But the Well-Ordering Principle is independently useful because it permits us to define a number by the property that the number is the smallest element in a certain non-empty set. For example:

**Proposition 4.22** *Every two numbers  $a$  and  $b$  have a least common multiple, that is, a number  $m$  which is a common multiple of  $a$  and  $b$  and which is  $\leq$  any other common multiple of  $a$  and  $b$ .*

*Proof* The set  $S$  of common multiples of  $a$  and  $b$  contains  $a \cdot b$ , so is nonempty. By well-ordering,  $S$  has a smallest element, which is the least common multiple of  $a$  and  $b$ .  $\square$

To see how to use well-ordering instead of induction to prove statements about natural numbers, here is a Euclid-like proof of:

*Every number  $m \geq 2$  is divisible by a prime number.*

*Proof* Given a number  $m \geq 2$ , let  $S$  be the set of numbers  $\geq 2$  that divide  $m$ . Then  $S$  is a non-empty set, because  $m$  divides  $m$ . So by the Well-Ordering Principle,  $S$  has a least element  $q \geq 2$ . So  $q$  is the smallest number  $\geq 2$  that divides  $m$ . Is  $q$  prime? If not, then  $q$  is divisible by some number  $r$  satisfying  $2 \leq r < q$ . But since  $q$  divides  $m$  and  $r$  divides  $q$ , then  $r$  divides  $m$ . This contradicts the leastness of  $q$ . So  $q$  must be prime.  $\square$

As a fairly natural example of the use of Well-Ordering, here is a proof of the existence of Bezout's Identity:

**Theorem 4.23** *Let  $a, b$  be natural numbers and let  $d = (a, b)$  be the greatest common divisor of  $a$  and  $b$ . Then there are integers  $s, t$  so that  $d = sa + tb$ .*

*Proof* Let  $J_+$  be the set of all natural numbers of the form  $za + wb$  where  $z, w$  are any integers:

$$J_+ = \{za + wb : z, w \text{ any integers}, za + wb > 0\}.$$

Then  $J_+$  is a nonempty set of natural numbers, because  $J_+$  contains  $a = 1 \cdot a + 0 \cdot b$ . Let  $e$  be the smallest natural number in  $J_+$  ( $e$  exists by Well-Ordering.) Since  $e$  is in  $J_+$ , we have  $e = sa + tb$  for some integers  $s, t$ .

We want to show that  $e$  is the greatest common divisor of  $a$  and  $b$ .

First, let  $d$  be a common divisor of  $a$  and  $b$ . Then  $d$  divides  $za + wb$  for all integers  $z, w$ , because if  $a = dm$  and  $b = dn$ , then  $za + wb = d(zm + wn)$ , a multiple of  $d$ . So in particular,  $d$  divides  $e$ . Hence  $d \leq e$  for all common divisors  $d$  of  $a$  and  $b$ . So  $(a, b) \leq e$ .

Now we show that  $e$  is a common divisor of  $a$  and  $b$ . That will imply that  $e = (a, b)$ , completing the proof.

To show that  $e$  divides  $a$ , we apply the Division Theorem:

$$a = eq + r \text{ with } 0 \leq r < e.$$

Observe that

$$r = a - qe = a - q(sa + tb) = (1 - sq)a + (qt)b,$$

If  $r > 0$ , then  $r$  is in  $J_+$ , and since  $r < e$ , this contradicts the assumption that  $e$  was the smallest positive integer in  $J_+$ . Hence  $r$  must be equal to 0. Thus  $e$  divides  $a$ .

The same argument shows that  $e$  must divide  $b$ .

Hence  $e$  is a common divisor of  $a$  and  $b$ . Therefore  $e$  is the greatest common divisor of  $a$  and  $b$ .

Thus  $(a, b) = e = sa + tb$  for some integers  $s, t$ , hence Bezout's Identity is true.  $\square$

For details as to why the Well-Ordering Principle is equivalent to induction, see, for example, [Ch09, pp. 19–21]. (Or you could try to prove it yourself!)

## Exercises

- 4.1. Find the greatest common divisor of 60000 and 76500 by
  - (i) Factoring the two numbers;
  - (ii) Using Euclid's algorithm.
- 4.2. Find the least common multiple of
  - (i) 96 and 360,
  - (ii) 210 and 98,
  - (iii) 72 and 165.
- 4.3. Find the least common multiple of 60000 and 76500.
- 4.4. Given natural numbers  $d$  and  $m$ , show that there are natural numbers  $a$  and  $b$  so that  $(a, b) = d$  and  $[a, b] = m$ , if and only if  $d$  divides  $m$ .
- 4.5. Find the least common multiple of 83767 and 90119.
- 4.6. Prove that every common divisor of  $a$  and  $b$  divides the greatest common divisor of  $a$  and  $b$ .
- 4.7. (i) Why is it true that if  $a$  and  $b$  are coprime, then no prime number divides both  $a$  and  $b$ ?  
 (ii) Why is it true that if no prime number divides both  $a$  and  $b$ , then  $a$  and  $b$  are coprime?
- 4.8. Prove that if  $(a, c) = 1$  and  $(b, c) = 1$ , then  $(ab, c) = 1$ :
  - (i) by using Unique Factorization;
  - (ii) by using just Bezout's Identity.
- 4.9. Show that if  $(a, b) = 1$  and  $c$  divides  $a$ , then  $(c, b) = 1$ .
- 4.10. Show that  $(ma, mb) = m(a, b)$  for all numbers  $m, a$  and  $b$ , by showing that for each prime  $p$  that divides  $mab$ ,  $p^e \parallel (ma, mb)$  if and only if  $p^e \parallel m(a, b)$ .

- 4.11. Show that  $(ma, mb) = m(a, b)$  for all numbers  $m, a$  and  $b$  in two parts:
- Show that  $m(a, b)$  divides  $(ma, mb)$ , using Bezout's Identity for  $ma$  and  $mb$ .
  - Show that  $(ma, mb)$  divides  $m(a, b)$ , using Bezout's Identity for  $a$  and  $b$ .
- 4.12. (i) Show that if  $a$  and  $b$  are coprime and you add  $1/a$  and  $1/b$  by using the common denominator  $ab$ , the resulting fraction  $\frac{a+b}{ab}$  is reduced (“reduced” means that the numerator is coprime to the denominator).
- (ii) Show that if  $a$  and  $b$  are not coprime, and you add  $1/a$  and  $1/b$  by using the common denominator  $ab$ , the resulting fraction  $\frac{a+b}{ab}$  is not reduced.
- (iii) Find examples of primes  $p_1, p_2, p_3$  and numbers  $a, b$  so that

$$\frac{a}{p_1 p_2} + \frac{b}{p_1 p_3} = \frac{c}{p_1 p_2 p_3}$$

where  $\frac{a}{p_1 p_2}$  and  $\frac{b}{p_1 p_3}$  are reduced, but  $\frac{c}{p_1 p_2 p_3}$  is not reduced.

- 4.13. Find the smallest  $k > 0$  so that
- $24$  divides  $9k$ ;
  - $24$  divides  $11k$ ;
  - $24$  divides  $12k$ .
- 4.14. (i) Show that the smallest  $x > 0$  so that  $bx \equiv 0 \pmod{a}$  is  $x = a/(a, b)$ .
- (ii) Show that the smallest  $t > 0$  so that  $a$  divides  $bt$  is  $t = [a, b]/b$ .
- (iii) Show that
- $$\{x | bx \equiv 0 \pmod{a}\} = \{t | a \text{ divides } bt\}$$
- (iv) Why does that imply Proposition 4.10?

- 4.15. Let  $a, b, c$  be numbers  $> 1$ . Show:
- $a, b$  and  $c$  have a least common multiple, call it  $[a, b, c]$ .
  - $[a, b, c] = [[a, b], c] = [a, [b, c]]$ .
  - $[a, b, c]$  divides every common multiple of  $a, b$  and  $c$ .
  - If  $a, b$  and  $c$  are pairwise coprime, then  $[a, b, c] = abc$ .
- 4.16. Prove by complete induction that every number  $n \geq 2$  is prime or factors into a product of primes.
- 4.17. (i) Give a proof by contradiction that if a number  $n \geq 2$  is not prime, then  $n$  has a divisor  $b$  with  $1 < b \leq \sqrt{n}$ .
- (ii) Show that if a number  $n \geq 2$  is not prime, then  $n$  has a prime divisor  $p$  with  $1 < p \leq \sqrt{n}$ .  
(This fact is useful for finding small prime numbers.)
- 4.18. Prove by induction that if a prime  $p$  divides a product  $a_1 a_2 \cdots a_n$  of numbers, then  $p$  divides one of the factors  $a_i$ .
- 4.19. By induction, prove Lamé's result (see the exercises in Chapter 3) that Euclid's algorithm on  $a_n$  and  $a_{n+1}$  requires more divisions than EA does on  $a$  and  $b$  for any  $a < a_n$  and any  $b > a$ .

The next four exercises are helpful for trying to factor large numbers, as we'll see later in the book.

- 4.20. (i) Show that for all numbers  $m, c, d > 0$ , if  $(c, d) = 1$ , then

$$(m, cd) = (m, c)(m, d).$$

(ii) Is (i) true if  $(c, d) > 1$ ?

- 4.21. Let  $m$  be an odd number  $> 7$ . Suppose  $a$  is a number with  $\sqrt{m} < a < m$  so that  $m$  divides  $a^2 - 1$ , but  $m$  does not divide  $a + 1$  and  $m$  does not divide  $a - 1$ . Show that  $m$  factors as

$$m = (m, a + 1)(m, a - 1).$$

- 4.22. Let  $m = pq$  where  $p, q$  are distinct odd primes. Suppose  $a > b$  are numbers so that  $m$  divides  $a^2 - b^2$ , but  $m$  does not divide  $a + b$  and  $m$  does not divide  $a - b$ . Show that  $m$  factors as

$$m = (m, a + b)(m, a - b).$$

- 4.23. Let  $m$  be an odd number. Suppose  $a > b$  are numbers so that  $m$  divides  $a^2 - b^2$ , but  $m$  does not divide  $a + b$  and  $m$  does not divide  $a - b$ . Show that  $m$  factors as

$$m = (m, a + b)(m, a - b).$$

- 4.24. Let  $\mathbb{Z}[\sqrt{-23}]$  denote the set of complex numbers of the form  $a + b\sqrt{-23}$ , where  $a$  and  $b$  are integers. Every element of  $\mathbb{Z}[\sqrt{-23}]$  is uniquely of the form  $a + b\sqrt{-23}$  (for if  $a + b\sqrt{-23} = c + d\sqrt{-23}$  where  $a, b, c, d$  are integers, then  $a - c = (d - b)\sqrt{-23}$ : since  $a - c$  is an integer and  $(d - b)\sqrt{-23}$  is imaginary if  $d - b \neq 0$ , we must have  $a = c$  and  $b = d$ . See also Exercise 18.8.)

- (i) Verify that  $3 \cdot 3 \cdot 3 = (2 + \sqrt{-23})(2 - \sqrt{-23})$ .
- (ii) Show that  $2 + \sqrt{-23}$  and  $2 - \sqrt{-23}$  are not multiples of 3 in  $\mathbb{Z}[\sqrt{-23}]$ .
- (iii) Show that the only elements of  $\mathbb{Z}[\sqrt{-23}]$  that divide 3 are 3,  $-3$ , 1 and  $-1$ . Thus 3 is a “prime” in  $\mathbb{Z}[\sqrt{-23}]$ , and 3 can divide a product of two numbers in  $\mathbb{Z}[\sqrt{-23}]$  without dividing either number. (Thus in  $\mathbb{Z}[\sqrt{-23}]$  Lemma 4.18 and Theorem 4.17 are not valid.)

- 4.25. Prove the Coprime Divisibility Lemma from Unique Factorization. (This exercise, together with the proof of unique factorization in Section 4.3, shows that in rings similar to  $\mathbb{Z}[\sqrt{-23}]$ , the Coprime Divisibility Lemma is equivalent to unique factorization of numbers into products of primes.)

- 4.26. Show that the Well-Ordering Principle is equivalent to:

Let  $S$  be a non-empty set of integers and suppose every element of  $S$  is  $> B$  for some integer  $B$ . Show that that  $S$  has a least element.

(Well-Ordering is this statement with  $B = 0$ .)

- 4.27. Use Exercise 4.26 to prove the Division Theorem: Let  $m \geq 1$  be a natural number and let  $a$  be any integer. Let  $S$  be the following set of integers:

$$S = \{s \geq 0 | s = a - mq \text{ for some } q \text{ in } \mathbb{Z}\}.$$

Show

- (i)  $S$  is non-empty;
- (ii) The least element  $r$  of  $S$  satisfies

$$a = mq + r \text{ with } 0 \leq r < m.$$

- 4.28. Prove the uniqueness part of the Division Theorem. (See the last lines of the proof of Proposition 2.6.)

# Chapter 5

## Rings and Fields



To describe Caesar and Vigenère codes in Chapter 1, we introduced  $\mathbb{Z}_m$ , the set of numbers  $\{0, 1, \dots, m - 1\}$  with addition and multiplication “mod  $m$ ”. We claimed that  $\mathbb{Z}_m$  satisfies nearly all of the properties of addition and multiplication that ordinary real numbers satisfy, properties like associativity of addition, or commutativity of multiplication, or distributivity. But that claim remains unproven.

So in this chapter, we define  $\mathbb{Z}_m$  “correctly”.

We begin by defining the concepts of group, abelian group, ring, commutative ring, field. These are sets with operations that satisfy various properties that addition or multiplication of numbers satisfy. One point of defining and studying an abstract concept such as “commutative ring” is this: suppose we encounter a particular set of “numbers”, such as  $\mathbb{Z}_m$ , or, in Chapter 6, the set of polynomials with rational coefficients. If we find that the set of “numbers” satisfies the defining properties of a commutative ring, then we will know, without any further proof, that other properties of commutative rings, for example, properties of signed numbers, will also be true for that set of numbers.

Examples of abelian groups, commutative rings and fields appear in all of the cryptography and error correction in the book.

In Section 5.4 we introduce the concept of an ideal. An ideal of a commutative ring is a subset of the ring that satisfies properties analogous to those satisfied by a subspace of a vector space. We determine all of the ideals of the ring of integers  $\mathbb{Z}$ .

The really new concept in this chapter, found in Section 5.5, is the concept of a coset of an ideal  $J$  of a commutative ring  $R$ . For  $J$  an ideal of  $R$  and  $a$  an element of  $R$ , the coset  $a + J$  is, as a set, the set of all elements of  $R$  of the form  $a + r$  where  $r$  is in  $J$ . The set of all the cosets of  $J$  in  $R$  is denoted  $R/J$ , “ $R$  mod  $J$ ”. It turns out that for every ideal  $J$  of a commutative ring  $R$ , the set  $R/J$  of cosets is itself a commutative ring. Once we show that, then specializing to the case where the commutative ring is  $\mathbb{Z}$ , the ring of integers, and the ideal is  $m\mathbb{Z}$  (= the subset of  $\mathbb{Z}$  consisting of all multiples of the number  $m$ ), then the commutative ring  $\mathbb{Z}/m\mathbb{Z}$  looks just like  $\mathbb{Z}_m$ . In this way, we show that  $\mathbb{Z}_m$  is a commutative ring.

Working with cosets of the ideal  $m\mathbb{Z}$  of the ring of integers  $\mathbb{Z}$  is the same as working with integers modulo  $m$ , in the sense that two integers are congruent modulo  $m$  if and only if they are in the same coset of  $m\mathbb{Z}$  in  $\mathbb{Z}$ . This explains a comment in Chapter 2 that congruence modulo  $m$  is “like” equality: congruence modulo  $m$  is the same as equality of cosets of  $m\mathbb{Z}$  in  $\mathbb{Z}$ .

We will use  $\mathbb{Z}_m$ , integers modulo  $m$ , everywhere in the rest of the book. What this chapter does is to ensure that all of the usual manipulations we do with integers (other than canceling) remain valid when we do modular arithmetic.

We finish the chapter by showing that if  $m$  is a prime number, then  $\mathbb{Z}_m$  is a field. As will be pointed out in Chapter 7, the fact that  $\mathbb{Z}_p$  is a field for  $p$  prime implies that much of elementary linear algebra is valid when the “numbers” are from  $\mathbb{Z}_p$ .

Cosets of subgroups of a group will be defined and used in an essential way in Chapter 10, and will also show up in Chapters 12, 14 and 16 to help us to better understand the security of cryptographic schemes. The strategy of constructing  $R/J$  as a commutative ring of cosets will show up again in Chapter 18, where  $R$  is the ring of polynomials in one variable over a field. In that case the construction yields a doubly infinite collection of new finite fields that have application in cryptography and in error correction. (We’ll see an example in Chapter 19.)

So the abstract algebra of this chapter is essential mathematics for understanding modern cryptography and error correction.

## 5.1 Groups, Commutative Rings, Fields, Units

We start with the concept of group. The definition generalizes examples such as the set  $\mathbb{Z}$  of integers or the set  $\mathbb{Q}$  of rational numbers with the operation of addition (among many other examples).

To define a group, start with a set  $G$  and an operation  $*$  on  $G$ . An *operation*  $*$  is a function from  $G \times G$  (ordered pairs of elements of  $G$ ) to  $G$ . We write this information about the operation  $*$  concisely as

$$*: G \times G \rightarrow G.$$

Thus for every ordered pair  $(a, b)$  in  $G \times G$ ,  $a * b$  is an element of  $G$ .

The property:

$$\text{for every } a \text{ and } b \text{ in } G, a * b \text{ is in } G$$

is often described in words by saying that  $G$  is *closed* under the operation  $*$ .

In all of our examples, the operation will either be addition (+) or multiplication ( $\cdot$ ).

**Definition** A set  $G$  with an operation  $*$  is a *group* if:

- (associativity) For all  $a, b, c$  in  $G$ ,  $(a * b) * c = a * (b * c)$ .
  - (identity) There exists a special element  $e$  in  $G$ , called the *identity*, with the property that for all  $a$  in  $G$ ,  $e * a = a * e = a$ .
  - (inverse) For every  $a$  in  $G$ , there is some element  $b$  in  $G$  so that  $a * b = b * a = e$ .
- The group  $G$  is called *abelian* if also:
- (commutativity) For all  $a, b$  in  $G$ ,  $a * b = b * a$ .

With the operation  $*$  being  $+$  and the identity being 0, then  $\mathbb{Z}$  and  $\mathbb{Q}$  are abelian groups. With the operation  $*$  being  $\cdot$  and the identity being 1, then  $\mathbb{Z}$  and  $\mathbb{Q}$  are not groups, because the element 0 has no inverse:  $0 \cdot x = 1$  has no solution in  $\mathbb{Z}$  or  $\mathbb{Q}$ . However, the set of nonzero rational numbers is an abelian group under the usual multiplication of rational numbers (because  $\frac{a}{b} \cdot \frac{b}{a} = 1$  in  $\mathbb{Q}$ ). The set  $\{1, -1\}$  of integers is closed under the usual multiplication in  $\mathbb{Z}$ , and is an abelian group.

**Definition** A *ring (with identity)* is a set  $R$  with two operations,  $+$  and  $\cdot$ , and two special elements, 0 and 1, that satisfy:

- With the operation  $+$  (addition),  $R$  is an abelian group with additive identity 0, called the *zero element* of  $R$ .
- With the operation  $\cdot$  (multiplication),  $R$  satisfies the associative property: for every  $a, b, c$  in  $R$ ,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

- the element 1 is the multiplicative identity element: for all  $a$  in  $R$ ,  $a \cdot 1 = a = 1 \cdot a$ .
- With  $+$  and  $\cdot$ ,  $R$  satisfies the distributive laws: for every  $a, b, c$  in  $R$ ,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

and

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

If in addition, the multiplication  $\cdot$  on  $R$  satisfies the commutative law:

- for all  $a, b$  in  $R$ ,  $a \cdot b = b \cdot a$ ,

then  $R$  is called a *commutative ring*.

**Examples and non-examples.** The properties that define a commutative ring are exactly the properties of addition and multiplication of integers that we wrote down in Section 2.1. So the set  $\mathbb{Z}$  of integers, the set  $\mathbb{Q}$  of rational numbers, the set  $\mathbb{R}$  of real numbers, and the set  $\mathbb{C}$  of complex numbers, with addition and multiplication as we know them, are commutative rings. All of the properties that define a commutative ring, such as associativity and commutativity of addition, and distributivity, are typically used without thinking by anyone in secondary school who works with integers, or real numbers, or polynomial equations with real coefficients.

One point of formally introducing the concept of commutative ring is that once we show, for example, that  $\mathbb{Z}_m$ , the set  $\{0, 1, 2, \dots, m - 1\}$  with addition and multiplication mod  $m$  is a commutative ring, then we can confidently work with elements of  $\mathbb{Z}_m$  in the same way that we have done with real numbers in previous mathematics courses.

An example of a set that is not a commutative ring is the set  $\mathbb{N}$  of natural numbers, with the usual operations of addition ( $+$ ) and multiplication ( $\cdot$ ).  $\mathbb{N}$  is not a ring because it is not a group under addition. For example, 2 does not have a negative.

Another example, for students who have seen some calculus in three variables, is the set  $\mathbb{R}^3$  of all vectors in real three-space, with vector addition and cross product as multiplication. See Exercise 5.3 below.

If  $R$  is a ring, and  $S$  is a subset of  $R$  that is closed under addition, multiplication, taking negatives, and has 0 and 1, then  $S$  is also a ring. To see this, one has to check the properties, associativity of addition, distributivity, etc. But all of them hold in  $S$  because  $S$  is a subset of  $R$ , and all of the operations on  $S$  are the same as those on  $R$ . So all of the properties are valid for  $S$  because they are valid for  $R$ .

When  $R$  is a ring and  $S$  is a subset of  $R$  which is a ring with the operations those of  $R$ , we call  $S$  a *subring* of  $R$ .

*Example 5.1*  $\mathbb{Z}$  can be thought of as a subset of  $\mathbb{Q}$  by identifying the integer  $a$  with the rational number  $a/1$ . Then  $\mathbb{Z}$  is a subring of  $\mathbb{Q}$ . Similarly,  $\mathbb{Q}$  can be viewed as a subring of  $\mathbb{R}$  by writing a fraction as a decimal. And  $\mathbb{R}$  is a subring of the set  $\mathbb{C}$  of complex numbers.

But  $\mathbb{Z}_m = \{0, 1, 2, \dots, m - 1\}$  is not a subring of  $\mathbb{Z}$ , because the operations of addition and multiplication in  $\mathbb{Z}_m$  are not the same as those in  $\mathbb{Z}$ . (For example, in  $\mathbb{Z}$ ,  $2 + 2 = 4$ , while in  $\mathbb{Z}_3$ ,  $2 + 2 = 1$ .) We'll be precise about how  $\mathbb{Z}$  and  $\mathbb{Z}_m$  are related later in this chapter.

## 5.2 Basic Properties of Groups and Rings

In this section we obtain some other well-known properties of a group or a ring. Typically, when we define a mathematical structure, such as a group, we don't list all of the interesting properties that the structure has, but only a minimal number of properties, from which we can derive the other properties.

So when encountering a new possible group, if we verify just the minimal properties that define a group, then all the other properties will follow.

**Proposition 5.2** *A group (with operation  $*$ ) has only one identity element.*

*Proof* Suppose  $e$  and  $e'$  are both identity elements. Then  $e * e' = e'$  since  $e$  is an identity element, and  $e * e' = e$  since  $e'$  is an identity element. So  $e = e'$ .  $\square$

**Proposition 5.3** *A ring with identity contains only one zero element and only one identity element.*

*Proof* If  $R$  is a ring, then  $R$  is a group under addition, so has only one zero element by the last proposition. If  $1$  and  $1'$  are two identity elements, then  $1 = 1 \cdot 1' = 1'$  as in the proof of the last proposition.  $\square$

**Proposition 5.4** *In a group  $G$  (with operation  $*$ ), an element has only one inverse.*

*Proof* Call the identity element of  $G$  by  $e$ . Given  $g$  in the group, let  $h$  and  $k$  be inverses for  $g$ . Then  $h * g = g * h = e$ , and  $g * k = e$ . Then

$$g * h = g * k.$$

Multiplying by  $h$  on the left gives:

$$\begin{aligned} h * (g * h) &= h * (g * k) \\ (h * g) * h &= (h * g) * k \text{ by associativity,} \\ e * h &= e * k \text{ since } h * g = e, \\ h &= k \end{aligned}$$

$\square$

This result implies that each element of a commutative ring has a unique negative: that is, for  $a$  in a commutative ring, if  $a + b = 0$  and  $a + b' = 0$ , then  $b = b'$  (just copy the last argument). The unique  $b$  so that  $a + b = 0$  is called the negative of  $a$ . The negative of  $a$  is denoted by  $-a$ .

**Proposition 5.5** *In a commutative ring  $R$ , if an element  $a$  has an inverse  $b$  under multiplication (so that  $ab = ba = 1$ ), then  $b$  is unique.*

The proof is the same as that of Proposition 5.4.

If  $a$  in  $R$  has a multiplicative inverse (for short, “ $a$  has an inverse”), we’ll often denote the unique inverse of  $a$  by  $a^{-1}$  (but not by  $\frac{1}{a}$ ).

Two more useful properties of a commutative ring, involving the zero element and negatives, are:

**Proposition 5.6** *In a commutative ring  $R$ ,*

- (i)  $a \cdot 0 = 0$  for all  $a$  in  $R$ ;
- (ii)  $-a = (-1)a$  for all  $a$  in  $R$ .

*Proof* (i) We have  $0 + 0 = 0$  by the property of the zero element. Multiply both sides by  $a$  and distribute to get

$$a \cdot 0 + a \cdot 0 = a \cdot 0.$$

Add  $-(a \cdot 0)$  to both sides, reassociate the left side and use the property of negatives to get

$$a \cdot 0 + 0 = 0.$$

So again by the property of the zero element,  $a \cdot 0 = 0$ .

(ii) Starting from

$$1 + (-1) = 0,$$

multiply both sides on the right by  $a$  and distribute on the left side to get

$$1 \cdot a + (-1) \cdot a = 0 \cdot a.$$

Use (i) to get

$$a + (-1) \cdot a = 0.$$

Now use Proposition 5.4: both  $-a$  and  $(-1) \cdot a$  are negatives of  $a$ . So they must be equal.  $\square$

Property (ii) makes it easy to derive properties of “signed numbers”.

**Proposition 5.7** *In a commutative ring  $R$ ,*

- (i)  $(-1)(-1) = 1$
- (ii)  $-(-a) = a$  for all  $a$  in  $R$ .

*Proof* For (i): from Proposition 5.6, (ii), we have  $(-1)(-1) = -(-1)$ , the negative of  $-1$ . Since  $(-1) + 1 = 0$ ,  $1$  is a negative of  $-1$ . By uniqueness of the negative,  $-(-1) = 1$ . For (ii): both  $a$  and  $-(-a)$  are negatives of  $-a$ , so they must be equal.  $\square$

**Corollary 5.8** *For  $a, b$  in a commutative ring,  $(-a)(-b) = ab$ .*

*Proof* From Proposition 5.6, we have  $-a = (-1)a$  and  $-b = (-1)b$ . So

$$(-a)(-b) = ((-1)a)((-1)b).$$

By commutativity and associativity of multiplication, this is

$$= ((-1)(-1))(ab) = 1(ab) = ab.$$

$\square$

More properties of groups and commutative rings are found in Exercises 5.5–5.9.

### 5.3 Units and Fields

Associated to any commutative ring  $(R, +, \cdot)$  are two abelian groups, the additive group of  $R$  and the group of units of  $R$ .

The additive group of  $R$ , sometimes denoted as  $(R, +)$ , is the set  $R$  with the operation of addition. For the additive group we forget that  $R$  also has an operation of multiplication.

The other group involves the operation of multiplication in  $R$ .

**Definition** An element  $a$  of a commutative ring  $R$  is called a *unit* of  $R$  if there exists some  $b$  in  $R$  so that  $a \cdot b = b \cdot a = 1$ .

*Example 5.9* In  $\mathbb{Z}$  only  $1$  and  $-1$  are units. In  $\mathbb{Q}$  every rational number except  $0$  is a unit.

The statements “ $a$  is a unit of  $R$ ” and “ $a$  has an inverse in  $R$ ” mean the same thing.

We found that in  $\mathbb{Z}_m$ ,  $a$  is a unit if and only if there is an integer  $b$  so that  $(ab \bmod m) = 1$ , if and only if  $(a, m) = 1$ .

**Proposition 5.10** *The set of units of a commutative ring  $R$  is closed under multiplication, hence forms an abelian group, denoted by  $U_R$ .*

*Proof* If  $a$  and  $b$  are units of a ring  $R$ , and  $a^{-1}, b^{-1}$  are their (unique) inverses, then  $ab$  has an inverse also, namely,  $b^{-1}a^{-1}$ . So  $ab$  is a unit of  $R$ . Therefore the set of units  $U_R$  is closed under multiplication. Multiplication of units is associative and commutative because multiplication in  $R$  is associative and commutative. The multiplicative identity 1 of  $R$  is a unit of  $U_R$  because  $1 \cdot 1 = 1$ . Finally, every element of  $U_R$  has an inverse in  $U_R$ , because if  $a$  is in  $U_R$  and  $a'$  is the inverse of  $a$  in  $R$ , then  $a$  is the inverse of  $a'$  in  $R$ , so  $a'$  is in  $U_R$ . So  $U_R$  is an abelian group.  $\square$

The group  $U_{\mathbb{Z}}$  is the set  $\{1, -1\}$  with the usual multiplication.

## Fields.

**Definition** A *field*  $F$  is a commutative ring in which  $0 \neq 1$  (hence is a set with addition, multiplication and two different special elements 0 and 1, satisfying all the properties of a commutative ring) with the additional property:

- (inverses) Each  $a \neq 0$  in  $F$  is a unit.

Fields that you have almost certainly encountered are the rational numbers  $\mathbb{Q}$  and the real numbers  $\mathbb{R}$ . You have probably met  $\mathbb{C}$ , the complex numbers. By the end of this chapter we'll see that  $\mathbb{Z}_p$  is a field for every prime number  $p$ . An example of particular interest in applications to error correction is  $\mathbb{Z}_2 = \{0, 1\}$  with addition and multiplication modulo 2. We'll use it in Chapter 7.

The group of units of a field  $F$  is  $U_F = F \setminus \{0\}$ , the set of all elements of  $F$  except for the zero element. We just proved that  $U_F$  is closed under multiplication. So if  $a$  and  $b$  are non-zero elements of a field, then  $a \cdot b$  must also be a non-zero element of the field.

However, for some commutative rings that aren't fields or subrings of a field, it is possible for the product of two non-zero elements to be equal to zero. For example,  $\mathbb{Z}_6$  is not a field, because 2 and 3 don't have inverses modulo 6, and  $2 \cdot_6 3 = 0$  in  $\mathbb{Z}_6$ .

## 5.4 Ideals

As noted in the introduction to this chapter, we want to construct the integers modulo  $m$  in a way that will make it easy to see that  $\mathbb{Z}_m$  is a commutative ring. The strategy we adopt involves the concept of *ideal*.

**Definition** An *ideal*  $J$  of a commutative ring  $R$  is a non-empty subset of  $R$  that is closed under addition and scalar multiplication: that is,

- for all  $h, k$  in  $J$ ,  $h + k$  is in  $J$ ;
- for all  $k$  in  $J$  and all  $r$  in  $R$ ,  $rk$  is in  $J$ .

Readers acquainted with linear algebra and vector spaces may recall the notion of a subspace of a vector space. In linear algebra, a subset  $W$  of a vector space  $V$  over a field  $F$  is a subspace if  $W$  is closed under addition, and also closed under scalar multiplication by elements of  $F$ . Those are the same properties that define an ideal. So an ideal is like a subspace of the ring  $R$ .

But if you remember enough about linear algebra, you will know that a subspace of a one-dimensional vector space  $V$  is either the whole space  $V$  or consists of only the zero vector. This is also true for an ideal if the commutative ring is a field (see Proposition 5.12, below). But it is no longer true if  $R$  is a commutative ring but not a field, as we'll see very soon.

Continuing with analogies to linear algebra, there are two “natural” ways to obtain subspaces of a vector space  $V$ . One is as the subspace  $W$  spanned by a set of vectors in  $V$ . The other way is as the null space of a matrix, or equivalently as the set of solutions to a system of homogeneous linear equations. We’ll see that analogues of both methods yield ideals.

In this chapter we’ll look at the spanning idea.

**Definition** Let  $R$  be a commutative ring. The ideal  $J$  of  $R$  generated by elements  $a_1, \dots, a_n$  of  $R$  is the set of all elements of  $R$  that are  $R$ -linear combinations of  $a_1, \dots, a_n$ . Thus a general element of  $J$  is

$$a = r_1a_1 + r_2a_2 + \dots + r_na_n$$

where  $r_1, r_2, \dots, r_n$  are any elements of  $R$ .

The ideal  $J$  spanned by  $a_1, \dots, a_n$  is denoted by

$$J = \langle a_1, \dots, a_n \rangle.$$

It is easy to check that the set  $\langle a_1, \dots, a_n \rangle$  is closed under addition and scalar multiplication, hence is an ideal. For addition, let  $r_1, \dots, r_n, s_1, \dots, s_n$  be any elements of  $R$ . Then

$$(r_1a_1 + \dots + r_na_n) + (s_1a_1 + \dots + s_na_n) = (r_1 + s_1)a_1 + \dots + (r_n + s_n)a_n;$$

for scalar multiplication, let  $r_1, \dots, r_n, t$  be any elements of  $R$ . Then

$$t(r_1a_1 + \dots + r_na_n) = (tr_1)a_1 + \dots + (tr_n)a_n.$$

(This argument used associativity of multiplication and addition, commutativity of addition, and distributivity in  $R$ .)

Note that every ideal contains 0. For if  $a$  is any element of  $J$ , then  $0 \cdot a = 0$  is in  $J$  because  $J$  is closed under scalar multiplication. This property is analogous to the property that every subspace of a vector space contains the zero vector.

*Example 5.11* Every commutative ring contains two trivial ideals.

The ideal  $\langle 0 \rangle$  consists of only the element 0 of  $R$ . We call  $\langle 0 \rangle$  the zero ideal of  $R$ .

The ideal  $\langle 1 \rangle = R$ . For if  $r$  is any element of  $R$ , then  $r = r \cdot 1$  is in  $\langle 1 \rangle$ .

**Proposition 5.12** A field has no ideals other than the two trivial ideals.

*Proof* Suppose  $J$  is an ideal of a field  $F$  and contains an element  $a$  other than 0. Then  $a$  is a unit of  $F$  with inverse  $a^{-1}$ , and  $J$  contains  $a^{-1} \cdot a = 1$  because  $J$  is closed under scalar multiplication. So  $J = F$ .  $\square$

(This is the same proof that shows that a non-zero subspace of a one-dimensional vector space  $V$  is all of  $V$ .)

**Ideals of  $\mathbb{Z}$ .** On the other hand, a commutative ring that is not a field typically has many ideals. We’ll illustrate by finding all of the ideals of  $\mathbb{Z}$ .

**Definition** An ideal of a commutative ring  $R$  that is generated by a single element  $b$  is called a *principal ideal* of  $R$ .

The principal ideal  $\langle b \rangle$  generated by an element  $b$  of  $R$  is

$$\langle b \rangle = \{rb : r \text{ in } R\},$$

the set of all scalar multiples of  $b$ .

**Theorem 5.13** Every ideal of  $\mathbb{Z}$  is a principal ideal.

The proof is almost identical to the proof of Bezout's Identity in Chapter 4.

*Proof* Let  $J$  be a non-zero ideal of  $\mathbb{Z}$ . Let  $a \neq 0$  be in  $J$ . Then  $(-1)a = -a$  is also in  $J$ , so  $J$  contains a positive integer.

Let  $J_+$  denote the set of all positive integers in  $J$ . Since  $J_+$  is non-empty, then Well-Ordering implies that there is a smallest positive integer  $d$  in  $J$ .

We claim that  $J = \langle d \rangle = \{rd : r \in \mathbb{Z}\}$ . To see this, we let  $b$  be any element of  $J$ , and show that  $d$  divides  $b$ . To do so, we apply the Division Theorem:

$$b = qd + r \text{ with } 0 \leq r < d.$$

Now  $J$  contains  $b$  and  $d$ , and is closed under addition and scalar multiplication, so  $J$  contains  $b - qd = r$ . If  $r \neq 0$ , then  $r$  is a smaller positive integer than  $d$  in  $J$ , contradicting the minimality of  $d$ .

Hence  $r = 0$ , and  $d$  divides  $b$ . Thus  $J$  consists entirely of multiples of  $d$ . So  $J = \langle d \rangle$  is principal, as claimed.  $\square$

We recall some terminology about functions.

**Definition** A function  $f$  from a set  $S$  to a set  $T$ , written for short,  $f : S \rightarrow T$ , is a bijection if  $f$  is one-to-one and onto  $T$ . One-to-one means, if  $s_1 \neq s_2$  in  $S$ , then  $f(s_1) \neq f(s_2)$  in  $T$ . Onto means, for every  $t$  in  $T$ , there is some  $s$  in  $S$ , so that  $f(s) = t$ .

We can describe all ideals of  $\mathbb{Z}$ .

**Proposition 5.14** There is a bijection between the non-zero ideals of  $\mathbb{Z}$  and the natural numbers.

*Proof* Define a function  $\mathcal{G}$  [think of  $\mathcal{G}$  as “ideal generated by”] from the natural numbers  $\mathbb{N}$  to the set of non-zero ideals of  $\mathbb{Z}$  by

$$m \mapsto \mathcal{G}(m) = \langle m \rangle = \{\text{the set of all integer multiples of } m\} = m\mathbb{Z}.$$

We just showed that every non-zero ideal  $J$  contains a smallest positive integer  $d$ , and then  $J = \langle d \rangle$  consists of all multiples of  $d$ . Thus the function  $\mathcal{G}$  maps the natural numbers onto the set of all non-zero ideals of  $\mathbb{Z}$ .

We now show  $\mathcal{G}$  is one-to-one.

If  $\mathcal{G}(d) = \mathcal{G}(e)$  for some natural numbers  $d$  and  $e$ , then  $\langle d \rangle = \langle e \rangle$ . But then  $d$  is in  $\langle e \rangle$ , so  $d$  is a multiple of  $e$ , and similarly  $e$  is a multiple of  $d$ : thus

$$dr = e \text{ and } es = d$$

for some positive integers  $r$  and  $s$ . But then  $esr = e$ . Cancellation holds in  $\mathbb{Z}$ , so  $sr = 1$ . But the only positive integers  $r$  and  $s$  so that  $sr = 1$  are  $r = s = 1$ , hence  $e = d$ . Thus the map  $\mathcal{G}$  from  $\mathbb{N}$  to ideals of  $\mathbb{Z}$  given by  $m \mapsto \langle m \rangle$  is bijective.  $\square$

Since  $\langle m \rangle \subseteq \mathbb{Z}$  consists of all integer multiples of  $m$ ,

$$\langle m \rangle = \{mt : t \in \mathbb{Z}\} = m\mathbb{Z},$$

we will often denote  $\langle m \rangle$  by  $m\mathbb{Z}$  hereafter.

## 5.5 Cosets and Integers Modulo $m$

In this section we show how to construct a new commutative ring from a known commutative ring and an ideal of that ring. The construction will give us a new view of  $\mathbb{Z}_m$ .

We begin by generalizing the notion of congruence modulo  $m$  for integers.

**Definition** Let  $R$  be a commutative ring and  $J$  be an ideal of  $R$ . For  $a, b$  in  $R$ ,  $a$  is congruent to  $b$  modulo  $J$ , written

$$a \equiv b \pmod{J},$$

if  $a - b$  is in  $J$ .

Because  $J$  is an ideal of  $R$ , all the properties of congruence modulo  $m$  in  $\mathbb{Z}$  hold in the more general setting. For example, congruence modulo  $J$  is reflexive, symmetric and transitive, and also gets along with addition and multiplication in  $R$ , namely:

**Proposition 5.15** *Given an ideal  $J$  of a commutative ring  $R$ , for all  $a, a', b, b'$  in  $R$ :*

*if  $a \equiv a' \pmod{J}$  and  $b \equiv b' \pmod{J}$ , then*

*$a + b \equiv a' + b' \pmod{J}$ , and*

*$a \cdot b \equiv a' \cdot b' \pmod{J}$ .*

*Proof* The proof is virtually identical to the proof of the corresponding result for congruence modulo  $m$ . What makes it work is precisely the properties that an ideal  $J$  is closed under addition and scalar multiplication. To see this, we do the multiplication rule.

If  $a \equiv a' \pmod{J}$ , then  $a - a' = h$  is in  $J$  and  $a = a' + h$ . If  $b \equiv b' \pmod{J}$ , then  $b - b' = k$  is in  $J$ , and  $b = b' + k$ . So

$$ab = (a' + h)(b' + k) = a'b' + hb' + a'k + hk.$$

Since  $h$  and  $k$  are in  $J$ , so are  $hb'$  and  $a'k$  and  $hk$ , because an ideal is closed under scalar multiplication by any elements of  $R$ . Then  $hb' + a'k + hk$  is in  $J$  because  $J$  is closed under addition. So  $ab = a'b' + (\text{an element of } J)$ . Hence

$$ab \equiv a'b' \pmod{J}.$$

The addition rule only needs that  $J$  is closed under addition. □

Congruence modulo  $m$  in  $\mathbb{Z}$  is the same as congruence modulo the ideal  $m\mathbb{Z}$ , as is easily checked.

Now for new rings.

**Definition** Let  $R$  be a commutative ring,  $J$  an ideal of  $R$ , and  $a$  an element of  $R$ . The subset  $a + J = \{a + k : k \in J\}$  of  $R$  is called the *coset of  $J$  represented by  $a$* .

*Example 5.16* Let  $R = \mathbb{Z}$ ,  $J = 2\mathbb{Z}$ . The coset  $1 + 2\mathbb{Z}$  of  $\mathbb{Z}$  consists of all the odd integers, and the coset  $0 + 2\mathbb{Z}$  consists of all the even integers.

More generally, the coset  $a + m\mathbb{Z}$  of  $\mathbb{Z}$  consists of all the integers of the form  $a + (\text{multiple of } m)$ , hence consists of all integers that are congruent to  $a$  modulo  $m$ .

**Definition** The set of all distinct cosets of  $J$  in  $R$  is denoted  $R/J$ , “ $R$  mod  $J$ ”.

We will make a commutative ring out of  $R/J$ . But first, we ask when two cosets are equal.

**Proposition 5.17** (Equality of cosets) *Let  $R$  be a commutative ring,  $J$  an ideal of  $R$ ,  $a, b$  in  $R$ . Then  $a + J = b + J$  if and only if any of the following four conditions hold:*

- (i)  $a$  is in  $b + J$  (which means,  $a = b + h$  for some  $h$  in  $J$ );
- (ii)  $b$  is in  $a + J$ ;
- (iii)  $a - b$  is in  $J$ ;
- (iv)  $a \equiv b \pmod{J}$ .

*Proof* Given Exercise 5.20, which says that an ideal is closed under taking negatives, the first three conditions are all easily seen to be equivalent, and we defined (iv) by condition (iii). So we just need to show that two cosets are equal if any of the four conditions holds.

First, suppose  $a + J = b + J$ . Then  $a = a + 0$  is in  $a + J$ , so  $a$  is in  $b + J$ , so condition (ii) holds.

Conversely, suppose  $a$  is in  $b + J$ . Then  $a = b + h$  for some  $h$  in  $J$ . So for all  $k$  in  $J$ ,  $a + k = b + (h + k)$  is in the coset  $b + J$  (since  $J$  is closed under addition). So the set  $a + J$  is a subset of  $b + J$ .

If  $a$  is in  $b + J$ , then since (i) implies (ii),  $b$  is in  $a + J$ , so the same argument shows that  $b + J$  is a subset of  $a + J$ .

So the two cosets are equal.  $\square$

If we specialize to  $J = m\mathbb{Z}$ , congruence modulo the ideal  $m\mathbb{Z}$  is exactly the same as congruence modulo  $m$ . So we have

**Proposition 5.18** *Let  $R = \mathbb{Z}$ ,  $J = \langle m \rangle = m\mathbb{Z}$ . For all  $a, b$  in  $\mathbb{Z}$ , the following are equivalent:*

- $a + m\mathbb{Z} = a' + m\mathbb{Z}$
- $a \equiv a' \pmod{m}$
- $a$  and  $a'$  have the same remainder when divided by  $m$ .

*Proof* The only part that is not a special case of Proposition 5.17 is the result from Section 2.3 that  $a \equiv a' \pmod{m}$  if and only if  $a$  and  $a'$  have the same remainder when divided by  $m$ .  $\square$

A consequence of Proposition 5.18 is that a coset of  $J$  in  $R$  can be described by any element in the coset. If an element  $a$  is in the coset, then the coset is  $a + J$ . We have as many choices for  $a$  as we have elements in the coset.

If we write a coset of  $J$  as  $a + J$ , we call  $a$  a *representative* of the coset. Every element of a coset can be a representative of the coset.

If  $b$  is congruent to  $a$  modulo  $J$ , then  $b$  is in  $a + J$ . So every element  $b$  of  $R$  that is congruent to  $a$  modulo  $J$  can be chosen as a representative of the coset  $a + J$ .

Specializing to  $\mathbb{Z}/m\mathbb{Z}$ , Proposition 5.18 implies that we can represent the elements of  $\mathbb{Z}/m\mathbb{Z}$  as

$$0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, (m - 1) + m\mathbb{Z},$$

because every integer  $b = mq + r$  where  $0 \leq r < m$  by the Division Theorem, and so  $b + m\mathbb{Z} = r + m\mathbb{Z}$ .

**Another view of  $\mathbb{Z}_m$ .** Recall from Section 2.1 of Chapter 2 that  $\mathbb{Z}_m$ , “arithmetic modulo  $m$ ” is the set

$$\{0, 1, 2, \dots, m - 1\},$$

with addition and multiplication “mod  $m$ ”.

There is an obvious function  $\mathcal{C}$ , “coset of”,

$$\mathcal{C} : \mathbb{Z}_m \rightarrow \mathbb{Z}/m\mathbb{Z}$$

defined by

$$\mathcal{C}(a) = a + m\mathbb{Z}$$

for  $a = 0, 1, \dots, m - 1$ .

Proposition 5.18 implies that the function  $\mathcal{C}$  is bijective. Soon, we'll see that  $\mathcal{C}$  has other nice properties.

**Arithmetic properties of  $R/J$ .** Now we want to show that if  $J$  is an ideal of a commutative ring  $R$ , then  $R/J$  is itself a commutative ring, with the following addition and multiplication:

$$\begin{aligned} (i) \quad (a + J) + (b + J) &= (a + b) + J \\ (ii) \quad (a + J) \cdot (b + J) &= (a \cdot b) + J. \end{aligned}$$

In words, to add (multiply) two cosets, take the coset of the sum (product) of representatives.

In formula (ii), the plus signs  $+$  are part of the notation for the three cosets in the formula. They remind us that, for example, the coset  $a + J$  is the subset of  $R$  consisting of elements  $a + k$  where  $k$  is in  $J$ .

Formula (i) is littered with plus signs, but the ones immediately to the left of the  $J$ 's are part of the notation for the cosets. There are two significant plus signs.

The  $+$  between  $(a + J)$  and  $(b + J)$  is the new addition of cosets that we are defining. This new addition uses the known addition in  $R$  that shows up on the right side:  $(a + b)$ . The first formula tells us that when we add the elements  $a + J$  and  $b + J$  of  $R/J$ , the result is the coset  $c + J$  where  $c = a + b$ , the sum of  $a$  and  $b$  in  $R$ .

Beyond the notation, we need to be a bit careful with these definitions. The problem is that we've defined addition and multiplication of cosets by using particular representatives. We need to observe that the choice of representatives doesn't matter, that addition and multiplication of cosets is "well-defined", that is, not dependent on the choice of representatives we used to describe the cosets. More concisely,

**Proposition 5.19** *Let  $J$  be an ideal of a commutative ring  $R$ , and suppose  $a, b, a', b'$  are in  $R$ . If  $a + J = a' + J$  and  $b + J = b' + J$ , then*

$$\begin{aligned} (i) \quad (a + b) + J &= (a' + b') + J \\ (ii) \quad (a \cdot b) + J &= (a' \cdot b') + J. \end{aligned}$$

*Proof* These follow immediately from the condition that  $c + J = c' + J$  if and only if  $c \equiv c' \pmod{J}$ , and Proposition 5.15, which says that if  $a \equiv a' \pmod{J}$  and  $b \equiv b' \pmod{J}$ , then  $a + b \equiv a' + b' \pmod{J}$  and  $a \cdot b \equiv a' \cdot b' \pmod{J}$ .  $\square$

The properties that an ideal  $J$  is closed under both addition and scalar multiplication are precisely what are needed to show that Proposition 5.15 is true, and therefore that cosets of  $J$  in  $R$  have a well-defined addition and multiplication.

Once we have well-definedness, we can show:

**Theorem 5.20** *Let  $R$  be a commutative ring and  $J$  an ideal. Then  $R/J$  is a commutative ring.*

*Proof* This follows routinely from the fact that  $R$  does. We illustrate with some of the properties and leave the rest for the reader. In what follows,  $a, b, c$ , etc. are arbitrary elements of  $R$ . We use only the definition of addition and multiplication of cosets, together with properties of addition and multiplication of  $R$ .

- Associativity of addition.

$$((a + J) + (b + J)) + (c + J) = ((a + b) + J) + (c + J) = ((a + b) + c) + J$$

while

$$(a + J) + ((b + J) + (c + J)) = (a + J) + ((b + c) + J) = (a + (b + c)) + J.$$

Since associativity holds in  $R$ , we have  $((a + b) + c) = (a + (b + c))$ . Thus associativity holds in  $R/J$ .

- Commutativity of addition holds in exactly the same way. So does associativity of multiplication.
- Commutativity of multiplication.

$$(a + J) \cdot (b + J) = (a \cdot b) + J = (b \cdot a) + J = (b + J) \cdot (a + J)$$

since multiplication is commutative in  $R$ .

- Distributivity is shown in the same way.
- Zero element:  $0 + J$  is the zero element of  $R/J$ :  $(0 + J) + (a + J) = (0 + a) + J = a + J$ .
- Negatives: the negative of  $a + J$  is  $(-a) + J$ , as is quickly checked.
- Identity element: the identity of  $R/J$  is  $1 + J$ , as is quickly checked.

We're done. □

## 5.6 $\mathbb{Z}_m$ is a Commutative Ring

Now we can complete our new description of  $\mathbb{Z}_m$ .

*Example 5.21* Recall the bijective function  $\mathcal{C} : \mathbb{Z}_m \rightarrow \mathbb{Z}/m\mathbb{Z}$ , defined on  $\mathbb{Z}_m = \{0, 1, 2, \dots, m - 1\}$  by  $\mathcal{C}(a) = a + m\mathbb{Z}$ . We show that  $\mathcal{C}$  respects addition and multiplication in  $\mathbb{Z}_m$  and  $\mathbb{Z}/m\mathbb{Z}$ .

Addition. In  $\mathbb{Z}_m$ , we add  $a$  and  $b$  by:  $a +_m b$  is the remainder when  $a + b$  is divided by  $m$ . In  $\mathbb{Z}/m\mathbb{Z}$  we add cosets by

$$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}.$$

Now  $(a +_m b)$  is the remainder when  $a + b$  is divided by  $m$ , so

$$(a + b) \equiv (a +_m b) \pmod{m}.$$

So by Proposition 5.18,

$$(a + b) + m\mathbb{Z} = (a +_m b) + m\mathbb{Z}.$$

So the map  $\mathcal{C}$  from  $\mathbb{Z}_m$  to  $\mathbb{Z}/m\mathbb{Z}$  respects addition:

$$\begin{aligned} \mathcal{C}(a +_m b) &= (a +_m b) + m\mathbb{Z} \\ &= (a + b) + m\mathbb{Z} \\ &= (a + m\mathbb{Z}) + (b + m\mathbb{Z}) \\ &= \mathcal{C}(a) + \mathcal{C}(b). \end{aligned}$$

Multiplication. In  $\mathbb{Z}_m$ , we multiply  $a$  and  $b$  by  $a \cdot_m b$ , defined to be the remainder when  $a \cdot b$  is divided by  $m$ . In  $\mathbb{Z}/m\mathbb{Z}$  we multiply cosets by

$$(a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) = (a \cdot b) + m\mathbb{Z}.$$

But since

$$a \cdot b \equiv a \cdot_m b \pmod{m},$$

we have

$$(a \cdot b) + m\mathbb{Z} = (a \cdot_m b) + m\mathbb{Z}.$$

So the map  $\mathcal{C}$  from  $\mathbb{Z}_m$  to  $\mathbb{Z}/m\mathbb{Z}$  respects multiplication:

$$\begin{aligned}\mathcal{C}(a \cdot_m b) &= a \cdot_m b + m\mathbb{Z} \\ &= a \cdot b + m\mathbb{Z} \\ &= (a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) \\ &= \mathcal{C}(a) \cdot \mathcal{C}(b).\end{aligned}$$

So under the correspondence  $\mathcal{C}$  between  $\mathbb{Z}_m$  and  $\mathbb{Z}/m\mathbb{Z}$ , addition and multiplication in  $\mathbb{Z}_m$  become addition and multiplication in  $\mathbb{Z}/m\mathbb{Z}$ .

The function  $\mathcal{C}$  is an example of what we'll call in Chapter 12 a *ring homomorphism* from  $\mathbb{Z}_m$  to  $\mathbb{Z}/m\mathbb{Z}$ .

Because the function  $\mathcal{C}$  is bijective and respects addition and multiplication, it follows that since  $\mathbb{Z}/m\mathbb{Z}$  is a commutative ring, so is  $\mathbb{Z}_m$ , because every property of  $\mathbb{Z}/m\mathbb{Z}$  that makes  $\mathbb{Z}/m\mathbb{Z}$  into a commutative ring translates to the corresponding property for  $\mathbb{Z}_m$ .

For example, let us show distributivity:

$$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c).$$

Since  $\mathcal{C}$  is bijective and respects addition and multiplication, it suffices to show that

$$\mathcal{C}(a \cdot_m (b +_m c)) = \mathcal{C}((a \cdot_m b) +_m (a \cdot_m c)).$$

The left side is

$$\begin{aligned}\mathcal{C}(a) \cdot \mathcal{C}(b +_m c) &= \mathcal{C}(a) \cdot (\mathcal{C}(b) + \mathcal{C}(c)) \\ &= (a + m\mathbb{Z}) \cdot ((b + m\mathbb{Z}) + (c + m\mathbb{Z})) \\ &= (a + m\mathbb{Z}) \cdot ((b + c) + m\mathbb{Z}) \\ &= (a \cdot (b + c)) + m\mathbb{Z}.\end{aligned}$$

Similarly, the right side is

$$= ((a \cdot b) + (a \cdot c)) + m\mathbb{Z}.$$

The left and right sides are equal because of distributivity in  $\mathbb{Z}$ .

Since  $\mathbb{Z}_m$  is a commutative ring, the manipulations we did with decrypting in the multiplicative Caesar cipher of Chapter 2 are valid.

*Example 5.22* Suppose Alice wants to encrypt the message GO LEFT, or 7, 15, 0, 12, 5, 6, 20, working in  $\mathbb{Z}_{27}$ , where the encrypting multiplier is 5. She gets

$$35, 75, 0, 60, 2, 30, 100 \bmod 27$$

or

$$8, 21, 0, 2, 25, 3, 19,$$

and sends that sequence to Bob. Bob decrypts by multiplying by 11 modulo 27, since  $5 \cdot 11 \bmod 27 = 1$ . He can decrypt by multiplying by 11 because for all numbers  $a$ ,

$$(a \cdot_{27} 5) \cdot_{27} 11 = a \cdot_{27} (5 \cdot_{27} 11) = a \cdot_{27} 1 = a,$$

since multiplication in  $\mathbb{Z}_{27}$  is associative and 1 in  $\mathbb{Z}_{27}$  satisfies the identity property. We know this because the map  $\mathcal{C}$  from  $\mathbb{Z}_{27}$  to  $\mathbb{Z}/27\mathbb{Z}$  is bijective and respects addition and multiplication, and the corresponding properties hold in  $\mathbb{Z}/27\mathbb{Z}$ .

## 5.7 Complete Sets of Representatives for $\mathbb{Z}/m\mathbb{Z}$

Now that we know that  $\mathbb{Z}_m$ , integers modulo  $m$ , and  $\mathbb{Z}/m\mathbb{Z}$ , cosets of the ideal  $m\mathbb{Z}$ , are essentially the same, and that  $\mathbb{Z}/m\mathbb{Z}$  is a commutative ring, it follows that  $\mathbb{Z}_m$  is a commutative ring and we can be completely comfortable doing computations modulo  $m$  without worrying that something might go wrong.

But thinking of  $\mathbb{Z}_m$  as  $\mathbb{Z}/m\mathbb{Z}$ , cosets, and doing computations modulo  $m$  gives us more flexibility in computations. We don't need to immediately reduce modulo  $m$  when we do computations. We can reduce modulo  $m$  by replacing the representative  $a$  of  $a + m\mathbb{Z}$  by  $(a \bmod m)$  only when or if it is convenient.

In turn, using  $\mathbb{Z}/m\mathbb{Z}$  is equivalent to using congruence modulo  $m$ , that is, doing computations in  $\mathbb{Z}$  with the understanding that the computations are defined modulo  $m$ . So we can just work with integers, with the understanding that all computations are valid “modulo  $m$ ”. In particular, we can replace numbers by other numbers modulo  $m$  as convenient. We saw this in several examples where we solved congruences in earlier chapters.

*Example 5.23* Suppose we want to solve the equation

$$(13 + 29\mathbb{Z})(x + 29\mathbb{Z}) = 17 + 29\mathbb{Z}, \text{ or } 13 \cdot_{29} x = 17.$$

This is the same as solving the congruence

$$13x \equiv 17 \pmod{29}.$$

By multiplying the congruence by suitable numbers coprime to 29 and replacing numbers by other numbers modulo 29, we get  $x = 8$ . (Try it! You could start by multiplying both sides by  $-2$ , then by 10.)

**Definition** A set of integers  $\{r_1, r_2, \dots, r_m\}$  is a *complete set of representatives modulo  $m$*  if every coset in  $\mathbb{Z}/m\mathbb{Z}$  is represented by exactly one of the integers  $r_1, \dots, r_m$ .

*Example 5.24* The set of integers

$$\{0, 1, 2, 3, \dots, 10\}$$

is a complete set of representatives for  $\mathbb{Z}/11\mathbb{Z}$ . So also is

$$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$$

which is usually easier to work with when adding or multiplying modulo 11 manually, because the numbers are smaller.

A less obvious but useful complete set of representatives for  $\mathbb{Z}/11\mathbb{Z}$  is

$$\{0, 1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9\},$$

a sequence of numbers which is congruent modulo 11 to the sequence

$$\{0, 1, 2, 4, 8, 5, 10, 9, 7, 3, 6\}.$$

The set of powers of 2 is easy to work with when multiplying in  $\mathbb{Z}/11\mathbb{Z}$  because  $2^5 = 32 \equiv -1 \pmod{11}$ . Thus if we multiply  $2^6$  and  $2^7$  modulo 11, we have

$$2^6 \cdot 2^7 = 2^{13} = 2^{10} \cdot 2^3 \equiv 8 \pmod{11}.$$

A number  $b$  whose powers represent all of the non-zero cosets of  $\mathbb{Z}/m\mathbb{Z}$  is called a *primitive root* modulo  $m$ . Thus 2 is a primitive root modulo 11. We'll see primitive roots again in Chapter 8 and in particular in Chapter 13.

## 5.8 When is $\mathbb{Z}/m\mathbb{Z}$ a Field?

**Theorem 5.25**  $\mathbb{Z}/m\mathbb{Z}$  is a field if and only if  $m$  is prime.

A field is a commutative ring  $F$  with the property that every non-zero element of  $F$  has an inverse in  $F$ . We know that  $\mathbb{Z}/m\mathbb{Z}$  is a commutative ring. So we just need to show that every non-zero element of  $\mathbb{Z}/m\mathbb{Z}$  has an inverse if and only if  $m$  is a prime number.

We first recall some terminology.

**Definition** A *unit* of a commutative ring  $R$  is an element  $a$  of  $R$  that has a multiplicative inverse in  $R$ . In other words,  $a$  is a unit of  $R$  if there is an element  $b$  of  $R$  so that  $ab = 1$ .

A *zero divisor* of a commutative ring  $R$  is a non-zero element  $a$  of  $R$  for which there is a non-zero element  $b$  of  $R$  so that  $ab = 0$ .

To prove Theorem 5.25 we show first:

**Proposition 5.26** In  $\mathbb{Z}/m\mathbb{Z}$ , an element  $a + m\mathbb{Z}$  is a unit if and only if  $(a, m) = 1$ , and is a zero divisor if and only if  $1 < (a, m) < m$ .

To show this, we first suppose that  $0 < a < m$  and  $(a, m) = d > 1$ . Then  $m = dt$  is a non-trivial factorization of  $m$  with  $0 < t < m$ . Letting  $a = ds$  for some integer  $s$ , we have  $at = dst = sdt = sm \equiv 0 \pmod{m}$ . So  $a$  is a zero divisor modulo  $m$ . Then  $a$  cannot be a unit modulo  $m$ , because of:

**Lemma 5.27** Let  $a$  be an element of a commutative ring  $R$ . If  $a$  is a unit of  $R$ , then  $a$  is not a zero divisor in  $R$ .

*Proof* Suppose  $a$  is a unit of  $R$  with inverse  $a^{-1}$ . Suppose  $a \cdot c = 0$  for some element  $c$  of  $R$ . Then

$$0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot c) = (a^{-1} \cdot a) \cdot c = 1 \cdot c = c.$$

Since  $a \cdot c = 0$  only for  $c = 0$ ,  $a$  is not a zero divisor.  $\square$

On the other hand, if  $(a, m) = 1$ , then by Bezout's Identity,  $as + mt = 1$  for some integers  $s, t$ , and then

$$as \equiv 1 \pmod{m}.$$

So the units of  $\mathbb{Z}/m\mathbb{Z}$  are precisely those elements  $a + m\mathbb{Z}$  for which  $(a, m) = 1$ .

Theorem 5.25 follows easily. For the  $m$  for which  $\mathbb{Z}/m\mathbb{Z}$  is a field are those  $m$  for which every non-zero number  $< m$  is coprime to  $m$ . That is the case exactly when  $m$  is prime.

What we showed in Proposition 5.26 is that  $\mathbb{Z}_m$  has three kinds of elements:

- 0;
- units, elements  $a$  where  $(a, m) = 1$ ; and
- zero divisors, elements  $a$  where  $1 < (a, m) < m$ .

This trichotomy does not hold in general for commutative rings: for example the ring  $\mathbb{Z}$  of integers has no zero divisors and only two units, so it has many elements that are neither units nor zero divisors.

*Example 5.28* In  $\mathbb{Z}_5$ , each of 1, 2, 3, 4 is a unit, because

$$1 \cdot 1 = 2 \cdot 3 = 4 \cdot 4 \equiv 1 \pmod{5}.$$

In  $\mathbb{Z}_{15}$ , 1, 2, 4, 7,  $-7$ ,  $-4$ ,  $-2$  and  $-1$  are units, because

$$1 \cdot 1 \equiv -1 \cdot -1 \equiv 2 \cdot -7 \equiv -2 \cdot 7 \equiv 4 \cdot 4 \equiv -4 \cdot -4 \equiv 1 \pmod{15}.$$

The other non-zero elements, 3, 5, 6, 9, 10 and 12, are zero divisors. Since

$$3 \cdot 5 = 3 \cdot 10 = 0,$$

we say that 5 and 10 are *complementary zero divisors of 3*. The complementary zero divisors of 10 are 3, 6, 9, and 12.

We know that if  $p$  is prime then  $\mathbb{Z}/p\mathbb{Z}$  is a field. So we now know infinitely many fields. The smallest of them is  $\mathbb{Z}/2\mathbb{Z} = \{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}\}$ , which we will usually view as  $\mathbb{Z}_2 = \{0, 1\}$  with operations modulo 2.

We'll use  $\mathbb{Z}/2\mathbb{Z}$  in Chapter 7.

We observed in the last section that 2 is a primitive root of  $\mathbb{Z}/11\mathbb{Z}$ . We'll show later that for every prime  $p$ ,  $\mathbb{Z}/p\mathbb{Z}$  has a primitive root. (But it need not be 2.)

We haven't done much with groups in this chapter. But we'll return to groups in Chapters 10, 12, 13, 14 and 16.

## Exercises

- 5.1. Starting from the definition of a ring in Section 5.1, prove the rule called FOIL: if  $a, b, c, d$  are elements of a commutative ring  $R$ , then

$$(a + b) \cdot (c + d) = ac + ad + bc + bd : \text{First} + \text{Outside} + \text{Inside} + \text{Last}.$$

The basic properties of addition and multiplication in a commutative ring are behind the usual algorithm for multiplying multidigit numbers. (The algorithm dates back at least to the Indian mathematician Brahmagupta (628 AD).) But they also lead to a faster algorithm, discovered in 1960 by the Russian mathematician Anatoly Karatsuba:

- 5.2. Fix a number  $r > 0$  (such as  $r = 10$ ). Suppose we want to multiply  $a_1 \cdot r + a_0$  and  $b_1 \cdot r + b_0$ , where  $0 \leq a_0, a_1, b_0, b_1 < r$

(i) Show that with the usual multiplication algorithm, we find

$$(a_1 \cdot r + a_0)(b_1 \cdot r + b_0)$$

by FOIL, so we need to do four multiplications:  $a_1 b_1$ ,  $a_1 b_0$ ,  $a_0 b_1$  and  $a_0 b_0$ .

(ii) Show that for all  $a_0, a_1, b_0, b_1$  in a commutative ring,

$$a_1 b_0 + a_0 b_1 = a_1 b_1 + a_0 b_0 - (a_1 - a_0)(b_1 - b_0).$$

(iii) Show that to multiply  $a_1 \cdot r + a_0$  and  $b_1 \cdot r + b_0$ , we only need to do three multiplications involving the digits  $a_0, a_1, b_0, b_1$ :  $a_0 b_0, a_1 b_1$  and  $(a_1 - a_0)(b_1 - b_0)$ .

[(ii) is the key idea behind Karatsuba multiplication, which, for example, multiplies two numbers of  $2^4 = 16$  digits using  $3^4 = 81$  digit multiplications rather than  $4^4 = 256$  digit multiplications. Look up “Karatsuba multiplication” online, or see [Ch09, pp 132–4].]

- 5.3. The set  $\mathbb{R}^3$  of vectors with three real components has two operations on it, vector addition and the crossed product. Every vector  $\mathbf{v} = (a, b, c)$  is a sum

$$\mathbf{v} = a\mathbf{i} + b\mathbf{j} + c\mathbf{k},$$

where  $\mathbf{i} = (1, 0, 0), \mathbf{j} = (0, 1, 0), \mathbf{k} = (0, 0, 1)$ . Let  $\mathbf{0} = (0, 0, 0)$ . Then the crossed product is defined on  $\mathbf{i}, \mathbf{j}, \mathbf{k}$  by

$$\begin{aligned}\mathbf{i} \times \mathbf{i} &= \mathbf{j} \times \mathbf{j} = \mathbf{k} \times \mathbf{k} = \mathbf{0}, \\ \mathbf{i} \times \mathbf{j} &= -\mathbf{j} \times \mathbf{i} = \mathbf{k}, \mathbf{j} \times \mathbf{k} = -\mathbf{k} \times \mathbf{j} = \mathbf{i}, \mathbf{k} \times \mathbf{i} = -\mathbf{i} \times \mathbf{k} = \mathbf{j}.\end{aligned}$$

and extended to all vectors in  $\mathbb{R}^3$  by distributivity.

- (i) Can you find two vectors  $\mathbf{v}$  and  $\mathbf{w}$  so that

$$\mathbf{v} \times \mathbf{w} = \mathbf{w} \times \mathbf{v}$$

and  $\mathbf{v} \times \mathbf{w}$  is not the zero vector?

- (ii) Can you find three vectors  $\mathbf{v}, \mathbf{w}$  and  $\mathbf{y}$  so that

$$(\mathbf{v} \times \mathbf{w}) \times \mathbf{y} = \mathbf{v} \times (\mathbf{w} \times \mathbf{y})$$

and  $(\mathbf{v} \times \mathbf{w}) \times \mathbf{y}$  is not the zero vector?

- (iii) Show that the set  $(\mathbb{R}^3, +, \times)$  is not a commutative ring: the operation  $\times$  is not associative or commutative, and there is no identity element.

- 5.4. (i) Show that the set of natural numbers  $\mathbb{N}$  with the operation  $a * b = (a, b)$ , where  $(a, b)$  is the greatest common divisor of  $a$  and  $b$ , is not a group: show that the operation  $*$  is associative and commutative, but there is no identity element.  
(ii) Repeat (i) where the operation is  $a * b = [a, b]$ , where  $[a, b]$  is the least common multiple of  $a$  and  $b$ . Show that there is an identity element, but not every number has an inverse.

In the next three exercises, assume that  $R$  is a commutative ring.

- 5.5. Prove that for all  $a, b$  in  $R$ ,  $(-a)b = -(ab)$ .  
5.6. Show that for all  $a, b, c, d$  in  $R$ , if  $a + b = d$  and  $a + c = d$ , then  $b = c$ .  
5.7. Show that for all  $a, d$  in  $R$ , if  $a$  has an inverse in  $R$ , then there is a unique solution in  $R$  to the equation  $ax = d$ .  
5.8. Let  $G$  be a group, with operation  $*$  and identity element  $e$ . Prove *left cancellation* in  $G$ : for all  $a, b, c$  in  $G$ , if  $a * b = a * c$ , then  $b = c$ .  
5.9. Let  $G$  be a group, with operation  $*$ . Prove *left solvability* in  $G$ : for every  $a$  and  $b$  in  $G$ , there is some  $x$  in  $G$  so that  $a * x = b$ .  
5.10. Find the inverse of 2 in  $\mathbb{Z}_m$  for  
(i)  $m = 9$ ;  
(ii)  $m = 101$   
(iii) each odd  $m > 1$ .  
5.11. Let  $a, b$  be real numbers, not both  $= 0$ . Write down a formula for the inverse of the complex number  $a + bi$  (where  $i = \sqrt{-1}$  satisfies  $i^2 = -1$ ).

- 5.12. Let  $\mathbb{Q}[\sqrt{-23}]$  be the set of complex numbers  $\mathbb{C}$  of the form  $a + b\sqrt{-23}$  where  $a, b$  are in  $\mathbb{Q}$ . Show that  $\mathbb{Q}[\sqrt{-23}]$  is a field. (Assume that  $\mathbb{C}$  is a field.)
- 5.13. Suppose  $R$  is a commutative ring with identity  $1 \neq 0$ , such that for all  $a \neq 0$  and  $b$  in  $R$ , the equation  $ax = b$  has a unique solution in  $R$ . Show that  $R$  is a field.
- 5.14. Suppose  $F$  is a field, and  $a$  is a nonzero element of  $F$ . Show that if  $r, s$  are in  $F$  and  $ar = as$ , then  $r = s$ .
- 5.15. Write down the elements of the group  $U_{10}$  of units of  $\mathbb{Z}_{10}$ . Find the inverse of each element of  $U_{10}$ .
- 5.16. (i) Show that if  $a, b, c$  are numbers,  $q$  is an integer and  $b = aq + c$ , then the ideals  $\langle a, b \rangle$  and  $\langle a, c \rangle$  are equal.  
(ii) Using Euclid's Algorithm, show that for numbers  $a, b$ , the ideal  $\langle a, b \rangle = \langle d \rangle$  where  $d$  is the greatest common divisor of  $a$  and  $b$ .
- 5.17. Decide whether or not 238 is in the ideal  $\langle 391, 493 \rangle$  of  $\mathbb{Z}$ .
- 5.18. Write the ideal  $\langle 1001, 1541, 1911 \rangle$  of  $\mathbb{Z}$  as a principal ideal.
- 5.19. Carefully write down the proof of (ii) of Proposition 5.19.
- 5.20. Why is it that if  $J$  is an ideal of a commutative ring and  $a$  is in  $J$ , then  $-a$  is also in  $J$ ?
- 5.21. Write down the proof of distributivity for Theorem 5.20.
- 5.22. One student tried to prove distributivity by writing down the left side of the distributive law as

$$(a + J)((b + J) + (c + J)) = (a + J)(b + c + J + J) = (ab + ac + aJ + aJ + Jb + Jc + JJ + JJ),$$

distributing as though  $J$  were an element of  $R$  rather than a subset of  $R$ . Is there any way to make sense of this?

- 5.23. Show that if  $J$  is a non-zero ideal of  $\mathbb{Z}_m$ , then  $J$  is the principal ideal generated by  $a$  where  $a$  is the smallest positive integer in the set

$$\{b \in \mathbb{N} : b \text{ is in } J\}.$$

- 5.24. What are the ideals of  $R = \mathbb{Z}_6$ ?
- 5.25. Let  $D_0$  be the subset of  $\mathbb{Z}_m$  consisting of 0 and all of the zero divisors of  $\mathbb{Z}_m$ . Is  $D_0$  an ideal of  $\mathbb{Z}_m$  for all  $m$ ? Are there any numbers  $m$  so that  $D_0$  is an ideal of  $\mathbb{Z}_m$ ? (Try some examples.)
- 5.26. Find a primitive root of  
(i)  $\mathbb{Z}_5$ ;  
(ii)  $\mathbb{Z}_{13}$ ;  
(iii)  $\mathbb{Z}_{17}$ .

- 5.27. Assuming you have learned the multiplication table for the numbers 0 through 10, multiply in your head the product

$$16 \cdot 13 \cdot 17 \pmod{21}$$

by using the complete set of representatives  $\{-10, -9, \dots, 9, 10\}$  for  $\mathbb{Z}_{21}$ .

- 5.28. Two fields sometimes used in applications are  $\mathbb{Z}_{257}$ , where  $257 = 2^8 + 1$  is a prime number, and  $\mathbb{Z}_{127}$ , where  $127 = 2^7 - 1$  is a prime number. Is 2 a primitive root of  $\mathbb{Z}_{257}$ ? of  $\mathbb{Z}_{127}$ ? Explain.
- 5.29. Let  $p$  and  $q$  be distinct prime numbers and  $m = pq$ . What is the size of the group  $U_m$  of units of  $\mathbb{Z}_m$ ?

# Chapter 6

## Polynomials



In Chapter 5 we introduced commutative rings, such as  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  and  $\mathbb{Z}_m$  for  $m$  a positive integer. Other familiar examples are the rings of polynomials with coefficients in a commutative ring. Polynomials with real coefficients, viewed as functions, arise in introductory calculus and in secondary school mathematics. In this chapter we take our first look at polynomials.

For polynomials with coefficients in a field, there is a Division Theorem, just as for integers. Our modest goal in this chapter is D'Alembert's Theorem: *a polynomial of degree  $n$  with coefficients in a field has at most  $n$  roots in a field*. D'Alembert's Theorem is surprisingly useful later in the book, for example, in connection with Reed–Solomon error correcting codes.

Chapter 18 will complete the analogue for polynomials of the theory for  $\mathbb{Z}$  presented in Chapters 4 and 5. Doing so will yield all fields with finitely many elements. See Section 18.5.

### 6.1 Basic Concepts

We begin with the definition of a polynomial and the definition of addition and multiplication of polynomials.

Let  $R$  be a commutative ring.

**Definition** A polynomial with coefficients in  $R$  is an expression of the form

$$f = \dots + a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x^1 + a_0 x^0,$$

where the coefficients  $\dots, a_n, a_{n-1}, \dots, a_1, a_0$  are elements of  $R$ , only a finite number of the coefficients are non-zero, and  $x$  is a symbol called an indeterminate.

Some examples of polynomials (with  $R = \mathbb{R}$ , the real numbers):

$$\begin{aligned} f(x) &= 2x^6 - 3x + 2, \\ f(x) &= x^4 + \pi x + \sqrt{3} \\ f(x) &= 2 \text{ (here } a_0 = 2, \text{ and } 0 = a_1 = a_2 = \dots). \end{aligned}$$

A polynomial is uniquely defined by its coefficients. Thus if

$$g = \dots + b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x^1 + b_0 x^0,$$

is another polynomial with coefficients in  $R$ , then  $f = g$  if and only if  $a_0 = b_0, a_1 = b_1, \dots, a_n = b_n, \dots$

A polynomial  $f$  is very similar to a polynomial function on the commutative ring  $R$ ,

$$f(x) = \dots + a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x^1 + a_0 x^0.$$

The function  $f(x)$  takes an element  $r$  of  $R$  and sends it to the element

$$\begin{aligned} f(r) &= \dots + a_n r^n + a_{n-1} r^{n-1} + \dots + a_1 r^1 + a_0 r^0 \\ &= \dots + a_n r^n + a_{n-1} r^{n-1} + \dots + a_1 r + a_0 \end{aligned}$$

of  $R$ , obtained by viewing  $x^k$  as the  $k$ -th power of the indeterminate element  $x$  and replacing  $x^k$  by the  $k$ -th power  $r^k$  of the element  $r$  for all  $k$ . (So we'll write  $x^1 = x$  and  $x^0 = 1$  hereafter.) The term "indeterminate" for  $x$  expresses the idea that when viewing the polynomial  $f$  as a function on  $R$ ,  $x$  may be viewed as an indeterminate element of  $R$ .

There is little harm in viewing a polynomial  $f$  as a function  $f(x)$  on  $R$ , except for the question of equality.

Two functions  $f$  and  $g$  with domain a set  $S$  are equal precisely when  $f(s) = g(s)$  for all  $s$  in  $S$ .

If two polynomial functions are equal as polynomials, they are equal as functions.

But it is possible for two different polynomials with coefficients in a field  $F$  to define the same function on  $F$ : for example, the two polynomials  $f(x) = x^2$  and  $g(x) = x$  are equal as functions on the field  $\mathbb{Z}_2 = \{0, 1\}$  (because  $f(0) = g(0) = 0$  and  $f(1) = g(1) = 1$ ) even though  $f$  and  $g$  are not equal as polynomials. We'll see that the two definitions of equality are the same if and only if the field of coefficients  $F$  has infinitely many elements. We'll consider the case where  $R$  is a field with finitely many elements when we discuss D'Alembert's Theorem later in this chapter.

In any case, we'll use the notation  $f$  and  $f(x)$  interchangeably for a polynomial.

The set of all polynomials with coefficients in  $R$  is denoted by  $R[x]$  (assuming the indeterminate is called  $x$ ).

We can add and multiply polynomials in  $R[x]$  by thinking of the polynomials as functions evaluated at an indeterminate element of  $R$  and adding and multiplying the polynomials as though they were elements of  $R$ . Thus addition is defined by

$$f(x) + g(x) = \dots + (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \dots + (a_1 + b_1)x + (a_0 + b_0).$$

To describe how multiplication works, call a polynomial with one non-zero term  $ax^m$  a *monomial*. We multiply monomials by  $ax^m \cdot bx^n = abx^{m+n}$ , and then multiply polynomials by viewing a polynomial as a sum of monomials and using the distributive law. (See the proof of Proposition 6.1, below, for what multiplication looks like for general polynomials.)

The polynomial whose only non-zero coefficient is  $a_0 = 1$  is the multiplicative identity.

The addition and multiplication just defined on  $R[x]$  makes  $R[x]$  into a commutative ring (which seems plausible because if we view  $x$  as an indeterminate element of  $R$ , then  $R[x]$  is a commutative ring because  $R$  is).

Some terminology related to polynomials:

**Definition** The polynomial  $f(x) = a_n x^n + \dots + a_1 x + a_0$  has *degree*  $n$  if  $x^n$  is the highest power of  $x$  appearing in  $f(x)$  with its coefficient  $a_n$  not zero. The monomial  $a_n x^n$  is called the *leading term* of  $f(x)$ .

The coefficient  $a_n$  of the leading term of  $f(x)$  is called the *leading coefficient* of  $f(x)$ .

If  $f(x)$  has degree  $\geq 0$  and the leading coefficient of  $f(x)$  is 1, then  $f(x)$  is called *monic*. Thus  $x^3 + 6x - 2$  is a monic polynomial of degree 3, while  $2x^9 + 1$  has degree 9 but is not monic.

The polynomial with  $a_0 = a_1 = \dots = 0$  is called the zero polynomial and is denoted by 0.

By convention, the degree of the zero polynomial is  $-\infty$ . We'll see why shortly. Every other polynomial  $f(x)$  has degree  $\geq 0$ . The degree of a polynomial  $f(x)$  is denoted by  $\deg f(x)$ .

We can think of  $R$  as a subset of  $R[x]$  by identifying  $a$  in  $R$  with the polynomial  $ax^0$  (which we also write as  $a$  because  $x^0 = 1$  and  $a \cdot 1 = a$ ).

For polynomials with coefficients in a field  $F$ , the degree of a polynomial is a useful tool. In particular, we have

**Proposition 6.1** (Degree Formula) *Let  $R$  be a commutative ring with no zero divisors. If  $f(x)$  and  $g(x)$  are non-zero polynomials in  $F[x]$ , then*

$$\deg(fg) = \deg(f) + \deg(g).$$

*Proof* Let

$$f(x) = a_m x^m + \dots + a_1 x + a_0$$

and

$$g(x) = b_n x^n + \dots + b_1 x + b_0,$$

where  $a_m$  and  $b_n$  are the leading coefficients of  $f$  and  $g$ , respectively. Then  $\deg(f) = m$ ,  $\deg(g) = n$ . Using the distributive law and collecting the coefficients of each power of  $x$ , multiplication of  $f(x)$  and  $g(x)$  is

$$\begin{aligned} f(x) \cdot g(x) &= (a_n x^n + \dots + a_1 x + a_0)(b_m x^m + \dots + b_1 x + b_0) \\ &= a_n b_m x^{m+n} + \dots + (\sum_{i+j=k} a_i b_j) x^k + \dots + (a_0 b_1 + a_1 b_0) x + \dots + a_0 b_0. \end{aligned}$$

Now  $a_n$  and  $b_m$  are not zero and there are no zero divisors in  $R$ . Therefore  $a_n b_m \neq 0$ , so  $a_n b_m x^{m+n}$  is the leading term of  $f(x)g(x)$ . So  $f(x)g(x)$  has degree  $n + m = \deg(f(x)) + \deg(g(x))$ .  $\square$

The convention that the zero polynomial has degree  $-\infty$ , together with the reasonable assumption that  $-\infty + m = -\infty$  for  $m$  any integer or  $m = -\infty$ , allows the formula  $\deg(fg) = \deg(f) + \deg(g)$  to extend to the case where one or both of  $f$  and  $g$  is the zero polynomial.

In Chapter 5 we looked at units and zero divisors for  $\mathbb{Z}_m$ . Using the degree formula we can find the units and zero divisors of  $R[x]$  if  $R$  has no zero divisors.

**Corollary 6.2** *If  $R$  has no zero divisors, then the units of  $R[x]$  are the units of  $R$  (viewed as polynomials of degree 0), and  $R[x]$  has no zero divisors.*

*Proof* Let  $f, g$  be in  $R[x]$ . If  $fg = 1$ , then the degree formula says that  $\deg(f) + \deg(g) = 0$ . Since  $f$  and  $g$  cannot be zero, they have degrees  $\geq 0$ . Thus both must have degree 0, hence are in  $R$ . Since  $fg = 1$ ,  $f$  and  $g$  must be units of  $R$ .

If  $fg = 0$ , then  $-\infty = \deg(fg) = \deg(f) + \deg(g)$ , so  $\deg(f)$  or  $\deg(g) = -\infty$ , hence one of  $f$  and  $g = 0$ . So  $R[x]$  has no zero divisors.  $\square$

On the other hand, if  $R$  has zero divisors (such as, for example  $R = \mathbb{Z}_4$ ), then of course  $R[x]$  has zero divisors (for example,  $0 = 2 \cdot 2 = (2 \cdot x^0) \cdot (2 \cdot x^0)$ ) and also has units of degree  $> 0$  (for example,  $1 + 2x$ , which has inverse  $1 + 2x$ ). Finding all of the units and zero divisors of  $R[x]$  when  $R$  has zero divisors can be an interesting problem.

## 6.2 Division Theorem

For the rest of this chapter,  $R$  will be a field, which we will call  $F$ .

Hopefully you learned long division for polynomials. Here is an example, with  $F = \mathbb{Q}$ . We divide  $2x^2 - 2x - 4$  into  $6x^4 + 6x^3 - x^2 + x + 3$  in  $\mathbb{Q}[x]$ :

$$\begin{array}{r}
 & 3x^2 & +6x & +\frac{23}{2} \\
 \hline
 2x^2 - 2x - 4 ) & 6x^4 & +6x^3 & -x^2 & +x & +3 \\
 & 6x^4 & -6x^3 & -12x^2 & & \\
 \hline
 & 12x^3 & +11x^2 & +x & +3 \\
 & 12x^3 & -12x^2 & -24x & & \\
 \hline
 & 23x^2 & +25x & +3 \\
 & 23x^2 & -23x & -46 & & \\
 \hline
 & 48x & +49 & & &
 \end{array}$$

Long division for polynomials proceeds like long division for numbers, except that it is easier (there is no guessing of terms in the quotient). For the long division laid out above, there are three steps, one for each monomial in the quotient. We start by dividing the leading term  $2x^2$  of the divisor  $2x^2 - 2x - 4$  into the leading term  $6x^4$  of the dividend  $6x^4 + 6x^3 - x^2 + x + 3$ : we get  $6x^4 = 2x^2 \cdot 3x^2$ . So  $3x^2$  becomes the first term of the quotient, and we find that

$$6x^4 + 6x^3 - x^2 + x + 3 = (2x^2 - 2x - 4) \cdot 3x^2 + (12x^3 + 11x^2 + x + 3).$$

Thus for a remainder we get a polynomial  $12x^3 + 11x^2 + x + 3$  of degree less than the degree of our original dividend. That polynomial acts as a new dividend. Then we repeat two more times, until we obtain a polynomial,  $48x + 49$ , whose degree is  $<$  the degree of the divisor. That last polynomial is the remainder in the long division presented above, where we divided  $2x^2 - 2x - 4$  into  $6x^4 + 6x^3 - x^2 + x + 3$ .

Long division tells us that the dividend is the product of the divisor and the quotient, plus the remainder, where the degree of the remainder is less than the degree of the divisor. In the example above, we find that

$$6x^4 + 6x^3 - x^2 + x + 3 = (2x^2 - 2x - 4)(3x^2 + 6x + \frac{23}{2}) + (48x + 49).$$

Generalizing this example yields the Division Theorem for Polynomials. We will often let  $f, g, p, q, r$ , etc., denote polynomials, omitting the “ $(x)$ ” in “ $f(x)$ .”

**Theorem 6.3** (Division Theorem for Polynomials) *Let  $F$  be a field. Let  $f, g$  be in  $F[x]$  with  $f \neq 0$ . Then there are unique polynomials  $q$  (the quotient) and  $r$  (the remainder), with  $\deg r < \deg f$ , such that  $g = fq + r$ .*

*Proof* Fix the divisor  $f \neq 0$ . We'll prove that for any dividend  $g$ , there exists some quotient  $q$  and some remainder  $r$  satisfying the statement of the theorem, using complete induction on the degree of  $g$ .

Formally, given the polynomial  $f$  of degree  $d \geq 0$ , we let  $P(n)$  be the statement:

*For every polynomial  $g$  of degree  $n$ , there exist polynomials  $q$  and  $r$  with  $\deg r \leq d = \deg f$  so that  $g = fq + r$ .*

We first look at the case where  $\deg g < \deg f$ . Then we don't need to do anything: we just set  $q = 0$  and  $r = g$ : then obviously  $g = fq + r$  with  $\deg r < \deg f$ . (If we set up the long division, we do nothing: this case is illustrated by the case  $f = 2x^2 - 2x - 4$  and  $g = 48x + 49$  in our long division example above.) This includes the base case of the induction argument.

Suppose  $n = \deg g \geq \deg f$ . Let  $f = f(x) = a_d x^d + \dots + a_0$  have degree  $d$ , so that  $a_d \neq 0$  in  $F$ . Write  $n = d + s$  with  $s \geq 0$  and let  $g = g(x) = b_{d+s} x^{d+s} + \dots + b_0$  with  $b_{d+s} \neq 0$ .

Since  $a_d$  is non-zero, it has an inverse  $a_d^{-1}$  in the field  $F$ . So divide the leading term of  $g$  by the leading term of  $f$ :

$$\frac{b_{d+s} x^{d+s}}{a_d x^d} = (b_{d+s} a_d^{-1}) x^s,$$

and let  $g_1 = g - (b_{d+s} a_d^{-1}) x^s \cdot f$ . Then the coefficient of  $x^n = x^{d+s}$  in  $g_1$  is

$$b_{d+s} - (b_{d+s} a_d^{-1}) a_d = 0.$$

So  $\deg g_1 < \deg g$ . By complete induction, we may assume that  $g_1 = fq_1 + r$  for some polynomials  $q_1$  and  $r$ , with  $\deg r < \deg f$ . But then

$$\begin{aligned} g &= b_{d+s} a_d^{-1} x^s \cdot f + g_1 \\ &= b_{d+s} a_d^{-1} x^s \cdot f + fq_1 + r \\ &= f(b_{d+s} a_d^{-1} x^s + q_1) + r, \end{aligned}$$

proving the existence of a quotient and remainder for  $f$  and  $g$ . That completes the induction step.

By induction, the existence of  $q$  and  $r$  is proven: the statement  $P(n)$  is true for all  $n \geq 0$ .

Note that we need the leading coefficient of the divisor  $f$  to have an inverse to carry out the division. That will always be the case if the coefficients of the polynomials come from a field.

We now show that the quotient  $q$  and the remainder  $r$  are unique.

Suppose  $g = fq + r = fq_1 + r_1$ , with  $\deg r < \deg f$  and  $\deg r_1 < \deg f$ . Then

$$f(q - q_1) = r_1 - r.$$

If  $q - q_1 \neq 0$ , let  $s \geq 0$  be the degree of  $q - q_1$ . Then  $f(q - q_1)$  has degree  $\deg(f) + s$  by Proposition 6.1, while  $r_1 - r$  has degree  $< \deg(f)$ , which is impossible. Thus  $q - q_1 = 0$  and  $r_1 - r = 0$ .  $\square$

A polynomial  $f$  divides a polynomial  $g$  if  $g = fq$  for some polynomial  $q$ .

For example, in  $\mathbb{Q}[x]$ ,  $x^2 - 1$  divides  $x^4 - 1$  because  $(x^2 - 1)(x^2 + 1) = x^4 - 1$ .

Similarly,  $2x^2 - 2x + 2$  divides  $x^3 + 1$  because  $x^3 + 1 = (2x^2 - 2x + 2)(\frac{1}{2}x + \frac{1}{2})$ .

But  $x - 1$  does not divide  $x^3 - 2$ . A quick way to verify that claim is to use the following useful criterion:

**Theorem 6.4** (Remainder Theorem) *If  $f(x)$  is a polynomial with coefficients in a field  $F$ , and  $a$  is in  $F$ , then the remainder when dividing  $f(x)$  by  $x - a$  is  $f(a)$ .*

*Proof* Write  $f(x) = (x - a)q(x) + r(x)$ , by the Division Theorem. Then  $\deg r(x) < \deg(x - a)$ , so the remainder  $r(x)$  has degree  $\leq 0$ , so is the polynomial defined by an element  $r$  of the field  $F$ . That is,

$$f(x) = (x - a)q(x) + r.$$

Evaluating both sides at  $x = a$ , we have in the field  $F$ :

$$f(a) = (a - a)q(a) + r = r.$$

So the remainder  $r$  is  $f(a)$ .  $\square$

**Definition** Let  $F$  be a field,  $f(x)$  a non-zero polynomial with coefficients in  $F$ . An element  $a$  of  $F$  is a *root* of  $f(x)$  if  $f(a) = 0$ .

Hopefully you are familiar with the idea of roots of polynomials. In particular, if  $f(x) = ax^2 + bx + c$  is a polynomial of degree 2 with real coefficients, then the famous quadratic formula describes the roots of  $f(x)$  as a function of the coefficients  $a, b, c$  of  $f(x)$ :

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

This formula was in essence known to Euclid (300 B.C.).

The special case of the Remainder Theorem when  $a$  is a root of  $f(x)$  is called:

**Corollary 6.5** (Root Theorem) *If  $f(x)$  is a polynomial with coefficients in a field  $F$ , and  $a$  is in  $F$ , then  $f(a) = 0$  if and only if  $x - a$  divides  $f(x)$ .*

Returning to the example just above the Remainder Theorem,  $x - 1$  does not divide  $x^3 - 2$  because 1 is not a root of  $x^3 - 2$ .

But  $x - 1$  does divide  $f(x) = x^3 + x - 2$ , because  $f(1) = 0$ . In fact,

$$x^3 + x - 2 = (x - 1)(x^2 + x + 2).$$

### 6.3 D'Alembert's Theorem

The Root Theorem is a key to proving

**Theorem 6.6** (D'Alembert's Theorem) *Let  $F$  be a field. A nonzero polynomial  $f(x)$  of degree  $n$  has at most  $n$  distinct roots in  $F$ .*

To prove this, we recall from Chapter 5:

**Lemma 6.7** *A field has no zero divisors.*

*Proof* Recall that a field  $F$  is a commutative ring in which every non-zero element of  $F$  has an inverse in  $F$ . A zero divisor in  $F$  is a non-zero element  $a$  of  $F$  for which there is some non-zero element  $b$  of  $F$  so that  $ab = 0$ .

In Lemma 5.27 we proved that a unit of a commutative ring cannot be a zero divisor. Since every non-zero element of a field is a unit, no non-zero element of the field can be a zero divisor.

So a field cannot have zero divisors.  $\square$

Now we can prove D'Alembert's Theorem.

*Proof* We do this by induction on the degree  $n$  of  $f$ .

If  $\deg f = 0$ , then  $f$  is a nonzero constant polynomial, so has no roots in  $F$ .

Now suppose  $f$  is a polynomial of degree  $n > 0$ , and suppose it has exactly  $r$  distinct roots  $a_1, \dots, a_r$  in  $F$ . We must show that  $r \leq n$ .

Since  $f(a_r) = 0$ , by the Root Theorem,  $f(x)$  factors as

$$f(x) = (x - a_r)g(x),$$

where  $g(x)$  has degree  $n - 1$ . Now evaluate this last equation at each of the other roots  $x = a_i$  of  $f(x)$ , for  $i = 1, \dots, r - 1$ . We get

$$0 = f(a_i) = (a_i - a_r)g(a_i)$$

in  $F$ . Now as we just observed, a field has no zero divisors. So since  $a_i \neq a_r$ , we must have  $g(a_i) = 0$ . Hence each of  $a_1, \dots, a_{r-1}$  is a root of  $g(x)$ . But  $\deg g = n - 1$ , and so by induction, we can assume that  $g(x)$  has at most  $n - 1$  roots in  $F$ . Thus  $r - 1 \leq n - 1 = \deg g$ . Hence  $r \leq n = \deg f$ : the polynomial  $f(x)$  of degree  $n$  has at most  $n$  roots in  $F$ .  $\square$

We'll find D'Alembert's Theorem useful in several settings in this book. For example, it plays a critical role in proving the Primitive Root Theorem in Section 13.7, and in proving that the Reed–Solomon multiple error correcting code in Chapter 15 works as claimed.

Here we'll just look at a couple of immediate consequences.

**Corollary 6.8** *Let  $f(x)$  and  $g(x)$  be two polynomials with coefficients in a field  $F$ , each of degree  $\leq n$ . If  $f(a) = g(a)$  for at least  $n + 1$  distinct elements of  $F$ , then  $f(x) = g(x)$ .*

*Proof* Let  $f(x) = g(x) - h(x)$ . Then  $\deg h(x) \leq n$  and  $h(x)$  has at least  $n + 1$  roots in  $F$ . By D'Alembert's Theorem,  $h(x)$  cannot be a non-zero polynomial. So  $0 = h(x) = f(x) - g(x)$ , so  $f(x) = g(x)$ .  $\square$

The next result confirms an assertion earlier in the chapter about two polynomials being equal as functions.

**Corollary 6.9** *If  $F$  is a field with infinitely many elements and  $f(x)$  and  $g(x)$  are two polynomials with coefficients in  $F$ , then  $f(x)$  and  $g(x)$  are equal as polynomials with coefficients in  $F$  if and only if  $f(x) = g(x)$  as functions on  $F$ .*

*Proof* If  $f(x) = g(x)$  as polynomials, then for any element  $a$  of  $F$ ,  $f(a) = g(a)$ . That is,  $f(x)$  and  $g(x)$  are equal as functions on  $F$ .

Conversely, suppose  $f(x)$  and  $g(x)$  are two polynomials and let  $n \geq \deg(f)$  and  $n \geq \deg(g)$ . If  $f(a) = g(a)$  for all  $a$  in  $F$  and  $F$  is an infinite field, then  $f(a) = g(a)$  for more than  $n$  elements of  $F$ . By Corollary 6.8,  $f(x) = g(x)$ .  $\square$

The second immediate consequence of D'Alembert's Theorem is the foundation for a way of testing a number for primeness and possibly factoring the number.

**Corollary 6.10** *Let  $m > 2$ , let  $b$  be a non-zero element of  $\mathbb{Z}_m$  and let  $f(x) = x^2 - b^2$ , a polynomial with coefficients in  $\mathbb{Z}_m$ . If  $f(x)$  has more than two roots in  $\mathbb{Z}_m$ , then  $m$  is composite and easy to factor.*

*Proof* Suppose  $p$  is prime. Then  $x^2 - b^2 = (x + b)(x - b)$  in  $\mathbb{Z}_p[x]$ . Since  $\mathbb{Z}_p$  is a field when  $m$  is prime and  $x^2 - b^2$  has degree 2, D'Alembert's Theorem implies that  $b$  and  $-b$  are the only roots of  $x^2 - b^2$  in  $\mathbb{Z}_p$ .

Thus if there is a polynomial  $x^2 - b^2$  with coefficients in  $\mathbb{Z}_m$  that has a root  $c$  not equal to  $b$  or  $-b$ , then by D'Alembert's Theorem,  $\mathbb{Z}_m$  cannot be a field, and so  $m$  is composite.

To show that  $m$  is then easy to factor, we turn the problem into one of solving a congruence modulo  $m$ : Finding a root of  $x^2 - b^2$  in  $\mathbb{Z}_m$  is the same as finding a solution of the congruence

$$x^2 - b^2 \equiv 0 \pmod{m}.$$

Suppose  $c$  is a solution of this congruence and  $c$  is not congruent to either  $b$  or  $-b$  modulo  $m$ . Then

$$c^2 - b^2 \equiv 0 \pmod{m},$$

so

$$m \text{ divides } c^2 - b^2 = (c + b)(c - b),$$

but  $m$  does not divide  $c + b$  or  $c - b$ . This then implies that  $(m, c + b) > 1$  and  $(m, c - b) > 1$ . For by the Coprime Divisibility Lemma, if  $m$  were coprime to  $c + b$ , then  $m$  would divide  $c - b$ . Similarly, if  $m$  were coprime to  $c - b$ , then  $m$  would divide  $c + b$ .

Thus  $(m, c - b)$  and  $(m, c + b)$  are each non-trivial factors of  $m$ . Computing those greatest common divisors is easy to do, using Euclid's Algorithm.  $\square$

*Example 6.11* Let  $m = 91$ . The congruence

$$x^2 \equiv 25 \pmod{91}$$

has a solution  $x = 47$ . So  $91$  divides  $47^2 - 5^2 = (47 + 5)(47 - 5) = 52 \cdot 42$ . (In fact,  $52 \cdot 42 = 2184 = 91 \cdot 24$ .) But  $91$  does not divide  $52$  or  $42$ . So  $(91, 52) = 13$  and  $(91, 42) = 7$  are both factors of  $91$ .

This result is the starting point for some factoring algorithms, which seek to find numbers  $b$  for which there is some solution  $x = a$  of  $x^2 \equiv b^2$  modulo  $m$  with  $a \not\equiv b$  or  $-b$  modulo  $m$ . See Sections 17.2 and 17.3.

## Exercises

- 6.1. Show that  $f(x) = x$  and  $g(x) = x^3$  in  $\mathbb{Z}_3[x]$  are equal as functions on the field  $\mathbb{Z}_3$ .
- 6.2. Find the units and zero divisors of  $\mathbb{Z}_4[x]$ . (Hint: try using that if  $f(x)g(x) = 1$ , resp. 0, then  $f(a)g(a) = 1$ , resp. 0, for all  $a$  in  $\mathbb{Z}_4$ .)
- 6.3. (i) Write down the zero divisors of  $\mathbb{Z}_{12}$ . For each zero divisor  $b$ , find all of the complementary zero divisors of  $b$ , that is, all of the non-zero numbers  $c$  of  $\mathbb{Z}_{12}$  so that  $bc = 0$ .  
(ii) Find two non-zero polynomials  $f$  and  $g$  in  $\mathbb{Z}_{12}[x]$  so that  $\deg(fg) < \deg(f) + \deg(g)$ .
- 6.4. Find the quotient  $q$  and the remainder  $r$  in the Division Theorem equation  $g = fq + r$  for  $f$  and  $g$  in  $\mathbb{Q}[x]$  when
  - (i)  $g = x^3 - 3x^2 - 1$ ;  $f = x - 2$ ;
  - (ii)  $g = x^4 - 6x^2 - 1$ ;  $f = x^2 + 3x - 1$ ;
  - (iii)  $g = 3x^3 - x^2 + 1$ ;  $f = x$ ;
  - (iv)  $g = x^3 + 4x + 8$ ;  $f = 2$ ;
  - (v)  $g = 3x^2 - x - 1$ ;  $f = x^3 - 2$ .

- 6.5. Without using long division of polynomials, find the remainder in the Division Theorem (in  $\mathbb{Q}[x]$ ) when:

- (i)  $x^3 - 2x + 1$  is divided by  $x - 3$ ;
- (ii)  $x^4 - 8x^2 + 3$  is divided by  $x - 1$ ;
- (iii)  $x^{32} - x^{12} + 2$  is divided by  $x^4 + 1$ .

- 6.6. For which values of  $k$  in  $\mathbb{Q}$  does  $x - k$  divide  $x^3 - kx^2 - 2x + k + 3$ ?

- 6.7. Show that for  $m < n$ , if  $n = mq + r$  with  $r < m$ , then

$$x^n - 1 = (x^m - 1)(x^{n-m} + x^{n-2m} + \dots + x^{n-qm}) + (x^r - 1).$$

- 6.8. (i) Show that if a polynomial  $f(x)$  of degree 3 in  $F[x]$ ,  $F$  a field, factors into a product of polynomials of degree  $< 3$ , then  $f(x)$  has a root in  $F$ .  
(ii) Give an example of a field  $F$  and a polynomial of degree 4 which factors into a product of polynomials of degrees  $< 4$  but which has no root in  $F$ .

- 6.9. Let  $F = \mathbb{Z}_p$  with  $p$  an odd prime. Let

$$f(x) = ax^2 + bx + c$$

in  $F[x]$  with  $a \neq 0$  in  $F$ . Show that  $f(x)$  has a root in  $F$  if and only if  $b^2 - 4ac$  is a square in  $F$ .

- 6.10. Is Exercise 6.9 true if  $p = 2$ ?

- 6.11. Using the fact that  $37559^2 = 1410678481 = 1 + 21360 \cdot 66043$ , factor 66043.

- 6.12. Let  $m = 3013$ . Suppose you know that

$$392^2 \equiv 1 \pmod{m}.$$

Use that fact to factor  $m$  with the aid of Euclid's algorithm.

- 6.13. Find a polynomial of degree 2 with coefficients in  $\mathbb{Z}_6$  with at least three roots in  $\mathbb{Z}_6$ .

- 6.14. Suppose  $m > 4$  and  $m = ab$  with  $1 < a, b < m$ . Find a polynomial of degree 2 with coefficients in  $\mathbb{Z}_m$  with at least four roots in  $\mathbb{Z}_m$ .

# Chapter 7

## Matrices and Hamming Codes



In this chapter we use the field  $\mathbb{F}_2 = \mathbb{Z}_2$  of two elements to construct two related single-error correcting codes. These are called Hamming codes, because they were invented by Richard Hamming of Bell Labs and published in 1950.

Hamming codes were the first efficient codes that can actually correct errors, unlike parity check schemes like the Luhn code (Section 1.4) or Hamming's own check digit scheme (Exercise 8 in Chapter 1) that are efficient but can only detect an error, or the triple modular redundancy code (Chapter 1), which corrects one error but is inefficient.

Error correction has advanced considerably since 1950, but Hamming codes continue to be used in settings such as in computer data storage, where errors are rare but can occur because of background or cosmic ray radiation, or because of manufacturing defects. See [Wikipedia, ECC memory, retrieved 4/19/17.]

The construction of Hamming codes uses some elementary matrix theory. So in the first section of this chapter we review some basic ideas about matrices, vectors and systems of linear equations. Matrix theory and elementary linear algebra will also be needed in later chapters, particularly in Chapters 15 and 19 for Reed–Solomon codes, in Chapter 17 for the Quadratic Sieve and Index Calculus algorithms, and in some examples in Section 14.1.

### 7.1 Matrices and Vectors

For readers who have studied linear algebra, the message of this section is:

**Theorem 7.1** *The elementary theory of matrices and determinants, and the theory of vector spaces, including subspaces, spanning, linear independence, bases and dimension, are valid when the field of coefficients is  $\mathbb{F}_2$  (or any other field).*

To check this, browse through an elementary linear algebra textbook. The first time one actually needs the field of real numbers in an elementary linear algebra course is in the theory of orthogonality (orthogonal bases, Gram–Schmidt, projections, etc.), and in the theory of eigenvectors and eigenvalues, where one encounters the theorem that given a symmetric  $n \times n$  matrix  $A$  with real entries there is an orthonormal basis of real  $n$ -space consisting of eigenvectors of  $A$ .

If you haven't had any linear algebra, don't worry, but do read this section carefully. It will make the rest of this chapter and material in some later chapters easier to follow.

Let  $R$  be a commutative ring (like  $\mathbb{R}$  or  $\mathbb{F}_2$  or  $\mathbb{Z}$ ).

**Definition** A *column vector* is a column of elements of  $R$ :

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

A *row vector* is a row of elements of  $R$ :

$$(a_1 \ a_2 \ \cdots \ a_n).$$

The entries of a vector are often called the *components* of the vector:  $a_1$  is the first component,  $\dots$ ,  $a_r$  is the  $r$ -th component, etc.

An  $m \times n$  matrix is a rectangular array of  $mn$  elements of  $R$ :

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

which can be thought of as a collection of row vectors placed in a column, or a collection of column vectors laid out in a row. For example,

$$\begin{pmatrix} 1 & 2 & 3 \\ 5 & 7 & 9 \end{pmatrix} = \begin{pmatrix} (1 & 2 & 3) \\ (5 & 7 & 9) \end{pmatrix} = \begin{pmatrix} (1) & (2) & (3) \\ (5) & (7) & (9) \end{pmatrix}.$$

When we say that a matrix is  $m \times n$ , the first number  $m$  is always the number of rows, and the second number  $n$  is the number of columns.

Given the column vector

$$\mathbf{v} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix},$$

the row vector

$$\mathbf{w} = (a_1 \ a_2 \ \cdots \ a_n)$$

is the *transpose* of  $\mathbf{v}$ , written  $\mathbf{w} = \mathbf{v}^T$ . Similarly,  $\mathbf{v} = \mathbf{w}^T$ . The notation  $( )^T$  is read "the transpose of". In words, the transpose of a row vector is the column vector with the same components, and the transpose of a column vector is the row vector with the same components. So  $(\mathbf{v}^T)^T = \mathbf{v}$ .

Transpose notation is useful for writing down column vectors using a normal keyboard. Thus  $(2, 4)^T$  means the column vector  $\begin{pmatrix} 2 \\ 4 \end{pmatrix}$ .

**Matrix multiplication.** Given a row vector with  $n$  elements of a commutative ring  $R$  (placed on the left) and a column vector with the same number of elements (placed on the right), we may multiply them to get an element of the ring  $R$ , as follows:

$$(a_1 \ a_2 \ \cdots \ a_n) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.$$

Here are some examples where  $R = \mathbb{Z}$ :

$$\begin{aligned} (3 \ 2 \ 5) \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix} &= 2, \\ (-3 \ 2) \begin{pmatrix} 1 \\ 2 \end{pmatrix} &= 1, \\ (3) (5) &= 15. \end{aligned}$$

Matrix multiplication involves a set of row-column multiplications.

To begin, given an  $m \times n$  matrix  $\mathbf{A}$ , we can multiply  $\mathbf{A}$  (placed on the left) and an  $n$ -element column vector  $\mathbf{w}$  (placed on the right) by thinking of the matrix as a collection of  $m$  row vectors, each containing  $n$  elements, and doing  $m$  multiplications of the row vectors of  $\mathbf{A}$  with  $\mathbf{w}$ . The result,  $\mathbf{Aw}$ , is a column of  $m$  elements. Some examples:

$$\begin{aligned} \begin{pmatrix} 1 & 2 \\ 2 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} -1 \\ 2 \end{pmatrix} &= \begin{pmatrix} (1 & 2) \\ (2 & 4) \\ (2 & 3) \end{pmatrix} \begin{pmatrix} -1 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \\ 4 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} &= \begin{pmatrix} (1 & 2 & 3) \\ (0 & 0 & 1) \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix}. \end{aligned}$$

Given an  $m \times n$  matrix  $\mathbf{A}$  (on the left) and an  $n \times p$  matrix  $\mathbf{B}$  (on the right), we can multiply  $\mathbf{A}$  and  $\mathbf{B}$  by thinking of  $\mathbf{A}$  as a collection of  $n$ -element rows and  $\mathbf{B}$  as a collection of  $n$ -element columns. The result,  $\mathbf{AB}$ , is an  $m \times p$  matrix whose element in the  $i$ th row and  $j$ th column is obtained by multiplying the  $i$ th row of  $\mathbf{A}$  and the  $j$ th column of  $\mathbf{B}$ . Thus

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \\ 1 & 3 \end{pmatrix} &= \begin{pmatrix} (1 & 2 & 1) \\ (2 & 3 & 0) \end{pmatrix} \begin{pmatrix} (2) & (1) \\ (0) & (1) \\ (1) & (3) \end{pmatrix} \\ &= \begin{pmatrix} (1 & 2 & 1) \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} & (1 & 2 & 1) \begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix} \\ (2 & 3 & 0) \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} & (2 & 3 & 0) \begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} 3 & 6 \\ 4 & 5 \end{pmatrix}. \end{aligned}$$

Other examples:

$$\begin{pmatrix} 1 \\ 3 \end{pmatrix} (1 \ 2 \ 5) = \begin{pmatrix} 1 & 2 & 5 \\ 3 & 6 & 15 \end{pmatrix};$$

$$\begin{pmatrix} 2 & 1 \\ 0 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ 4 & 5 \\ 12 & 16 \end{pmatrix}.$$

Notice that *the order in which the matrices are multiplied* (i.e., which matrix is on the left and which is on the right) is very important. In the last examples,

$$(1 \ 2 \ 5) \begin{pmatrix} 1 \\ 3 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 4 & 5 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \\ 1 & 3 \end{pmatrix}$$

make no sense, because they would require multiplying a row vector and a column vector with different numbers of elements. Even when it makes sense to multiply in either order, the results are usually different: compare

$$\begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix} (1 \ 2 \ 5) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 2 & 5 \\ 3 & 6 & 15 \end{pmatrix},$$

a  $3 \times 3$  matrix, with

$$(1 \ 2 \ 5) \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix} = (17),$$

a  $1 \times 1$  matrix; or compare the two products

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

In short, matrix multiplication is (usually) not commutative.

**Definition** The  $n \times n$  identity matrix  $\mathbf{I}$  is the matrix whose entries are 1 along the main diagonal (from upper left to lower right) and 0 elsewhere.

The matrix  $\mathbf{I}$  has the property that for any  $n$ -rowed column vector  $\mathbf{B}$ , hence for any  $n \times p$  matrix  $\mathbf{B}$ ,  $\mathbf{IB} = \mathbf{B}$ . This is easily verified for  $n = 2$ :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \cdot a + 0 \cdot b \\ 0 \cdot a + 1 \cdot b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

**Vector addition and scalar multiplication.** We add column vectors with equal numbers of components by

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix}.$$

We multiply a column vector by a scalar (an element of the ring  $R$ ), by

$$r \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ ra_2 \\ \vdots \\ ra_n \end{pmatrix}.$$

Thus adding vectors or multiplying a vector by a scalar is done by doing it on each of the  $n$  components of the vector, or as we say, componentwise. If

$$\mathbf{a} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

and  $r$  and  $s$  are some scalars, then an expression of the form

$$r\mathbf{a} + s\mathbf{b},$$

whose  $k$ th component is  $ra_k + sb_k$  for  $k = 1, \dots, n$ , is called a *linear combination* of  $\mathbf{a}$  and  $\mathbf{b}$ .

*Example 7.2*

$$\begin{aligned} 7 \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} + (-8) \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} &= \begin{pmatrix} 7 \cdot 1 + (-8) \cdot 2 \\ 7 \cdot 3 + (-8) \cdot 4 \\ 7 \cdot 5 + (-8) \cdot 6 \end{pmatrix} \\ &= \begin{pmatrix} 7 - 16 \\ 21 - 32 \\ 35 - 48 \end{pmatrix} \\ &= \begin{pmatrix} -9 \\ -11 \\ -13 \end{pmatrix}. \end{aligned}$$

*Example 7.3* Linear combinations of row vectors showed up in Section 3.4 in the Extended Euclidean Algorithm. For example, from Euclid's Algorithm for 85 and 37, we found that

$$\begin{aligned} 11 &= 1 \cdot 85 - 2 \cdot 37 \\ 4 &= -3 \cdot 85 + 7 \cdot 37 \\ 3 &= 7 \cdot 85 - 16 \cdot 37. \end{aligned}$$

These corresponded to the vectors

$$\begin{aligned} (11, 1, -2) \\ (4, -3, 7) \\ (3, 7, -16), \end{aligned}$$

where the center and right components of the vector are the coefficients when we write the left component as an integer linear combination of 85 and 37, respectively.

In fact, we found the vector  $(3, 7, -16)$  from the other two vectors by observing that  $3 = 11 - 2 \cdot 4$ , and so computing  $(11, 1, -2) - 2(4, -3, 7)$  yields the vector for 3.

Suppose we want to write  $10 = a \cdot 85 + b \cdot 37$  for some integers  $a$  and  $b$ . If we can find some way of writing 10 as an integer linear combination of 11, 4 and 3, then we can compute the corresponding linear combination of vectors to find an  $a$  and  $b$ . For example:

Since  $4 + 2 \cdot 3 = 10$ , we compute

$$(4, -3, 7) + 2(3, 7, -16) = (10, 11, -25),$$

so  $10 = 11 \cdot 85 + (-25) \cdot 37$ .

Since  $2 \cdot 11 - 4 \cdot 3 = 10$ , we compute

$$2(11, 1, -2) - 4(3, 7, -16) = (10, -26, 60),$$

so  $10 = (-26) \cdot 85 + 60 \cdot 37$ .

Since  $6 \cdot 3 - 2 \cdot 4 = 10$ , we compute

$$6(3, 7, -16) - 2(4, -3, 7) = (10, 48, -110),$$

so  $10 = 48 \cdot 85 - 110 \cdot 37$ .

In this way we get three of the infinitely many solutions of  $10 = a \cdot 85 + b \cdot 37$ .

The next fact is helpful in understanding error correcting codes later in this chapter.

**Proposition 7.4** *If  $\mathbf{A}$  is a matrix with columns  $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$  and  $\mathbf{v}$  is a column vector*

$$\mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix},$$

*then the product  $\mathbf{Av}$  is a linear combination of the columns of  $\mathbf{A}$ , namely,*

$$\mathbf{Av} = v_1 \mathbf{a}_1 + v_2 \mathbf{a}_2 + \dots + v_n \mathbf{a}_n.$$

*Example 7.5*

$$\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 7 \\ 6 \end{pmatrix} = \begin{pmatrix} 1 \cdot 7 + 3 \cdot 6 \\ 2 \cdot 7 + 4 \cdot 6 \end{pmatrix},$$

while

$$7 \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} + 6 \cdot \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 7 \cdot 1 + 6 \cdot 3 \\ 7 \cdot 2 + 6 \cdot 4 \end{pmatrix}.$$

*Example 7.6* Let  $\mathbb{Z}_2 = \{0, 1\}$  be the field of coefficients. Let

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Then

$$\mathbf{Hv} = \mathbf{H} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0+0+1+0+0+0+0 \\ 0+0+1+0+0+1+0 \\ 0+0+0+0+0+1+0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix},$$

while the corresponding linear combination of columns of  $\mathbf{H}$  is

$$0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

This example will appear in Section 7.2, below.

Proposition 7.4 is proved by generalizing the examples: just write both the left side  $\mathbf{Av}$  and the right side  $v_1\mathbf{a}_1 + \dots + v_n\mathbf{a}_n$  as a single column vector, as in Example 7.5.

**Corollary 7.7** *Let  $\mathbf{v} = (v_1, \dots, v_n)^T$  (a column vector), and let*

$$\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$$

*be an  $m \times n$  matrix (so that  $\mathbf{a}_j$  is a column vector with  $m$  components). Then  $\mathbf{Av} = 0$  if and only if*

$$v_1\mathbf{a}_1 + v_2\mathbf{a}_2 + \dots + v_n\mathbf{a}_n = 0.$$

Matrix multiplication gets along with addition of column vectors (the distributive law):

$$\mathbf{A}(\mathbf{u} + \mathbf{v}) = \mathbf{Au} + \mathbf{Av}$$

as can be checked by first doing it for  $\mathbf{A}$  a  $1 \times n$  matrix and then generalizing to the  $m \times n$  case. For example,

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \left( \begin{pmatrix} 3 \\ 1 \end{pmatrix} + \begin{pmatrix} 8 \\ 9 \end{pmatrix} \right) = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 11 \\ 10 \end{pmatrix} = \begin{pmatrix} 31 \\ 73 \end{pmatrix}$$

while

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 8 \\ 9 \end{pmatrix} = \begin{pmatrix} 5 \\ 13 \end{pmatrix} + \begin{pmatrix} 26 \\ 60 \end{pmatrix} = \begin{pmatrix} 31 \\ 73 \end{pmatrix}.$$

Matrix multiplication also gets along with scalar multiples of column vectors:

$$\mathbf{A}(r\mathbf{u}) = r\mathbf{Au}$$

and so matrix multiplication gets along with linear combinations of vectors:

$$\mathbf{A}(r\mathbf{u} + s\mathbf{v}) = r\mathbf{A}(\mathbf{u}) + s\mathbf{A}(\mathbf{v}).$$

Matrix multiplication also satisfies properties of multiplication of ordinary numbers, such as associativity:

$$\mathbf{A}(\mathbf{B}\mathbf{C}) = (\mathbf{AB})\mathbf{C}$$

and distributivity:

$$\mathbf{A}(\mathbf{B} + \mathbf{C}) = \mathbf{AB} + \mathbf{AC}$$

when the addition of matrices is defined (that is,  $\mathbf{B}$  and  $\mathbf{C}$  have the same size), and the multiplication is defined (that is, when the number of columns of the matrix on the left is equal to the number of rows of the matrix on the right).

But matrix multiplication (usually) does not satisfy commutativity, as we observed above.

**Systems of linear equations.** Matrices and matrix multiplication show up in connection with systems of linear equations.

*Example 7.8* Suppose we have the system

$$\begin{array}{rcl} 3x + 4y & + 5z & = 6 \\ x & - z & = -3. \end{array}$$

We can write this as an equality of column vectors:

$$\begin{pmatrix} 3x + 4y + 5z \\ x - z \end{pmatrix} = \begin{pmatrix} 6 \\ -3 \end{pmatrix}$$

and then recognize the vector on the left side as the result of multiplying the column vector  $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$  by the *matrix of coefficients*:

$$\begin{pmatrix} 3 & 4 & 5 \\ 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 6 \\ -3 \end{pmatrix}.$$

So a system of linear equations translates into a matrix equation. Conversely, if we have a matrix equation, such as

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ a \\ z \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

(where the  $3 \times 7$  matrix is the matrix  $\mathbf{H}$  in Example 7.6, above), multiplying out the left side, and then equating corresponding components of the resulting vectors on the left and right sides of the equation, yields the system of equations

$$\begin{aligned}x + a + b + d &= 0 \\y + a + c + d &= 0 \\z + b + c + d &= 0.\end{aligned}$$

The matrix  $\mathbf{H}$  is the matrix of coefficients of this system of equations.

A system of linear equations is *homogeneous* if the constants on the right-hand side of the equations are all zero.

The fact, above, that matrix multiplication respects linear combinations of vectors, implies that if we have two solutions  $\mathbf{u}$  and  $\mathbf{v}$  of a set of homogeneous equations, then any linear combination of the two solutions is also a solution of the set of homogeneous equations. For if  $\mathbf{A}$  is the matrix of coefficients of the set of equations, and if  $\mathbf{Au} = \mathbf{0}$  and  $\mathbf{Av} = \mathbf{0}$ , then for all scalars  $r$  and  $s$ ,

$$\mathbf{A}(r\mathbf{u} + s\mathbf{v}) = r\mathbf{Au} + s\mathbf{Av} = r \cdot \mathbf{0} + s \cdot \mathbf{0} = \mathbf{0} :$$

the set of solutions of a system of homogenous linear equations is closed under taking linear combinations. In particular, if  $\mathbf{Au} = \mathbf{0}$  and  $\mathbf{Av} = \mathbf{0}$ , then  $\mathbf{A}(\mathbf{u} + \mathbf{v}) = \mathbf{0}$ : the sum of two vectors multiplied to  $\mathbf{0}$  by  $\mathbf{A}$  is also multiplied to  $\mathbf{0}$  by  $\mathbf{A}$ .

**Definition** The set of vectors  $\mathbf{w}$  so that  $\mathbf{Aw} = \mathbf{0}$  is called the *null space* of  $\mathbf{A}$ .

If  $\mathbf{A}$  is the matrix of coefficients of a homogenous system of linear equations, then the null space of  $\mathbf{A}$  is the set of vectors whose components are a solution of the system of equations.

Assume for the rest of this chapter that the commutative ring  $R$  is a field, which we'll call  $\mathbb{F}$ .

**Proposition 7.9** *The null space  $\mathcal{C}$  of an  $m \times n$  matrix  $\mathbf{A}$  is a group under addition of vectors.*

*Proof* If  $\mathbf{Av} = \mathbf{0}$  and  $\mathbf{Aw} = \mathbf{0}$ , then

$$\mathbf{A}(\mathbf{v} + \mathbf{w}) = \mathbf{Av} + \mathbf{Aw} = \mathbf{0} + \mathbf{0} = \mathbf{0}.$$

If  $\mathbf{Av} = \mathbf{0}$ , then

$$\mathbf{A}(-\mathbf{v}) = -\mathbf{Av} = -\mathbf{0} = \mathbf{0}.$$

So the null space  $\mathcal{C}$  is closed under addition. The addition is associative and commutative, the zero vector  $\mathbf{0}$  is in  $\mathcal{C}$ , and the negative of any vector in  $\mathcal{C}$  is also in  $\mathcal{C}$ . So  $\mathcal{C}$  is a group. (Since we're assuming that the coefficients of  $\mathbf{A}$  are from a field  $\mathbb{F}$ ,  $\mathcal{C}$  is also a subspace of the  $\mathbb{F}$ -vector space of all vectors with  $n$  components from the field  $\mathbb{F}$ , but in this chapter we will only need that  $\mathcal{C}$  is closed under addition and negatives.)  $\square$

## 7.2 Error Correcting and Detecting Codes

We introduced the idea of error detecting and correcting in Chapter 1. Alice has a message that she wants to send to Bob through a communication channel. The channel is “noisy”: a random digit may be changed with low but non-zero probability. So Bob may receive Alice's message with errors. If there aren't too many errors, how can Bob determine what Alice sent?

The basic idea for the solution is for Alice to send Bob messages with redundant data, that is, messages with additional digits, but in a certain special pattern, or format. Bob can detect, or even

correct errors in the digits of the message he received, by seeing how what he received varies from the special pattern that Alice created for her original message before sending it.

In Chapter 1 we saw two examples: error detection schemes that use a check digit such as the Luhn formula for credit card numbers, and the repetition code.

In designing an error detecting or correcting code, the *efficiency* of the code is the ratio

$$\frac{\text{\# of information digits}}{\text{\# of code vector digits}}.$$

Then  $0 < \text{efficiency} \leq 1$ .

If the efficiency is near 1, then nearly all of an encoded word is information, with very little redundancy, while if the efficiency is near 0, then most of an encoded word is redundancy, and the transmission of information is slowed down.

The Luhn formula for credit cards discussed in Chapter 1 has efficiency  $\frac{15}{16}$ . Only the check digit is redundant. The Luhn formula detects one error.

The repetition code, to send 0 (or 1), send 00000 (or 11111), has efficiency  $\frac{1}{5}$ . It corrects up to two errors.

Error correcting codes typically assume that errors are uncommon. So a desirable code is one with efficiency close to 1 that is capable of correcting a small number of errors among the digits of each word.

In the rest of this chapter we describe two examples of efficient codes constructed using matrices with entries in the field  $\mathbb{F}_2 = \{0, 1\}$  (so  $1 + 1 = 0$ ). These codes are known as Hamming codes, after their inventor, R.W. Hamming of Bell Telephone Laboratories [Ham50].

So we will assume that all messages or information words are sequences of vectors of bits–0's and 1's, that is, vectors with entries in the field  $\mathbb{F}_2$ . (See Section 2.4 for a discussion on converting ordinary text into sequences of bits.)

### 7.3 The Hamming (7, 4) Code: A Single Error Correcting Code

We work with elements of  $\mathbb{F}_2 = \{0, 1\}$ . Recall that in  $\mathbb{F}_2$ ,  $1 + 1 = 0$ , so  $1 = -1$  and addition is the same as subtraction.

The Hamming (7, 4) code takes plaintext words with four bits and turns the plaintext words into code words with containing seven bits. The encoding introduces three bits of redundancy. The redundancy enables the receiver to detect and correct an error in one bit in the transmission of the coded word.

In this section we explain how to encode and decode the Hamming (7, 4) code.

Let

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

The  $r$ th column of the matrix  $\mathbf{H}$  represents  $r$  in base 2:

$$\begin{pmatrix} r \\ s \\ t \end{pmatrix}$$

is the  $r + 2s + 4t$ -th column of  $\mathbf{H}$ . Thus the sixth column is  $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$  and  $(0, 1, 1)$  translates to  $0 \cdot 1 + 1 \cdot 2 + 1 \cdot 4 = 6$ . So each column of  $\mathbf{H}$  describes its own location in the matrix  $\mathbf{H}$ . (Note: we choose  $(r, s, t)$  to correspond to  $r + 2s + 2^2t$ , with increasing powers of 2, so that the corresponding matrix  $\mathbf{H}$  is in reduced row echelon form.)

**Encoding.** Suppose Alice wishes to send the vector  $\mathbf{W} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ , where  $a, b, c, d$  are in  $\mathbb{F}_2$ . Call  $\mathbf{W}$  the information word. Alice embeds  $\mathbf{W}$  in a code vector

$$\mathbf{C} = \begin{pmatrix} x \\ y \\ a \\ z \\ b \\ c \\ d \end{pmatrix}$$

by choosing  $x, y, z$  so that

$$\mathbf{HC} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ a \\ z \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

This translates into the equations

$$\begin{aligned} x + a + b + d &= 0, \\ y + a + c + d &= 0, \\ z + b + c + d &= 0. \end{aligned}$$

or (since  $- = +$  in  $\mathbb{F}_2$ )

$$\begin{aligned} x &= a + b + d, \\ y &= a + c + d, \\ z &= b + c + d. \end{aligned}$$

Here  $(x, y, z)$  is the redundant part of the coded vector. Thus Alice finds the coded vector  $\mathbf{C}$  from  $(a, b, c, d)$  by substituting for  $x, y, z$  in  $\mathbf{C}$ :

$$\mathbf{C} = \begin{pmatrix} x \\ y \\ a \\ z \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a + b + d \\ a + c + d \\ a \\ b + c + d \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}.$$

So  $\mathbf{C}$  can be found from  $\mathbf{W}$  by recognizing that  $\mathbf{C}$  is the result of multiplying the information word  $\mathbf{W}$  by the  $7 \times 4$  matrix

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The code vector  $\mathbf{C}$  is made up of the bits  $a, b, c, d$  in the information word  $\mathbf{W} = (a, b, c, d)^T$  and the redundant bits  $x, y, z$ . Alice sends the code vector  $\mathbf{C}$  to Bob using a possibly noisy channel.

The key idea that Bob uses to decode what he receives from Alice is that every code word  $\mathbf{C}$  satisfies

$$\mathbf{H}\mathbf{C} = \mathbf{0}.$$

**Decoding.** Suppose Bob receives

$$\mathbf{R} = \begin{pmatrix} x' \\ y' \\ a' \\ z' \\ b' \\ c' \\ d' \end{pmatrix}.$$

He assumes that  $\mathbf{R}$  has either no errors or one error. To decide which, Bob computes  $\mathbf{H}\mathbf{R}$ . Then  $\mathbf{H}\mathbf{R}$  is either the zero vector, or not.

Case 0. Suppose  $\mathbf{H}\mathbf{R} = \mathbf{0}$ . Then Bob decides that no error occurred, so that  $\mathbf{R} = \mathbf{C}$ , because for every code vector  $\mathbf{C}$ ,  $\mathbf{H}\mathbf{C} = \mathbf{0}$ , while if  $R$  contained one error in it,  $\mathbf{H}\mathbf{R}$  would not be the zero vector.

For example, suppose Bob receives  $\mathbf{R} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ . He finds that

$$\mathbf{H}\mathbf{R} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

So Bob decides that  $\mathbf{C} = \mathbf{R}$ : the word  $\mathbf{R}$  that he received was the word that Alice sent. He can then pick off the word Alice wants to send by stripping off the redundant digits  $x, y, z$ , to get  $\mathbf{W} = (a, b, c, d) = (0, 0, 1, 0)$ , the 3rd, 5th, 6th and 7th bits of  $\mathbf{C}$ .

Case 1. If Bob computes  $\mathbf{HR}$  and doesn't get the zero vector, then he obtains a column of  $\mathbf{H}$ . Then Bob decides there is one error in  $\mathbf{R}$ , and changes the component of  $\mathbf{R}$  corresponding to the column of  $\mathbf{H}$  (so if, for example  $\mathbf{HR}$  is equal to the third column of  $H$ , then Bob changes the third entry of  $\mathbf{R}$ ).

To see why, suppose one component of  $\mathbf{C}$  was changed in the transmission, so that  $\mathbf{R}$  differs from  $\mathbf{C}$  in a single bit. Then  $\mathbf{R} = \mathbf{C} + \mathbf{E}$  where  $\mathbf{E}$  is a column vector with a single 1 in the component where the error occurred, and all other components are 0. So  $\mathbf{HE}$  is the column of  $\mathbf{H}$  corresponding to the location of the 1 in the vector  $\mathbf{E}$ .

For example, if

$$\mathbf{E} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

then

$$\mathbf{HE} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

as can be seen by doing the matrix multiplication or by referring back to Proposition 7.4.

When Bob computes  $\mathbf{HR}$ , he gets (using the distributive law for matrix multiplication):

$$\begin{aligned} \mathbf{HR} &= \mathbf{HC} + \mathbf{HE} \\ &= \mathbf{0} + \mathbf{HE} \\ &= \mathbf{HE} \\ &= (\text{the column of } \mathbf{H} \text{ corresponding to where the 1 is in } \mathbf{E}). \end{aligned}$$

Thus, if Bob assumes that there is one error, Bob can determine where the error is, because  $\mathbf{HR}$  is equal to the column of  $\mathbf{H}$  corresponding to the location of the incorrect entry in  $\mathbf{R}$ .

Once he finds where the error is, he changes that bit of  $\mathbf{R}$  to get  $\mathbf{C}$ , the encoded word that Alice transmitted.

*Example 7.10* Suppose Bob receives

$$\mathbf{R} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}. \text{ Then } \mathbf{HR} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}. \text{ So}$$

$$\mathbf{HR} = \mathbf{HE} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \text{ the last column of } \mathbf{H}.$$

Bob assumes that one error occurred, so that  $\mathbf{E}$  has a single non-zero component. Then the non-zero component of  $\mathbf{E}$  is the last component. Changing the last component of  $\mathbf{R}$  gives  $\mathbf{C}$ :

$$\mathbf{E} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \text{ and } \mathbf{C} = \mathbf{R} - \mathbf{E} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Suppose Bob receives  $\mathbf{R} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ . Then  $\mathbf{H}\mathbf{R} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ , the sixth column of  $\mathbf{H}$ . Assuming one error, Bob concludes that the only 1 in  $\mathbf{E}$  is in the sixth component:

$$\mathbf{E} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \text{ and so } \mathbf{C} = \mathbf{R} - \mathbf{E} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Suppose Bob receives  $\mathbf{R} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ , then  $\mathbf{H}\mathbf{R} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ , the third column of  $\mathbf{H}$ , so Bob changes the third component of  $\mathbf{R}$  to get  $\mathbf{C} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ .

Case 2. What happens if  $\mathbf{R}$  differs from  $\mathbf{C}$  in two or more entries? Then Bob will be misled. For

$$\begin{aligned} \mathbf{H}\mathbf{R} &= \mathbf{H}\mathbf{C} + \mathbf{H}\mathbf{E} \\ &= \mathbf{0} + (\text{sum of two or more columns of } \mathbf{H}). \end{aligned}$$

Since the sum of two or more columns of  $\mathbf{H}$  is either  $\mathbf{0}$  or a column of  $\mathbf{H}$ , Bob will decode inaccurately because he is assuming that no errors or one error occurred.

*Example 7.11* Suppose

$$\mathbf{C} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}.$$

Then  $\mathbf{H}\mathbf{C} = \mathbf{0}$ . If

$$\mathbf{R} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

then

$$\mathbf{E} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

and

$$\mathbf{HR} = \mathbf{HE} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},$$

the sixth column of  $\mathbf{H}$ . So Bob, thinking that one error occurred, will decide that

$$\mathbf{C} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

He will decode incorrectly.

The bottom line with this code is that when using it, Bob is capable of correcting exactly one error, but he will be misled whenever more than one error occurs in a given word.

Suppose  $p$ , the probability of an error in any given digit, is  $p = 0.01$ , and the probability of an error in some digit is independent of the probability of an error in any other digit. Then the probability of at most one error in a word is  $e = (1 - 0.01)^7 + 7(1 - 0.01)^6(0.01) = 0.998$ , so there is an 0.2 percent chance (two tenths of one percent chance) that Bob will be misled on each word.

The efficiency of this code is  $4/7$ .

## 7.4 The Hamming (8, 4) Code

Including one more redundant bit in the Hamming (7, 4) code will enable Bob to detect the presence of two errors, as well as to correct one error.

For the Hamming (8, 4) code we let

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

the matrix of the Hamming (7, 4) code with an additional column of zeros on the left and then a row of 1's on the top.

Alice wishes to send Bob the information word  $\mathbf{W} = (a, b, c, d)$ . To encode  $\mathbf{W}$ , she finds bits  $w, x, y, z$  so that the vector

$$\mathbf{C} = \begin{pmatrix} w \\ x \\ y \\ a \\ z \\ b \\ c \\ d \end{pmatrix}$$

satisfies  $\mathbf{HC} = \mathbf{0}$ . The resulting equations for  $x, y, z$  are the same as in the Hamming (7, 4) code:

$$\begin{aligned} x &= a + b + d, \\ y &= a + c + d, \\ z &= b + c + d. \end{aligned}$$

The equation for  $w$  is

$$0 = w + x + y + z + a + b + c + d.$$

But substituting for  $x, y$  and  $z$  in this equation, we obtain the simpler equation for  $w$ :

$$w = a + b + c.$$

Starting with the information word  $(a, b, c, d)$ , Alice computes the other four components  $w, x, y, z$  of the code vector  $\mathbf{C}$  using the equations for  $w, x, y$  and  $z$  that come from the condition  $\mathbf{HC} = \mathbf{0}$ , and transmits the vector  $\mathbf{C}$  to Bob. (She can also obtain  $\mathbf{C}$  from  $\mathbf{W}$  by multiplying  $\mathbf{W}$  by a suitable  $8 \times 4$  matrix  $\mathbf{G}$ , as we observed in the (7, 4) code.)

Suppose Bob receives  $\mathbf{R}$ . He computes  $\mathbf{HR}$ .

Case 0. If he finds that  $\mathbf{HR} = \mathbf{0}$ , then he decides that no error occurred and that  $\mathbf{R} = \mathbf{C}$ .

Case 1. If he finds that  $\mathbf{HR}$  is equal to a column of  $\mathbf{H}$ , he decides that one error occurred and he corrects the corresponding entry of  $\mathbf{R}$ .

Case 2. If he finds that  $\mathbf{HR}$  is non-zero but has a top component equal to 0, then he decides that at least two errors occurred.

Why?

Let  $\mathbf{E} = \mathbf{R} - \mathbf{C}$ .

- If no errors occurred, then  $\mathbf{R} = \mathbf{C}$ ,  $\mathbf{E} = \mathbf{0}$  and  $\mathbf{H}\mathbf{R} = \mathbf{H}\mathbf{E} = \mathbf{0}$ .
- If one error occurred, then  $\mathbf{E}$  has a single non-zero component, and so  $\mathbf{H}\mathbf{R} = \mathbf{H}\mathbf{E}$  is a column of  $\mathbf{H}$ . For example, if

$$\mathbf{E} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

then

$$\mathbf{H}\mathbf{R} = \mathbf{H}\mathbf{E} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix},$$

the third column of  $\mathbf{H}$ .

- If two errors occurred, then  $\mathbf{E}$  has two non-zero components. So  $\mathbf{H}\mathbf{R} = \mathbf{H}\mathbf{E}$  is the sum of two columns of  $\mathbf{H}$ . Looking at  $\mathbf{H}$ , we see that the sum of any two columns of  $\mathbf{H}$  is a non-zero vector with first component = 0. For example, if

$$\mathbf{E} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

then

$$\mathbf{H}\mathbf{R} = \mathbf{H}\mathbf{E} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

The three cases of no, one or two errors yield disjoint possibilities for  $\mathbf{H}\mathbf{R}$ , and every possible vector  $\mathbf{H}\mathbf{R}$  satisfies exactly one of those possibilities:  $\mathbf{0}$ , a column of  $\mathbf{H}$ , or a non-zero vector with first component 0. Bob assumes that at most two errors occurred. Computing  $\mathbf{H}\mathbf{R}$ , he can decide whether no, one or two errors occurred.

If  $\mathbf{H}\mathbf{R} = \mathbf{0}$ , Bob decides that  $\mathbf{R} = \mathbf{C}$ .

If  $\mathbf{H}\mathbf{R}$  is a column of  $\mathbf{H}$ , he corrects the corresponding component of  $\mathbf{R}$  to get  $\mathbf{C}$ .

If  $\mathbf{H}\mathbf{R}$  is non-zero but has a top entry of 0, then  $\mathbf{H}\mathbf{R}$  is not a column of  $\mathbf{H}$ . So Bob decides that two errors occurred. He cannot correct  $\mathbf{R}$ , because the same vector  $\mathbf{H}\mathbf{R}$  could be the sum of two columns of  $\mathbf{H}$  in several ways. For example,

$$\begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

- If three errors occurred, then  $\mathbf{E}$  has three non-zero components. Then  $\mathbf{HR} = \mathbf{HE}$  is the sum of three columns of  $\mathbf{H}$ . But the sum of any three columns of  $\mathbf{H}$  is a column of  $\mathbf{H}$ , because the sum has the form

$$\begin{pmatrix} 1 \\ a \\ b \\ c \end{pmatrix}$$

for some numbers  $a, b, c$  in  $\mathbb{F}_2$ , and each such vector is a column of  $\mathbf{H}$ . Bob will be misled. Bob will change the corresponding entry of  $\mathbf{R}$  and get an incorrect  $\mathbf{C}$ .

So the Hamming (8, 4) code is a code that corrects one error and detects two errors in words of length 8 with 4 information digits. Bob will be misled only if there are 3 or more errors. The efficiency is  $4/8 = 0.5$ .

## 7.5 Why Do These Codes Work?

Let us focus on the (8, 4) code. The number of possible received vectors  $\mathbf{R}$  is  $2^8 = 256$ , because each of the eight components of  $\mathbf{R}$  can be 0 or 1. The number of code vectors  $\mathbf{C}$  is 16, because each code vector is uniquely determined by the information word  $\mathbf{W} = (a, b, c, d)$ . So we have 16 code vectors among the 256 possible received vectors. (The sixteen code vectors are written out below.)

Let  $\mathcal{V}$  be the set of all 256 vectors with 8 components from  $\mathbb{F}_2$ . Define a distance function, called the *Hamming distance*, on the set  $\mathcal{V}$  by

$$d(\mathbf{V}_1, \mathbf{V}_2) = \text{the number of 1's in the vector } \mathbf{V}_1 - \mathbf{V}_2.$$

For example,

$$d\left(\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}\right) \text{ is the number of 1's in } \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix},$$

so

$$d\left(\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}\right) = 3.$$

The Hamming distance  $d(\mathbf{V}_1, \mathbf{V}_2)$  counts the number of components of  $\mathbf{V}_1$  that must be changed to get  $\mathbf{V}_2$ .

We have

**Proposition 7.12** *In a Hamming code, the minimum Hamming distance between any two different code vectors is equal to the minimum number of 1's in a non-zero code vector.*

*Proof* First, the zero vector  $\mathbf{0}$  is a code vector (because  $\mathbf{H}\mathbf{0} = \mathbf{0}$ ), so the minimum Hamming distance between any two different code vectors cannot be more than the minimum Hamming distance between the zero vector and any non-zero code vector, and that Hamming distance is equal to the minimum number of 1's in a non-zero code vector.

Now, given a Hamming code, such as the (7, 4) and (8, 4) codes, the set  $\mathcal{C}$  of code vectors are the vectors  $\mathbf{C}$  that satisfy the equation  $\mathbf{HC} = \mathbf{0}$ . So the set of code vectors is the null space of  $\mathbf{H}$ . We observed (Proposition 7.9) that the null space of  $\mathbf{H}$  is a group under addition, so the null space is closed under addition and taking negatives. Thus if  $\mathbf{C}_1$  and  $\mathbf{C}_2$  are code vectors, so is  $\mathbf{C}_3 = \mathbf{C}_1 - \mathbf{C}_2$ .

Now we observe that for any vectors  $\mathbf{V}_1, \mathbf{V}_2, \mathbf{W}$  in  $\mathcal{V}$ ,

$$d(\mathbf{V}_1, \mathbf{V}_2) = d(\mathbf{V}_1 - \mathbf{W}, \mathbf{V}_2 - \mathbf{W}).$$

This is because the Hamming distance counts the number of ones in the difference of the two vectors, and

$$\mathbf{V}_1 - \mathbf{V}_2 = (\mathbf{V}_1 - \mathbf{W}) - (\mathbf{V}_2 - \mathbf{W}).$$

In particular, for any two code vectors  $\mathbf{C}_1, \mathbf{C}_2$ ,

$$d(\mathbf{C}_1, \mathbf{C}_2) = d(\mathbf{C}_1 - \mathbf{C}_2, \mathbf{C}_2 - \mathbf{C}_2) = d(\mathbf{C}_3, \mathbf{0})$$

where  $\mathbf{C}_3 = \mathbf{C}_1 - \mathbf{C}_2$  is a code vector. And  $d(\mathbf{C}_3, \mathbf{0})$  counts the number of 1's in the code vector  $\mathbf{C}_3$ . So the Hamming distance between any two code vectors is equal to the number of 1's in some non-zero code vector.  $\square$

Thus to find the minimum Hamming distance between any two code vectors in the (8, 4) code, we just need to find the minimal number of ones in any non-zero code vector in the code. Call that minimum Hamming distance between any two code vectors the *Hamming distance of the code*.

**Corollary 7.13** *The Hamming distance of the (8, 4) code is equal to the smallest number of columns of the matrix  $\mathbf{H}$  that sum to the zero vector.*

This follows immediately from Corollary 7.7. For  $\mathbf{0} = \mathbf{HC}$  = the sum of the columns of  $\mathbf{H}$  corresponding to the non-zero components of  $\mathbf{C}$ . If  $\mathbf{C}$  is a code vector with  $r$  components equal to 1 and the rest equal to 0, then the sum of  $r$  components of  $\mathbf{H}$  is 0. So the smallest  $r$  so that  $r$  columns of  $\mathbf{H}$  sum to  $\mathbf{0}$  is equal to the smallest number of non-zero components of a code vector.

**Corollary 7.14** *The Hamming distance of the (8, 4) code is 4.*

*Proof* We can determine the Hamming distance of the (8, 4) code by looking at the matrix  $\mathbf{H}$ :

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Since the top row of  $\mathbf{H}$  has all 1's, it is easy to see that the sum of an odd number of distinct columns of  $\mathbf{H}$  cannot be  $= \mathbf{0}$ . It's also easy to see that the sum of two distinct columns cannot be  $= \mathbf{0}$ . So the Hamming distance must be at least 4. But it is also easy to find four columns of  $\mathbf{H}$  that sum to  $\mathbf{0}$ , for example, the sum of the first four columns. So the Hamming distance must be = 4.  $\square$

To confirm that the Hamming distance is = 4, here is a matrix whose columns are all of the code vectors in the (8, 4) code:

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

One sees quickly that every column vector has 4 ones in it except the vector  $\mathbf{0}$  and the vector of all 1's. That observation confirms that the Hamming distance for the (8, 4) code is 4.

When Bob receives a vector  $\mathbf{R}$ , computes  $\mathbf{HR}$  and gets a column of  $\mathbf{H}$ , then Bob knows that  $\mathbf{R}$  is a Hamming distance of 1 from some code vector  $\mathbf{C}$ . Since the Hamming distance of the code is 4, he then knows that  $\mathbf{R}$  is a Hamming distance of at least 3 from any other code vector. Since one error in getting from a code vector to  $\mathbf{R}$  is much more likely than three errors, Bob decodes  $\mathbf{R}$  to  $\mathbf{C}$ .

But if  $\mathbf{R}$  has two errors in it, then  $\mathbf{R}$  could be a Hamming distance from two or more different vectors. For example,

$$\mathbf{R} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \text{ is a Hamming distance of 2 from } \mathbf{C}_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \text{ and } \mathbf{C}_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

It is impossible to decide how to decode  $\mathbf{R}$ .

We will look again at this situation in Section 14.2.

In Chapter 15 we will describe a family of codes that correct more than one error.

## Exercises

7.1. Multiply:

$$(i) (1 \ 2 \ 3) \begin{pmatrix} -1 \\ -3 \\ 1 \end{pmatrix};$$

$$(ii) (0 \ -2 \ 5) \begin{pmatrix} -1 \\ -3 \\ 1 \end{pmatrix};$$

$$(iii) \begin{pmatrix} 1 & 2 & 3 \\ 0 & -2 & 5 \end{pmatrix} \begin{pmatrix} -1 \\ -3 \\ 1 \end{pmatrix}.$$

$$(iv) \begin{pmatrix} -1 \\ -3 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}.$$

- 7.2. Suppose  $\mathbf{A}$  is an  $m \times 1$  matrix and  $\mathbf{B}$  is a  $1 \times n$  matrix. Show that every row of  $\mathbf{AB}$  is a scalar multiple of the row of  $\mathbf{B}$ .
- 7.3. Analogous to Example 7.3 involving EEA vectors, find three different ways to write 10 as a linear combination of 11 and 18 by manipulating EEA vectors  $(r, a, b)$  where  $r = 11a + 18b$ . (Start with Euclid's Algorithm for 11 and 18.)
- 7.4. Write the system of equations

$$\begin{aligned} 2x + y + 5z &= 0 \\ x - 4z &= 0 \end{aligned}$$

as a matrix equation. Let  $\mathbf{A}$  be the matrix of coefficients of the system. Find all solutions of the system of equations. Write the solutions as column vectors  $\mathbf{v}$  and verify that  $\mathbf{Av} = \mathbf{0}$ .

- 7.5. Find two  $2 \times 2$  matrices  $\mathbf{A}$  and  $\mathbf{B}$  where no entry of  $\mathbf{A}$  or  $\mathbf{B}$  or  $\mathbf{BA}$  is zero, but  $\mathbf{AB} = \mathbf{0}$ .
- 7.6. Alice wants to send the message SELL to Bob, her broker. She turns SELL into a sequence of 0's and 1's. The sequence will have length 20. She wants to protect the message against random bit errors during the transmission. Help her by breaking up the sequence into a set of five information words and encoding them by the Hamming (8, 4) code.
- 7.7. Here are four received words which were transmitted after being encoded with the Hamming (8, 4) code. For each word  $\mathbf{R}$ , assume there are 0, 1, or 2 errors. Decode each word or decide that two errors occurred. If two errors occurred, list the nearest code vectors to  $\mathbf{R}$ .

$$\mathbf{R} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

- 7.8. Find the encoding matrix  $\mathbf{G}$  for the (8, 4) code.
- 7.9. (i) In the Hamming (7, 4) code, suppose Bob receives

$$\mathbf{R} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

He computes  $\mathbf{HR}$ . If there is one error in  $\mathbf{R}$ , find  $\mathbf{C}$ .

(ii) Suppose  $\mathbf{R}$  has two errors. Show that each of the following vectors are code vectors

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix},$$

and changing two suitable entries in each would yield  $\mathbf{R}$ .

- 7.10. In the  $(7, 4)$  Hamming code, Alice sends Bob the code vector  $\mathbf{C}$ . Bob receives  $\mathbf{R}$ , computes  $\mathbf{HR}$  and gets  $\mathbf{0}$ . Bob concludes that  $\mathbf{R} = \mathbf{C}$ . Explain why it is that if Bob is wrong, then  $\mathbf{R}$  and  $\mathbf{C}$  must differ in at least three bits.
- 7.11. Show that the Hamming distance of the  $(7, 4)$  code is 3, by showing that there is a code vector  $\mathbf{C}$  with exactly three non-zero components, but no code vector with one or two non-zero components. (Hint: try to find one, two or three columns of  $\mathbf{H}$  that sum to  $\mathbf{0}$ ).
- 7.12. Construct a code, analogous to the Hamming  $(8, 4)$  code, that uses a  $5 \times 16$  matrix  $\mathbf{H}$ , and sends out binary words of length 16 (of which 11 are information digits) such that the receiver can correct one error and detect two errors. Is it necessary for decoding that all of the columns of your matrix  $\mathbf{H}$  must be distinct?
- 7.13. What is the Hamming distance of the code you constructed in the last exercise?

**Hill codes.** The multiplicative Caesar cipher of Chapter 2 is not historically significant, but its matrix generalization is the first published cryptosystem based on “advanced” mathematics.

Suppose we wish to send the plaintext message GO, or, with the usual numerical correspondence, 8, 15. To encrypt, view these numbers modulo 27 (that is, as elements of the commutative ring  $\mathbb{Z}_{27}$ ), and encrypt by choosing some  $2 \times 2$  matrix  $\mathbf{E}$  and multiplying the vector  $\mathbf{w} = (8, 15)^T$  by the matrix  $\mathbf{E}$ . As with the multiplicative Caesar cipher, we need to know that  $\mathbf{E}$  has an inverse—a  $2 \times 2$  matrix  $\mathbf{D}$  so that  $\mathbf{DE} = \mathbf{I}$ , the  $2 \times 2$  identity matrix. For example, let

$$\mathbf{E} = \begin{pmatrix} 4 & 13 \\ 15 & 17 \end{pmatrix}.$$

If

$$\mathbf{D} = \begin{pmatrix} -8 & -5 \\ 15 & 14 \end{pmatrix}.$$

then (modulo 27),

$$\mathbf{DE} = \begin{pmatrix} -32 + -75 & -104 - 85 \\ 60 + 210 & 195 + 238 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}.$$

So we encrypt the message  $\mathbf{w} = (8, 15)^T$  by

$$\mathbf{c} = \mathbf{Ew} = \begin{pmatrix} 4 & 13 \\ 15 & 17 \end{pmatrix} \begin{pmatrix} 8 \\ 15 \end{pmatrix} = \begin{pmatrix} 227 \\ 275 \end{pmatrix} = \begin{pmatrix} 11 \\ 24 \end{pmatrix}.$$

Returning to letters, this is the ciphertext KW. To decrypt, we compute (always modulo 27):

$$\mathbf{Dc} = \begin{pmatrix} -8 & -5 \\ 15 & 14 \end{pmatrix} \begin{pmatrix} 11 \\ 24 \end{pmatrix} = \begin{pmatrix} 8 \\ 15 \end{pmatrix}.$$

7.14. Encrypt the message NO by using the matrix

$$\mathbf{E} = \begin{pmatrix} 20 & 10 \\ -4 & 6 \end{pmatrix}.$$

then verify that the matrix  $\mathbf{D}$  that decrypts your encrypted message is

$$\mathbf{D} = \begin{pmatrix} -3 & 5 \\ -2 & -10 \end{pmatrix}.$$

These codes, which can be constructed using square invertible matrices of any size over  $\mathbb{Z}/m\mathbb{Z}$  for any suitable  $m$ , are called Hill codes. They first appeared in publications of Lester Hill [[Hi29](#), [Hi31](#)]. They are insecure: Konheim [[Kon81](#)] describes how they can be broken. However, those publications are significant in the history of cryptography, because they were the first published research papers in mathematics to view cryptography as a legitimate branch of applied mathematics [[Kah67](#), pp. 408–10].

# Chapter 8

## Orders and Euler's Theorem



In the decade between 1970 and 1980, cryptography was transformed by the introduction of public key cryptography, and became a vigorous research area of applied mathematics. In Chapters 9, 14, and 16 we'll examine three different approaches to public key cryptography. All three involve hard problems related to modular exponentiation, that is, the raising of units modulo  $m$  to powers.

To prepare for those cryptographic methods, in this chapter we study the group  $U_m$  of units of  $\mathbb{Z}_m$  and the important concept of the order of a unit. We obtain Fermat's Theorem and Euler's Theorem, both of which are useful for applications in cryptography. The chapter concludes with a description of an algorithm for finding a number such as  $7^{171}$  modulo 447 on a minimal calculator.

Throughout this chapter we work with  $\mathbb{Z}_m$ , integers defined up to congruence modulo  $m$ , with operations modulo  $m$ . The results can be described in terms of cosets  $a + m\mathbb{Z}$  in  $\mathbb{Z}/m\mathbb{Z}$ , but as noted in Chapter 4, the notation is a bit less clunky using  $\mathbb{Z}_m$ .

### 8.1 Orders of Elements

The group of units  $U_m$  of  $\mathbb{Z}_m$  is an example of an abelian group. Recall the definition from Chapter 5. An abelian group is a set  $G$  with one operation, let's call it  $*$ , such that

- the associative law,  $(a * b) * c = a * (b * c)$ , is true for all  $a, b, c$  in  $G$ ,
- the commutative law,  $a * b = b * a$ , is true for all  $a, b$  in  $G$ ,
- $G$  has an identity element  $e$  satisfying  $e * a = a$  for all  $a$  in  $G$ , and
- every element of  $G$  has an inverse: for every  $a$  in  $G$ , there is some  $b$  in  $G$  so that  $ab = e$ .

In this chapter we're interested in the group of units  $U_m$  of  $\mathbb{Z}_m$ , so the operation  $*$  is multiplication, and the identity element  $e$  is 1.

An integer  $(a \bmod m)$  is in  $U_m$  if and only if there is some integer  $b$  so that

$$ab \equiv 1 \pmod{m}.$$

In Section 5.8 we showed that  $a$  is a unit modulo  $m$  if and only if  $a$  and  $m$  are coprime. If  $(a, m) = 1$  we saw in Chapter 3 how to find the inverse of  $a$  modulo  $m$  by Bezout's Identity.

The product of two units is a unit (Why? See Chapter 5). So the set  $U_R$  of units of a commutative ring  $R$  is closed under multiplication, and hence is an abelian group (because multiplication in the ring is commutative and associative, the multiplicative identity 1 is a unit, and by definition of unit, every unit has an inverse, which is also a unit of  $R$ ).

*Example 8.1* The units of  $\mathbb{Z}_{12}$  are 1, 5, 7 and 11. Each is its own inverse. (For example,  $7 \cdot 7 = 49 = 1 + 48 \equiv 1 \pmod{12}$ ).

The units of  $\mathbb{Z}_{14}$  are 1, 3, 5, 9, 11 and 13, with inverses 1, 5, 3, 11, 9 and 13, respectively. (For example,  $9 \cdot 11 = 99 = 14 \cdot 7 + 1$ , so  $9 \cdot 11 \equiv 1 \pmod{14}$ .)

In  $\mathbb{Z}_{11}$ , the units are the numbers 1 through 10. To see that each number has an inverse modulo 11, we observe that

$$1 \cdot 1 \equiv 2 \cdot 6 \equiv 3 \cdot 4 \equiv 5 \cdot 9 \equiv 7 \cdot 8 \equiv 10 \cdot 10 \equiv 1 \pmod{11}.$$

For multiplicative Caesar ciphers in Chapter 2, we were interested in the units of  $\mathbb{Z}_{27}$ . They are 1, 2, 4, 5, 7, 8, 10, 11, 13 and their negatives modulo 27. To show that each has an inverse, it suffices to observe that  $1 = 1 \cdot 1 \equiv 2 \cdot 14 \equiv 4 \cdot 7 \equiv 5 \cdot 11 \equiv 8 \cdot 10 \pmod{27}$  and recall that if  $a \cdot b = 1$ , then  $(-a) \cdot (-b) = 1$  (Chapter 5, Corollary 6).

The new mathematics in this section starts from the observation that if we take powers of a number  $a$ :  $1 = a^0, a, a^2, a^3, \dots$ , then eventually two of the powers will be congruent modulo  $m$ . So modulo  $m$ , the sequence of powers of  $a$  begins repeating.

*Example 8.2* The powers of 2:

$$1, 2, 4, 8, 16, 32, 64 \dots,$$

are congruent modulo 7 to

$$1, 2, 4, 1, 2, 4, 1, \dots$$

Modulo 18, the powers of 2 are congruent to

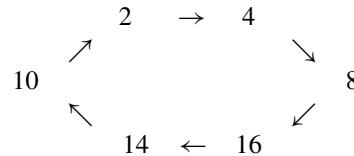
$$1, 2, 4, 8, 16, 14, 10, 2, 4, 8, \dots$$

Modulo 11, the powers of 2 are congruent to

$$1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1, 2, 4, 8, \dots$$

The reason the sequences begin repeating is sometimes called the “pigeonhole principle”. There are exactly  $m$  elements of  $\mathbb{Z}_m$ . If we look at  $1, a, a^2, a^3, \dots, a^m$ , then since these are  $m+1$  powers of  $a$ , at least two of the powers must be congruent modulo  $m$ . And once  $a^r \equiv a^s \pmod{m}$ , then  $a^{r+k} \equiv a^{s+k} \pmod{m}$  for every  $k \geq 0$ . The powers of  $a$  modulo  $m$  repeat with period at most  $s-r$ .

For example,  $2^7 \equiv 2 \pmod{18}$ . So  $2^8 \equiv 2^2, 2^9 \equiv 2^3$ , etc. Pictorially, we have



where the arrows mean “multiply by 2 (mod 18).”

If  $a^s \equiv 1 \pmod{m}$  for some  $s > 0$ , then  $a$  must be a unit modulo  $m$ , because  $a \cdot a^{s-1} \equiv 1 \pmod{m}$ . The converse is also true:

**Proposition 8.3** *If  $a$  is a unit of  $\mathbb{Z}_m$ , then  $a^t \equiv 1 \pmod{m}$  for some  $t$ .*

We can in fact get an upper bound for  $t$ , namely  $t \leq \phi(m)$ , Euler's phi function (or “Euler's totient”), which denotes the number of units of  $\mathbb{Z}_m$ . If  $m = p$  prime, then  $\phi(p) = p - 1$ , and for all  $m$ ,  $\phi(m) \leq m - 1$ . We'll be more precise about  $\phi(m)$  later.

*Proof* If  $a$  is a unit modulo  $m$ , then since units are closed under multiplication, the powers of  $a$  are all units modulo  $m$ . There are  $\phi(m)$  units of  $\mathbb{Z}_m$ . So two of the  $\phi(m) + 1$  powers  $1, a, a^2, \dots, a^{\phi(m)}$  must be congruent modulo  $m$ : that is, there exist numbers  $s$  and  $t$  with  $s \geq 0$  and  $0 < t \leq \phi(m)$  so that  $a^s \equiv a^{s+t} \pmod{m}$ . Now since  $a$  is a unit modulo  $m$ , we can cancel the common factor  $a^s$  from both sides of the congruence (equivalently, multiply both sides of the congruence by the inverse of  $a^s$ ) to get  $1 \equiv a^t \pmod{m}$ .  $\square$

Exactly the same argument applies to the elements of every finite group:

**Proposition 8.4** *Let  $G$ , with operation  $*$ , be a group with  $n$  elements, and with identity element  $e$ . For every  $g$  in  $G$ , let  $g^t$  denote the element  $g * g * \dots * g$  ( $t$  factors). Then  $g^d = e$  for some  $d$  with  $0 < d \leq n$ .*

*Proof* We have  $e = g^0, g, g^2, g^3, \dots, g^n$ , a sequence of  $n + 1$  elements of the set  $G$  that contains exactly  $n$  elements. So two of the powers must be equal:  $g^s = g^{s+d}$  for some numbers  $s$  and  $d$  with  $0 \leq s < s + d \leq n$ . But then canceling  $g^s$  from both sides of the equation yields  $g^d = e$  for some  $d$  with  $1 \leq d \leq n$ .  $\square$

This proposition yields the concept of the order of an element of a finite group.

**Definition** Let  $g$  be an element of a finite group  $G$ . The *order* of  $g$  is the smallest exponent  $d > 0$  so that  $g^d = e$ .

The order of an element exists: by Proposition 8.4,  $g^d = e$  for some number  $d \geq 1$ . So by Well Ordering, there must be a least number with that property.

Specializing this definition to  $G = U_m$ , the group of units of  $\mathbb{Z}_m$  for  $m \geq 2$ , we have:

**Definition** Let  $a$  be any integer coprime to  $m$ . The *order of  $a$  modulo  $m$*  is the smallest positive integer  $e$  so that  $a^e \equiv 1 \pmod{m}$ .

In terms of divisibility, the order of  $a$  mod  $m$  is the smallest  $e > 0$  so that  $m$  divides  $a^e - 1$ .

*Example 8.5* The order of 2 modulo 11 is 10, because  $2^{10} \equiv 1 \pmod{11}$ , while  $2^1, 2^2, \dots, 2^9$  are not  $\equiv 1 \pmod{11}$  (as we observed in Example 8.2).

To emphasize the subtlety in the definition of order, we note that to show that  $e$  is the order of  $a$  modulo  $m$ , two things must be checked:

- (i)  $a^e \equiv 1 \pmod{m}$ ; and
- (ii) for  $1 \leq s < e$ ,  $a^s \not\equiv 1 \pmod{m}$ .

Condition (ii) expresses the condition that the order of  $a$  is the *least* positive exponent so that  $a^e \equiv 1 \pmod{m}$ .

Note: We could also talk about the order of a number  $a$  in the set  $\mathbb{Z}_m$  of numbers modulo  $m$  viewed as a group under addition. But this chapter will exclusively look at orders of elements in the group  $U_m$  of units of  $\mathbb{Z}_m$ . So, for example, if we were to ask about the order of 12 modulo 15 in this chapter, it wouldn't make sense because 12 is not a unit modulo 15.

*Example 8.6* We found that the order of 2 modulo 11 is 10. We can find the orders of the other non-zero elements of  $\mathbb{Z}_{11}$  by direct computation, or, more efficiently, by working with exponents of 2 modulo 11.

For example, we found that  $2^8 \equiv 3 \pmod{11}$ . So starting at that point and using that  $2^{10} \equiv 1 \pmod{11}$ , we have

$$\begin{aligned} 3 &\equiv 2^8 \pmod{11} \\ 3^2 &\equiv 2^{16} \equiv 2^6 \pmod{11} \\ 3^3 &\equiv 2^{24} \equiv 2^4 \pmod{11} \\ 3^4 &\equiv 2^{32} \equiv 2^2 \pmod{11} \\ 3^5 &\equiv 2^{40} \equiv 1 \pmod{11}. \end{aligned}$$

So 3 has order 5  $(\bmod 11)$ .

To find orders of elements modulo  $m$ , we can often reduce the amount of computation by learning a few facts about order. Here is the first:

**Proposition 8.7** *If  $e$  is the order of a modulo  $m$ , and  $a^f \equiv 1 \pmod{m}$ , then  $e$  divides  $f$ .*

*Proof* We have  $a^e \equiv 1 \pmod{m}$  and  $a^f \equiv 1 \pmod{m}$ . Divide  $e$  into  $f$  to get  $f = eq + r$ , with  $0 \leq r < e$ . Then

$$a^f = (a^e)^q \cdot a^r.$$

Modulo  $m$ , this becomes

$$1 \equiv (1)^q \cdot a^r,$$

so  $a^r \equiv 1 \pmod{m}$ . But  $r < e$  and  $e$  is the *least positive* number with  $a^e \equiv 1 \pmod{m}$ . So  $r = 0$ , and so  $e$  divides  $f$ .  $\square$

Notice how crucial it is in the proof that the order of  $a$  is the least positive exponent so that  $a^e \equiv 1 \pmod{m}$ .

*Example 8.8* To find the order of 7 modulo 11, we notice that  $7 \equiv 2^7 \pmod{11}$ , and

$$7^{10} \equiv 2^{70} \equiv (2^{10})^7 \equiv 1 \pmod{11}.$$

So by Proposition 8.7 the order of 7 modulo 11 divides 10. Is it 1, or 2, or 5, or 10? We check, using that 2 has order 10  $(\bmod 11)$ :

$$\begin{aligned} 7^1 &\equiv 2^7 \not\equiv 1 \pmod{11} \\ 7^2 &\equiv 2^{14} \equiv 2^4 \not\equiv 1 \pmod{11} \\ 7^5 &\equiv 2^{35} \equiv 2^5 \not\equiv 1 \pmod{11}. \end{aligned}$$

So 7 must have order 10 modulo 11.

We can also see that the order of  $2^7$  modulo 11 is 10 by using:

**Proposition 8.9** *If  $a$  has order  $e$  modulo  $m$  and  $d > 0$ , then the order of  $a^d$  modulo  $m$  is  $e/(d, e)$ , where  $(d, e)$  is the greatest common divisor of  $d$  and  $e$ .*

*Proof* Recall that for numbers  $d, e$ , the least common multiple  $[d, e]$  satisfies

$$\frac{[d, e]}{d} = \frac{e}{(d, e)}.$$

Since  $a^e \equiv 1 \pmod{m}$ , we have

$$1 \equiv (a^e)^{\left(\frac{d}{(d, e)}\right)} = (a^d)^{\left(\frac{e}{(d, e)}\right)}.$$

To show that  $\frac{e}{[d,e]}$  is the order of  $a^d$ , we need to be sure that no smaller positive power of  $a^d$  is congruent to 1. So suppose  $(a^d)^s \equiv 1 \pmod{m}$  for  $s > 0$ . Then  $a^{ds} \equiv 1 \pmod{m}$ , so by Proposition 8.7,  $e$  divides  $ds$ . So  $ds$  is a common multiple of  $e$  and  $d$ , so  $ds \geq [d, e]$ , hence  $s \geq \frac{[d, e]}{d}$ . So the order of  $a^d$  is  $e/(d, e)$ .  $\square$

*Example 8.10* Applying Proposition 8.9 to the orders of units modulo 11, we find that

$$2, 2^3 \equiv 8, 2^7 \equiv 7 \text{ and } 2^9 \equiv 6 \text{ have order 10};$$

$$2^2 \equiv 4, 2^4 \equiv 5, 2^6 \equiv 9 \text{ and } 2^8 \equiv 3 \text{ have order 5};$$

$$2^5 \equiv 10 \equiv -1 \text{ has order 2};$$

$$2^{10} \equiv 1 \text{ has order 1 modulo 11.}$$

Often we will want to find the order of numbers modulo a composite modulus. For doing so, the following result will be helpful.

**Proposition 8.11** *Let  $m$  and  $n$  be coprime numbers  $> 2$ , and suppose the order of  $a$  modulo  $m$  is  $d$ , and the order of  $a$  modulo  $n$  is  $e$ . Then the order of  $a$  modulo  $mn$  is the least common multiple of  $d$  and  $e$ .*

*Proof* We first show that  $a^{[d,e]} \equiv 1 \pmod{mn}$ . Now  $[d, e]$  is a multiple of  $d$ , so  $a^{[d,e]} \equiv 1 \pmod{m}$ . Similarly,  $[d, e]$  is a multiple of  $e$ , so  $a^{[d,e]} \equiv 1 \pmod{n}$ . Since  $(m, n) = 1$ , Lemma 8.32 (below) implies that  $a^{[d,e]} \equiv 1 \pmod{mn}$ .

Now suppose  $a^f \equiv 1 \pmod{mn}$ . Then  $a^f \equiv 1 \pmod{m}$ . Since  $d$  is the order of  $a$  modulo  $m$ , Proposition 3 implies that  $d$  divides  $f$ . Similarly,  $a^f \equiv 1 \pmod{n}$ . Since  $e$  is the order of  $a$  modulo  $n$ , Proposition 3 implies that  $e$  divides  $f$ . So  $f$  is a common multiple of  $d$  and  $e$ . By Proposition 14 of Chapter 4,  $f$  is a multiple of  $[d, e]$ . So the smallest exponent  $f$  so that  $a^f \equiv 1 \pmod{mn}$  is  $f = [d, e]$ .  $\square$

*Example 8.12* We know that 2 has order 5 modulo 31, and 2 has order 6 modulo 9. So 2 has order  $[6, 5] = 30$  modulo 279.

Also, 2 has order 8 modulo 17 and has order 4 modulo 5. So 2 has order  $[8, 4] = 8$  modulo 85.

Also, 2 has order 6 modulo 9 and has order 4 modulo 5. So 2 has order  $[6, 4] = 12$  modulo 45.

Applications in Chapters 14 and 15 will find Proposition 8.11 helpful.

## 8.2 Fermat's Theorem

You may have noticed from Example 8.10 that if  $a$  is any number not divisible by 11, then the order of  $a$  modulo 11 divides 10.

That fact is a special case of

**Theorem 8.13** (Fermat's Theorem) *If  $p$  is a prime and  $a$  is an integer not divisible by  $p$ , then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

A proof of Fermat's Theorem is in Section 8.4 (and another proof is in Chapter 10).

Combining Fermat's Theorem with Proposition 8.7 yields:

**Proposition 8.14** *If  $p$  is prime and  $a$  is not divisible by  $p$ , then the order of  $a$  modulo  $p$  divides  $p - 1$ .*

Applying Proposition 8.14 can reduce computation in finding the order of a unit  $a$  modulo  $p$ .

*Example 8.15* Consider the order of 3 modulo 23. By Fermat's Theorem,

$$3^{22} \equiv 1 \pmod{23}.$$

So the order of 3 modulo 23 is 1, 2, 11 or 22. Clearly it is not 1 or 2. Is it 11? Or is it 22? To decide, we compute  $3^{11}$  modulo 23:

We have  $3^2 \equiv 9$ ;  $3^3 = 27 \equiv 4$ ;  $3^6 \equiv 3^3 \cdot 3^3 \equiv 16$ . So

$$3^9 \equiv 3^3 \cdot 3^6 \equiv 4 \cdot 16 = 64 \equiv -5 \pmod{23}.$$

Then

$$3^{11} \equiv 3^9 \cdot 3^2 \equiv (-5) \cdot 9 = -45 \equiv 1 \pmod{23}.$$

So the order of 3 modulo 23 is 11.

*Example 8.16* The order of 5 modulo 23 is not 1 or 2, so must be either 11 or 22. So we compute  $5^{11}$ : we see that  $5^2 = 25 \equiv 2$ , so

$$\begin{aligned} 5^{11} &= 5 \cdot 5^{10} \equiv 5 \cdot 2^5 \\ &\equiv 5 \cdot 9 = 45 \equiv -1 \pmod{23}. \end{aligned}$$

So 5 has order 22 modulo 23.

*Example 8.17* The order of 5 modulo 83 is either 41 or 82, and the order of 5 modulo 47 is either 23 or 46, both facts a consequence of Fermat's Theorem and Proposition 8.7. Therefore, by Proposition 8.11 the order of 5 modulo  $83 \cdot 47 = 3901$  is either  $[41, 23] = 943$  or  $[41, 46] = [82, 23] = [82, 46] = 1886$ .

Fermat's Theorem gives a way to write down the inverse of a number  $a$  as a power of  $a$  modulo  $p$ , where  $p$  is prime:

If  $a$  is any integer with  $(a, p) = 1$ , then  $a^{p-1} \equiv 1 \pmod{p}$ , so  $a \cdot a^{p-2} \equiv 1$ . Thus  $a^{p-2}$  is the inverse of  $a$  modulo  $p$ .

*Example 8.18* Since the order of 5 modulo 23 is 22, the inverse of 5 modulo 23 is  $5^{21}$ , which we can find as follows:

$$\begin{aligned} 5^2 &\equiv 2 \pmod{23} \\ 5^4 &\equiv 4 \\ 5^5 &\equiv 20 \equiv -3 \\ 5^{10} &\equiv 9 \\ 5^{20} &\equiv 81 \equiv 12 \\ 5^{21} &\equiv 12 \cdot 5 \equiv 60 \equiv 14 \pmod{23}. \end{aligned}$$

To verify the computation, we see that  $14 \cdot 5 = 70 \equiv 1 \pmod{23}$ .

(See Section 8.5, below for an explanation of the method we used, called the “XS binary method”.) Equivalent to Fermat's Theorem is:

**Theorem 8.19** *If  $p$  is prime, then for all integers  $a$ ,  $a^p \equiv a \pmod{p}$ .*

*Proof* Since  $p$  is a prime number, every integer  $a$  is either coprime to  $p$  or a multiple of  $p$ . If  $p$  divides  $a$ , then  $a^p \equiv 0 \pmod{p}$ . If  $a$  is coprime to  $p$ , then Fermat's Theorem says that  $a^{p-1} \equiv 1 \pmod{p}$ . Multiplying both sides by  $a$  gives  $a^p \equiv a \pmod{p}$ .  $\square$

Conversely, if Theorem 8.19 is true, then Fermat's Theorem follows, because if  $a^p \equiv a \pmod{p}$  and  $a$  is coprime to  $p$ , then we can cancel  $a$  from both sides of the congruence to get  $a^{p-1} \equiv 1 \pmod{p}$ .

So we can prove Fermat's Theorem by proving Theorem 8.19, which we'll do in Section 8.4, below.

### 8.3 Euler's Theorem

Proposition 8.3 showed that if  $m$  is a modulus and  $a$  any integer with  $(a, m) = 1$ , then there is some  $t$  with  $a^t \equiv 1 \pmod{m}$ .

If  $m$  is prime, Fermat's theorem asserts that we can choose  $t = m - 1$ .

If  $m$  is composite, we have:

**Theorem 8.20** (Euler's Theorem) *For every integer  $a$  coprime to  $m$ ,  $a^{\phi(m)} \equiv 1 \pmod{m}$ .*

Here,  $\phi(m)$  is the number of units modulo  $m$ , which is the same as the number of numbers  $a$  with  $1 \leq a \leq m$  that are coprime to  $m$ .

*Example 8.21* In  $\mathbb{Z}_{16}$ , there are eight units:  $\phi(16) = 8$ . So for every  $a$  coprime to 16,  $a^8 \equiv 1 \pmod{16}$ . For example,

$$5^8 \equiv 25^4 \equiv 9^4 \equiv 81^2 \equiv 81 \equiv 1 \pmod{16}.$$

Notice that Fermat's theorem is a special case of Euler's theorem. If  $p$  is prime, then  $\phi(p) = p - 1$ . We will prove Euler's Theorem in Chapter 10.

**Euler's phi function.** An obvious question related to Euler's theorem is, how do we compute the number  $\phi(m)$ , Euler's phi function? In order to use Euler's theorem, we need to know  $\phi(m)$ . Even for fairly small numbers  $m$ , the description of  $\phi(m)$  as the number of units of  $\mathbb{Z}_m$ , or as the number of numbers  $r$  with  $1 \leq r \leq m$  that are coprime to  $m$ , is not all that helpful for computing  $\phi(m)$ .

*Example 8.22* Let's compute  $\phi(60)$ . To do this, we know that the prime numbers that divide 60 are 2, 3 and 5. If we write down all the numbers  $\leq 60$  and then cross out all numbers that are multiples of 2, 3 or 5, the remaining numbers will be coprime to 60:

$$1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.$$

So  $\phi(60) = 16$ .

We could compute  $\phi(60)$  as we did because we knew the prime factors of 60. It turns out that if we can factor  $m$  into a product of prime powers, then finding  $\phi(m)$  is immediate, using the following facts:

- Proposition 8.23** (a) If  $p$  is prime, then  $\phi(p) = p - 1$ ;
- (b) If  $p$  is prime, then for all  $e > 0$ ,  $\phi(p^e) = p^{e-1}(p - 1)$ ;
- (c) If  $a$  and  $b$  are coprime, then  $\phi(ab) = \phi(a)\phi(b)$ .

We illustrate the first two facts.

*Example 8.24*  $\phi(17) = 16$  because every number  $< 17$  is coprime to 17.

We can see that  $\phi(27) = 27 - 9$  by the method of Example 8.22: we know that the only prime that divides 27 is 3. So a number  $n$  is coprime to 27 if and only if  $n$  is not a multiple of 3. We can then compute  $\phi(27)$  by counting all the 27 numbers  $\leq 27$  and then subtracting the number of numbers  $\leq 27$  that are multiples of 3: we get  $27 - 9 = 18$ .

These examples should make it clear how to prove facts (i) and (ii). (See Exercise 8.22) We'll suggest a method for proving (iii) in Exercises 8.35 and 8.36. We'll also give a proof of (iii) as an application of the Chinese Remainder Theorem in Chapter 13.

*Example 8.25*

$$60 = 2^2 \cdot 3 \cdot 5.$$

So

$$\phi(60) = \phi(2^2) \cdot \phi(3) \cdot \phi(5) = 2 \cdot 2 \cdot 4 = 16.$$

But what if we have a number  $m$  that we can't factor? How do we find  $\phi(m)$ ?

It turns out that for some numbers  $m$  that are particularly difficult to factor, we can't find  $\phi(m)$  either. That fact is of immense practical importance for cryptography as we'll see in Chapter 9.

In short:

Finding  $\phi(m)$  is easy if we can factor  $m$ . Finding  $\phi(m)$  is impossible if we cannot factor  $m$ .

**Summary.** We summarize results on the orders of units modulo  $m$ .

An integer  $a$  is a unit modulo  $m$  if  $a$  is coprime to  $m$ . Then  $a$  represents an element of the group  $U_m$  of units modulo  $m$ ,  $U_m$ . The elements of  $U_m$  can be represented by the numbers less than  $m$  and coprime to  $m$ . There are  $\phi(m)$  elements of  $U_m$ .

If  $a$  is a number coprime to  $m$ , then  $a^r \equiv 1 \pmod{m}$  for some  $r > 0$  (Proposition 8.3). Then  $a$  has order  $e$  modulo  $m$  if  $e$  is the smallest positive integer so that  $a^e \equiv 1 \pmod{m}$ . We have the following facts related to the orders of elements modulo  $m$ :

- (Proposition 8.7) If  $a^f \equiv 1 \pmod{m}$ , then the order of  $a$  modulo  $m$  divides  $f$ .
- (Proposition 8.20) Euler's Theorem says that if  $a$  is coprime to  $m$ , then  $a^{\phi(m)} \equiv 1 \pmod{m}$ . So the order of any unit  $a$  modulo  $m$  divides  $\phi(m)$ . If  $m$  is a prime number  $p$ , then  $\phi(p) = p - 1$  and Euler's Theorem specializes to Fermat's Theorem (Proposition 8.13).
- (Proposition 8.9) If  $a$  has order  $e$  modulo  $m$ , then  $a^r$  has order  $e/(r, e)$  modulo  $m$ . In particular, if  $r$  divides  $e$ , then  $a^r$  has order  $e/r$  modulo  $m$ , while if  $r$  is coprime to  $e$ , then  $a^r$  has order  $e$  modulo  $m$ .
- (Proposition 8.11) If  $a$  is coprime to  $m$  and  $m = rs$  with  $(r, s) = 1$ , then  $a$  is coprime to both  $r$  and  $s$ . If the order of  $a$  modulo  $r$  is  $e$  and the order of  $a$  modulo  $s$  is  $d$ , then the order of  $a$  modulo  $m$  is  $[e, d]$ , the least common multiple of the orders of  $a$  modulo  $r$  and modulo  $s$ .

A naive way to find the order of  $a$  modulo  $m$  is to start taking powers of  $a$  modulo  $m$ , and stop when we find a power of  $a$  that is congruent to 1 modulo  $m$ . The facts we've just listed help shorten the process of finding the order of an element  $a$  modulo  $m$ , as we've seen.

## 8.4 The Binomial Theorem and Fermat's Theorem

In this section we give a proof of Fermat's Theorem using the Binomial Theorem. We'll prove Fermat's Theorem and Euler's Theorem by a much different strategy in Chapter 10. So you can skip most of this section if you wish.

The Binomial Theorem is:

**Theorem 8.26** *For any two elements  $x, y$  of any commutative ring, and every number  $n$ ,*

$$(x + y)^n = x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{r} x^{n-r} y^r + \cdots + \binom{n}{n-1} x y^{n-1} + y^n,$$

where the “binomial coefficients”  $\binom{n}{r}$  are integers and satisfy

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

This standard result can be proven by induction. We omit the proof here.

The key fact for proving Fermat's Theorem is:

**Proposition 8.27** *If  $p$  is prime, then  $p$  divides  $\binom{p}{r}$  for all  $r$ ,  $0 < r < p$ .*

*Proof* Recall the Coprime Divisibility Lemma from Chapter 3, that if a number  $a$  divides a product  $bc$  of two numbers and  $a$  and  $b$  are coprime, then  $a$  must divide  $c$ .

For  $p$  prime,  $\binom{p}{r} = \frac{p!}{r!(p-r)!}$ . We show that  $p$  divides  $\binom{p}{r}$ , as follows. Since  $\binom{p}{r}$  is an integer,  $r!(p-r)!$  divides  $p! = p(p-1)!$ . But  $p$  does not divide  $r!$  or  $(p-r)!$  because both are products of numbers  $< p$ . So  $r!(p-r)!$  is coprime to  $p$ . Thus  $r!(p-r)!$  must divide  $(p-1)!$ , and so

$$\binom{p}{r} = p \left( \frac{(p-1)!}{r!(p-r)!} \right)$$

is an integer multiple of  $p$ . □

*Example 8.28* We can see examples of Proposition 13.15 by constructing Pascal's triangle.

The rows of Pascal's triangle are the binomial coefficients when you expand  $(x + y)^n$  by the Binomial Theorem. The first eight rows of Pascal's triangle are the coefficients for  $n = 0, 1, \dots, 7$ :

$$\begin{array}{ccccccc}
 & & & & 1 & & \\
 & & & & 1 & 1 & \\
 & & & & 1 & 2 & 1 \\
 & & & & 1 & 3 & 3 & 1 \\
 & & & & 1 & 4 & 6 & 4 & 1 \\
 & & & & 1 & 5 & 10 & 10 & 5 & 1 \\
 & & & & 1 & 6 & 15 & 20 & 15 & 6 & 1 \\
 & & & & 1 & 7 & 21 & 35 & 35 & 21 & 7 & 1
 \end{array} \cdot$$

As Proposition 13.15 proves, in the rows where the second number is prime (e.g., 2, 3, 5, 7) all of the interior entries in those rows are divisible by that prime.

**Proposition 8.29** *If  $p$  is prime, then  $(x + y)^p \equiv x^p + y^p \pmod{p}$  for all integers  $x$  and  $y$ .*

*Proof* Expand  $(x + y)^p$  by the Binomial Theorem. By Proposition 13.15, the prime  $p$  divides  $\binom{p}{r}$  for  $1 \leq r \leq p - 1$ , and so modulo  $p$ , all the binomial coefficients are  $\equiv 0 \pmod{p}$  except for  $r = 0$  and  $r = p$ . So

$$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

□

Fermat's Theorem is now provable by an easy induction argument:

**Theorem 8.30** (Fermat's Theorem) *If  $p$  is a prime, then every integer  $a$  satisfies the congruence  $a^p \equiv a \pmod{p}$ .*

*Proof* We prove the theorem for all integers  $a \geq 1$  by induction on  $a$ .

For  $a = 1$  it is obvious.

Suppose  $a$  is an integer  $\geq 1$ . Assume that  $a^p \equiv a \pmod{p}$ . Then

$$(a + 1)^p \equiv a^p + 1^p \pmod{p}$$

by Proposition 8.29. By the induction assumption,

$$a^p + 1^p \equiv a + 1 \pmod{p}.$$

So Fermat's Theorem is true for all  $a \geq 0$ .

If  $b$  is any integer, then  $b \equiv a \pmod{p}$  for some positive integer  $a$ . Since  $a^p \equiv a \pmod{p}$ , we have  $b^p \equiv a^p \equiv a \equiv b \pmod{p}$ . □

**On Euler's Theorem.** With more effort, we could also get a proof of Euler's theorem. But since we will prove Euler's Theorem in Chapter 10, we just do an interesting special case.

**Theorem 8.31** (Euler's Theorem) *If  $m = pq$  with  $p$  and  $q$  distinct odd primes, then for all numbers  $a$  coprime to  $m$ ,*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

To prove this, we will use

**Lemma 8.32** *Suppose  $m$  and  $n$  are coprime numbers. If  $a \equiv b \pmod{m}$  and  $a \equiv b \pmod{n}$ , then  $a \equiv b \pmod{mn}$ .*

*Proof* If  $a \equiv b \pmod{m}$ , then  $a - b$  is a multiple of  $m$ . Also, if  $a \equiv b \pmod{n}$ , then  $a - b$  is a multiple of  $n$ . So  $a - b$  is a common multiple of  $m$  and  $n$ , hence is a multiple of the least common multiple  $[m, n]$  of  $m$  and  $n$ .

But since  $m$  and  $n$  are coprime,  $[m, n] = mn$ . So  $mn$  divides  $a - b$ . Hence

$$a \equiv b \pmod{mn}.$$

□

Remember this lemma—we'll use it again later.

Now we prove Theorem 8.31.

*Proof* To prove that  $a^{\phi(m)} \equiv 1 \pmod{m}$  where  $m = pq$ ,  $p$  and  $q$  distinct primes, and  $a$  is coprime to  $m$ , it suffices to show by Lemma 8.32 that

$$a^{\phi(m)} \equiv 1 \pmod{p}$$

and also  $\pmod{q}$ . By Proposition 8.23,

$$\phi(m) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1).$$

Now  $a$  is coprime to  $p$ , so

$$a^{\phi(m)} = (a^{q-1})^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Theorem. Similarly,

$$a^{\phi(m)} = (a^{p-1})^{q-1} \equiv 1 \pmod{q}.$$

So we're done by Lemma 8.32. □

There is a complete proof of Euler's Theorem by this approach in Chapter 9 of [Ch09].

## 8.5 Finding High Powers Modulo $m$

For finding inverses by Euler's theorem and for other applications, we often want to find the least non-negative residue of a high power of a number modulo  $m$ . In this section we describe an efficient algorithm for doing this. D. Knuth calls the method the “XS binary method” ([Knu98], vol. 2, p. 461).

The idea is to write the exponent  $e$  in base 2, that is, as a sum of distinct powers of 2 (see Section 2.4). Doing so yields a sequence of instructions for finding  $a^e \pmod{m}$  by squaring and multiplying by the number  $a$ . To ensure that we never work with numbers larger than  $m^2$ , after each operation we reduce the result modulo the modulus  $m$ .

We illustrate the algorithm with an example.

*Example 8.33* The inverse of 17 modulo 89 is  $17^{87} \pmod{89}$  by Fermat's Theorem.

But if I put  $17^{87}$  into the calculator app on my “smart” phone, it gives me “1.11958265  $E + 107$ ”, which is completely useless for discovering that 21 is the inverse of 17 modulo 89.

We can find  $17^{87}$  modulo 89 efficiently without ever working with a number larger than  $89^2 = 7921$ .

We first find the exponent 87 as a sum of powers of 2:

$$\begin{aligned} 87 &= 64 + 16 + 4 + 2 + 1 \\ &= 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0, \end{aligned}$$

or, collecting the coefficients,

$$87 = (1, 0, 1, 0, 1, 1, 1)_2.$$

In this last expression, replace each comma by  $S$ , each 1 by  $X$ , and each 0 by  $\emptyset$ . We get

$$XS\emptyset SXS\emptyset SXSXSX.$$

Now discard the  $\emptyset$  (it means “empty set” in set theory). We’re left with an abbreviated set of instructions, reading from left to right:

$$XSSXSSXSXSX.$$

The instruction  $X$  means “multiply by 17 and reduce modulo 89.”

The instruction  $S$  means “square and reduce modulo 89”.

To find  $17^{87} \pmod{89}$ , start with the number 1 and apply the instructions from left to right. The result will be  $17^{87} \pmod{89}$ .

To see this, we first omit the “reduce modulo 89” part of each instruction. We get:

$$\begin{aligned} X : 1 &\longrightarrow 17 \\ S : 17 &\longrightarrow 17^2 \\ S : 17^2 &\longrightarrow 17^4 \\ X : 17^4 &\longrightarrow 17^5 \\ S : 17^5 &\longrightarrow 17^{10} \\ S : 17^{10} &\longrightarrow 17^{20} \\ X : 17^{20} &\longrightarrow 17^{21} \\ S : 17^{21} &\longrightarrow 17^{42} \\ X : 17^{42} &\longrightarrow 17^{43} \\ S : 17^{43} &\longrightarrow 17^{86} \\ X : 17^{86} &\longrightarrow 17^{87}. \end{aligned}$$

If we reduce modulo 89 at each step, we end up with the least non-negative residue of  $17^{87} \pmod{89}$ :

$$\begin{aligned} X : 1 &\longrightarrow 17 \pmod{89} \\ S : 17 &\longrightarrow 17^2 \equiv 22 \pmod{89} \\ S : 17^2 &\longrightarrow 17^4 \equiv 22^2 \equiv 39 \pmod{89} \\ X : 17^4 &\longrightarrow 17^5 \equiv 39 \cdot 17 \equiv 40 \pmod{89} \\ S : 17^5 &\longrightarrow 17^{10} \equiv 40^2 \equiv 87 \pmod{89} \\ S : 17^{10} &\longrightarrow 17^{20} \equiv 87^2 \equiv 4 \pmod{89} \\ X : 17^{20} &\longrightarrow 17^{21} \equiv 4 \cdot 17 \equiv 68 \pmod{89} \\ S : 17^{21} &\longrightarrow 17^{42} \equiv 68^2 \equiv 85 \pmod{89} \\ X : 17^{42} &\longrightarrow 17^{43} \equiv 85 \cdot 17 \equiv 21 \pmod{89} \\ S : 17^{43} &\longrightarrow 17^{86} \equiv 21^2 \equiv 85 \pmod{89} \\ X : 17^{86} &\longrightarrow 17^{87} \equiv 85 \cdot 17 \equiv 21 \pmod{89}. \end{aligned}$$

This method works for every modulus  $m$ , every number  $a$  and every exponent  $e$ , and is an efficient way to compute  $a^e \pmod{m}$ .

We’ll need the XS binary method for encrypting and decrypting in Chapters 9, 13 and 16. It is also useful for finding large prime numbers for use in cryptosystems, as shown in Sections 9.7 and 9.8.

Just because we have the XS-binary method for computing a high power modulo  $m$  does not mean that we should use it blindly.

*Example 8.34* Find  $52^{99}$  modulo 15.

We are free to replace 52 by any number congruent to 52 modulo 15, because, as is easily proven by induction (see Exercise 8.29),

**Proposition 8.35** *If  $a \equiv b \pmod{m}$ , then  $a^e \equiv b^e \pmod{m}$  for all numbers  $e \geq 1$ .*

Now  $52 \equiv 7 \equiv -8 \pmod{15}$ , so

$$52^{99} \equiv 7^{99} \equiv (-8)^{99} = -8^{99} = -2^{297} \pmod{15}.$$

We see that  $2^4 \equiv 1 \pmod{15}$ . So if we divide 297 by 4:  $297 = 4 \cdot 74 + 1$ , then

$$2^{297} \equiv (2^4)^{74} \cdot 2 \equiv 1^{74} \cdot 2 = 2 \pmod{15}.$$

So

$$52^{99} \equiv -2 \equiv 13 \pmod{15}.$$

The last part of the example generalizes to give

**Proposition 8.36** *Suppose  $(a, m) = 1$ . If  $f \equiv r \pmod{\phi(m)}$ , then  $a^f \equiv a^r \pmod{m}$ .*

This follows from Euler's Theorem, which says that  $a^{\phi(m)} \equiv 1 \pmod{m}$ .

Thus the XS-binary method only needs to be used on numbers of the form  $a^e \pmod{m}$  when  $a < m$  and  $e < \phi(m)$ .

**XS and Excel.** The XS-binary method is easy to implement for fairly small numbers in Microsoft Excel.

Suppose we want to find  $7^{171}$  modulo 447.

First we take the exponent 171, and obtain a succession of numbers, that you stack above 171, by the operations: divide by 2 if the number is even, subtract 1 if the number is odd, until you reach 1:

1
2
4
5
10
20
21
42
84
85
170
171

That sequence of numbers defines the XS operations.

Place the column of numbers, as shown, into cells A3 through A14.

Then in column B, beside each odd number place X, and beside each even number place S. The sequence of commands in the XS-binary algorithm is the sequence of X's and S's, from top to bottom.

1	X
2	S
4	S
5	X
10	S
20	S
21	X
42	S
84	S
85	X
170	S
171	X

In cell C1, place the number 7 that we want to raise to the power 171 modulo the modulus 447.

In cell D1, place the modulus 447.

In cell C2, place the number 1.

In cell D2, place: = MOD(C2, D\$1). This command replaces the number in cell C2 by its remainder modulo the modulus in cell D1, and puts it in cell D2.

In cell C3, place: = D2\*C\$1. This command takes the number in cell D2, multiplies it by the number in cell C1 and places the result in cell C3.

In cell C4, place: = D3^2. This command takes the number in cell D3, squares it, and places the result in cell C4.

Highlight cell C3, and copy the contents (using Ctrl C) into the clipboard. Paste (using Ctrl V) the contents into every cell in the C column where the row of the cell is headed by an X.

Highlight cell C4, and copy the contents into the clipboard. Paste the contents into every cell in the C column where the row of the cell is headed by an S. (The dollar sign in the command D2\*C\$1 fixes the base number 7 as you move down the C column.)

Highlight cell C2. Copy the contents into the clipboard. Highlight all of the D column headed by an X or an S, and paste the contents (with one Ctrl V) into all of those cells. (The dollar sign in the command MOD(C2, D\$1) tells Excel not to change that cell number as you paste the commands down the D column. That fixes the modulus in the column.)

If you did this correctly, the number (in C1) raised to the power 171 modulo the modulus (in D1) should be the number at the bottom of the D column.

This Excel setup will compute  $a^{171} \bmod m$  for any chosen number  $a$  (placed in C1) and any chosen modulus  $m$  (placed in D1).

Here is what the Excel looks like for computing  $7^{171} \bmod 447$ .

Row #	Col. A	Col. B	Col. C	Col. D
1			7	447
2			1	1
3	1	X	7	7
4	2	S	49	49
5	4	S	2401	166
6	5	X	1162	268
7	10	S	71824	304
8	20	S	92416	334
9	21	X	2338	103
10	42	S	10609	328
11	84	S	107584	304
12	85	X	2128	340
13	170	S	115600	274
14	171	X	1918	130

The computation shows that

$$7^{171} \equiv 130 \pmod{447}.$$

There are online calculators for finding powers modulo  $m$  for reasonably sized moduli: one such is [Tr09]. The scientific calculator that comes with Windows 10 is also useful for powers modulo  $m$ .

## Exercises

Except where stated otherwise, the exercises involving, “the order of  $a$  modulo  $m$ ” always means the order of  $a$  in the group  $U_m$  of units modulo  $m$  with the operation of multiplication.

- 8.1. Find the order of 7 modulo 45.
- 8.2. Find the order of 2 modulo 19. Then find the order of 8 modulo 19.
- 8.3. Show that 2 has order 12 modulo 13. Then find the orders of all the units of  $\mathbb{Z}_{13}$ , and verify that Fermat’s Theorem holds modulo 13.
- 8.4. Find the orders of the invertible elements of  $\mathbb{Z}_{24}$ .
- 8.5. (i) The order of 2 modulo 11 is 10 (Example 8.2). Find the order of 2 modulo 33; modulo 55; modulo 77; modulo 99.  
(ii) Find the order of 8 modulo 99.
- 8.6. Modulo 83,  $2^{41} \equiv 82$ . Find the order of 2 (mod 83).
- 8.7. Show without any computations that either 2 or  $-2$  has order 46 modulo 47, and the other has order 23 modulo 47.
- 8.8. Show that 2 has order 12 modulo 13. Then using Proposition 8.9, verify Fermat’s theorem for all  $a$  with  $(a, 13) = 1$ .
- 8.9. Find  $2^9 \pmod{11}$  with no computations of powers of 2.
- 8.10. Without any significant computations, explain why the order of 7 modulo 167 is at least 80.
- 8.11. Is there an element of order 15 in  $U_{97}$ ? If so, find it.

8.12. Let  $p$  be a prime number. Show that for all integers  $w$  and all numbers  $k$ ,

$$w^{1+(p-1)k} \equiv w \pmod{p}.$$

(Look at the two cases:  $(w, p) = 1$  and  $(w, p) = p$ .)

8.13. Find  $2^{49} \pmod{23}$ .

8.14. Show that the order of 2 modulo  $253 = 11 \cdot 23$  is at least 110.

8.15. Verify Euler's theorem for 1, 3, 7 and 9 modulo 10.

8.16. Compute  $2^{\phi(21)}$  modulo 21 and verify Euler's Theorem in that case.

8.17. Find  $40^{322} \pmod{21}$  using a method other than the XS binary method.

8.18. Find the order of 7 modulo  $172 = 43 \cdot 4$ .

8.19. (i) Find the order of 2 modulo  $119 = 7 \cdot 17$ .

(ii) Find the order of 3 modulo 119.

8.20. Observe that  $2^{10} = 1024 \equiv -1 \pmod{25}$ . Find the order of 2 modulo 25.

8.21. Prove that if  $a$  and  $m$  are coprime and  $f \equiv 1 \pmod{\phi(m)}$ , then

$$a^f \equiv a \pmod{m}.$$

8.22. Prove that

(i)  $\phi(p) = p - 1$  if  $p$  is prime;

(ii)  $\phi(p^n) = p^n - p^{n-1}$  if  $p$  is prime. (Count the multiples of  $p$  that are  $\leq p^n$ .)

8.23. Find  $\phi(m)$  by counting the numbers  $\leq m$  that are coprime to  $m$ , for  $m = 4, 5, 8, 10$  and 40. Then decide: is  $\phi(40) = \phi(10)\phi(4)$ ? Is  $\phi(40) = \phi(8)\phi(5)$ ?

8.24. Suppose  $m = pq$  is a product of two distinct odd primes. For which  $m$  is  $\phi(m)$  divisible by 8?

8.25. Give examples of  $a, b, m$  and  $n$  where  $(m, n) > 1$ , and

$$\begin{aligned} a &\equiv b \pmod{m} \text{ and } a \equiv b \pmod{n}, \\ \text{but } a &\not\equiv b \pmod{mn}. \end{aligned}$$

8.26. Find the least non-negative number  $a$  congruent to  $3^{340} \pmod{341}$ .

8.27. Find the least non-negative number  $a$  congruent to  $5^{1728} \pmod{1729}$ .

8.28. Let  $m = 252601$ . It is a fact (you don't need to verify) that

$$\begin{aligned} 3^{126300} &\equiv 67772 \pmod{252601} \\ 3^{252600} &\equiv 1 \pmod{252601}. \end{aligned}$$

Is then 252601 prime? composite? Or can we not decide for sure from the information given?

8.29. Prove by induction that if  $a \equiv b \pmod{m}$ , then  $a^e \equiv b^e \pmod{m}$  for all numbers  $e > 1$ .

8.30. Find  $23^{25} \pmod{49}$ .

8.31. Find  $25^{49} \pmod{23}$ .

8.32. Find  $100^{1234} \pmod{53}$ .

- 8.33. Find  $53^{100} \pmod{1234}$ .
- 8.34. Prove that if  $q > 2$  is odd and the order of  $3 \pmod{q}$  is  $q - 1$ , then  $q$  is prime. Why is this not contradicted by the fact that  $3^{90} \equiv 1 \pmod{91}$ ?
- 8.35. Show that if  $p$  and  $q$  are distinct primes, then  $\phi(pq) = (p - 1)(q - 1)$  as follows:  
Write the numbers  $0, 1, \dots, pq - 1$  in a rectangular array:

$$\begin{array}{ccccccccc}
 0 & 1 & 2 & \cdots & r & \cdots & p-1 \\
 p & p+1 & p+2 & \cdots & p+r & \cdots & p+(p-1) \\
 2p & 2p+1 & 2p+2 & \cdots & 2p+r & \cdots & 2p+(p-1) \\
 \vdots & & \vdots & & \vdots & & \vdots \\
 (q-1)p & (q-1)p+1 & (q-1)p+2 & \cdots & (q-1)p+r & \cdots & (q-1)p+p-1
 \end{array}$$

Cross out the first column. Show that every other column contains only numbers coprime to  $p$ , and is also a complete set of representatives modulo  $q$ , hence contains exactly one multiple of  $q$ . Conclude that  $\phi(pq) = (p - 1)(q - 1)$ .

- 8.36. Generalize the last exercise to show that if  $(a, b) = 1$  then  $\phi(ab) = \phi(a)\phi(b)$ .
- 8.37. The set  $(\mathbb{Z}_m, +)$  is a finite abelian group under addition, so the additive order of a number  $a$  in  $\mathbb{Z}_m$  is defined. Several of the results about order in this chapter are also valid for elements of  $(\mathbb{Z}_m, +)$  and are reasonable to prove.  
Define the order of  $a$  in  $(\mathbb{Z}_m, +)$  to be the smallest  $e > 0$  for which  $0 = ea = a + a + \dots + a$  ( $e$  summands).
- (i) (Additive Euler's Theorem) Show that for every  $a$  in  $(\mathbb{Z}_m, +)$ ,  $ma = 0$ .
  - (ii) Show that for every  $a$  in  $(\mathbb{Z}_m, +)$ , the order of  $a$  in  $(\mathbb{Z}_m, +)$  is  $m/(a, m)$ , hence divides  $m$ .
  - (iii) Show that if  $sa \equiv 0 \pmod{m}$ , then the order of  $a$  in  $(\mathbb{Z}_m, +)$  divides  $s$ .
  - (iv) Show that if the order of  $a$  in  $(\mathbb{Z}_m, +)$  is  $e$ , then the order of  $ra$  is  $e/(r, e)$ .
- 8.38. Explain how (ii) of Exercise 8.37 relates to solutions of the homogeneous congruence

$$ax \equiv 0 \pmod{m}.$$

- 8.39. Explain how (ii) of Exercise 8.37 relates to finding the least  $k > 0$  for which  $ak$  is a multiple of  $m$ .
- 8.40. Is there an element of order 15 in  $(\mathbb{Z}_{97}, +)$ ? If so, find it. (c.f. Exercise 8.11, above.)

# Chapter 9

## RSA Cryptography and Prime Numbers



RSA cryptography is a public key cryptosystem in wide use throughout the world. It was developed by R.L. Rivest, A. Shamir, and L. Adleman in 1978 [RSA78]. (It was independently discovered earlier by British government cryptologists, but their work remained secret until 1997: see [E87].)

RSA and the Diffie-Hellman key exchange cryptosystem (see Chapter 13) revolutionized cryptography when they were discovered in the mid-1970s. They were the first cryptosystems to solve the long-standing problem associated with private key cryptosystems such as the Vigenère and Vernam cryptosystems (see Chapter 1), or modern cryptosystems such as the US Government's Advanced Encryption Standard, AES (see Section 9.4): how can Alice and Bob share a private key while keeping it secret to everyone else?

RSA works by converting message words to numbers  $< m$  and encrypting them modulo  $m$ , where  $m$  is a product of two large prime numbers. The security of RSA is based on the idea that factoring the number  $m$  is a “hard problem”. What this means is that if the modulus  $m$  is sufficiently large, then factoring  $m$  would take so long (years, centuries) that it is in practice impossible to do.

In this chapter we describe RSA, review some efforts to factor RSA moduli, and then discuss how to find prime numbers to implement the cryptosystem. Further comments on RSA will appear in Sections 11.3, 13.8 and 14.6. Chapter 17 presents a method of factoring large numbers that was developed in 1982, no doubt motivated by the problem of attempting to factor RSA moduli.

### 9.1 RSA Cryptography

Alice and Bob, who are far apart, wish to send text messages back and forth to each other on the internet, and want them to be incomprehensible to Eve, who they suspect works for a government agency and can read anything they send.

To use the cryptosystem, they translate text into numbers in an agreed-upon way. For our examples, we'll count the alphabet as in Chapter 1, and replace each letter by its corresponding two-digit position number:

$$A \leftrightarrow 01; B \leftrightarrow 02; \dots; M \leftrightarrow 13; \dots; Z \leftrightarrow 26; \text{ (space)} \leftrightarrow 00.$$

Thus the word SEND MONEY would become 15 05 14 04 00 13 15 14 05 25. This sequence of digits is then split up into numerical words, each of which is separately encrypted.

After we describe how the method works, we'll explain why it is thought to be secure.

**How RSA works.** For Alice to send Bob a message, Bob sets up a cryptosystem for Alice to use. He chooses at random two different large primes  $p$  and  $q$ . (How he can do that will be discussed

later in this chapter.) For the cryptosystem to be secure, Bob must keep the two primes secret. He sets  $m = pq$ , the modulus, and chooses an encrypting exponent  $e$  that he privately checks is coprime to  $\phi(m) = (p - 1)(q - 1)$  (where  $\phi(m)$  is the number of units modulo  $m$ ). He computes the inverse  $d$  of  $e$  modulo  $\phi(m)$ , by solving the congruence

$$ed \equiv 1 \pmod{\phi(m)}.$$

Hence  $ed = 1 + k\phi(m)$  for some integer  $k$ .

The number  $d$  is Bob's decrypting exponent, which he keeps secret. Then Bob broadcasts the pair  $(m, e)$  to Alice (and, presumably, Eve). (The word "broadcast" implies that we assume that everyone can read what is sent.)

Alice wants to send Bob a message that consists of a sequence of numerical words, numbers  $w < m$ . To encrypt a word  $w$ , Alice uses the encrypting exponent  $e$  and the modulus  $m$  that Bob sent her, and computes

$$c = (w^e \pmod{m}).$$

So  $c$  is the number  $< m$  that is congruent to  $w^e$  modulo  $m$ . She broadcasts the encrypted word  $c$  to Bob.

To decrypt  $c$ , Bob uses his decrypting exponent  $d$  to compute

$$w' = (c^d \pmod{m})$$

(so  $w' < m$ ). Then  $w'$  will be the original word  $w$  of Alice. For  $e$  and  $d$  satisfy the congruence

$$ed \equiv 1 \pmod{\phi(m)},$$

so  $ed = 1 + k\phi(m)$  for some number  $k$ , and

$$\begin{aligned} w' &\equiv c^d \equiv (w^e)^d \\ &= w^{1+k\phi(m)} \\ &\equiv w \cdot (w^{\phi(m)})^k \\ &\equiv w \pmod{m} \end{aligned}$$

by Euler's Theorem (which says that  $w^{\phi(m)} \equiv 1 \pmod{m}$ ). Since both  $w$  and  $w'$  are numbers less than  $m$ , then  $w = w'$ .

*Example 9.1* Bob chooses the primes  $p = 31, q = 101$ , so  $m = 3131 = 31 \cdot 101$ . Then  $\phi(3131) = 30 \cdot 100 = 3000$ . Bob chooses the encrypting exponent  $e = 7$ , coprime to 30 and 100, and finds that

$$7 \cdot 2143 = 15001 \equiv 1 \pmod{3000}.$$

Then  $d = 2143$  is the decrypting exponent.

Bob broadcasts the pair  $(m, e) = (3131, 7)$  to Alice.

Alice wishes to send the message NO, or 1415. Since the largest possible number that corresponds to a pair of letters is 2626 (corresponding to ZZ), and  $2626 < m = 3131$ , Alice encrypts the single word  $w = 1415$ . She finds the least non-negative residue of  $1415^7 \pmod{3131}$  to be 607. So Alice broadcasts  $c = 607$  to Bob.

Bob takes the ciphertext 607, and finds the least non-negative residue modulo 3131 of  $607^{2143}$  (for example, by the XS binary algorithm). The resulting calculation yields 1415, which translates back into the message NO.

We'll discuss in Section 11.3 how Bob can decrypt more efficiently.

For a description of RSA from Rivest, Shamir and Adleman themselves, see [RSA11].

*Example 9.2* Here is a very small example. Bob chooses the primes 7 and 11, and sets  $m = 77$ . Then  $\phi(77) = \phi(7)\phi(11) = 6 \cdot 10 = 60$ . He chooses the encrypting exponent  $e = 13$ . Then his secret decrypting exponent is  $d = 37$ , since  $13 \cdot 37 = 481 \equiv 1 \pmod{60}$ . He sends  $m = 77$ ,  $e = 13$  to Alice.

Alice wants to send Bob the message GO, or 07, 15. So she computes

$$7^{13} \equiv 35 \pmod{77}$$

and

$$15^{13} \equiv 64 \pmod{77}$$

and sends 35, 64 to Bob. Bob decrypts by computing

$$35^{37} \equiv 7 \pmod{77}$$

and

$$64^{37} \equiv 15 \pmod{77}$$

and recovers the numerical message 07, 15, or GO.

At this point, an astute reader may ask, “But didn't we show that decrypting works because of Euler's Theorem? And doesn't Euler's Theorem,  $w^{\phi(m)} \equiv 1 \pmod{m}$ , require that  $w$  be coprime to  $m$ ? The number 7 isn't coprime to  $m = 77$ . Why does it still work?!”

All true. So we should explain why the cryptosystem works even on words  $w$  that are not coprime to the modulus  $m$ :

**Proposition 9.3** *Let  $m = pq$  be a product of two distinct primes, and let  $w$  be any integer. Then for all numbers  $k$ ,*

$$w^{\phi(m)k+1} \equiv w \pmod{m}.$$

*Proof* Since  $p$  and  $q$  are coprime, it suffices by Lemma 8.32 to show that

$$w^{\phi(m)k+1} \equiv w \pmod{p}$$

and

$$w^{\phi(m)k+1} \equiv w \pmod{q}.$$

We'll show it modulo  $p$ . The modulo  $q$  case is identical.

Since  $p$  is prime, either  $w$  is coprime to  $p$  or  $p$  divides  $w$ .

Case 1.  $(w, p) = 1$ . Then by Fermat's Theorem,  $w^{p-1} \equiv 1 \pmod{p}$ . Recalling that  $\phi(m) = \phi(p)\phi(q) = (p-1)(q-1)$  (since  $p$  and  $q$  are distinct primes), we have

$$w^{\phi(m)k+1} = w^{(p-1)(q-1)k} \cdot w = (w^{p-1})^{(q-1)k} \cdot w \equiv 1^{(q-1)k} \cdot w \equiv w \pmod{p},$$

as desired.

Case 2.  $p$  divides  $w$ . Then both  $w$  and  $w^{\phi(m)k+1}$  are congruent to 0 modulo  $p$ , so

$$w^{\phi(m)k+1} \equiv w \pmod{p}.$$

□

In other words, if  $w$  is not coprime to  $m$ , then

$$w^{\phi(m)} \equiv 1 \pmod{m}$$

is never true. But it is true that

$$w^{\phi(m)k} \cdot w \equiv w \pmod{m}$$

for all  $w$  as long as  $m$  is squarefree, that is,  $m$  is a product of distinct primes.

This result is similar to the two versions of Fermat's Theorem in Section 8.2. For  $p$  a prime number, one version is:

*For all integers  $a$  coprime to  $p$ ,  $a^{p-1} \equiv 1 \pmod{p}$ .*

The other is:

*For all integers  $a$ ,  $a^p \equiv a \pmod{p}$ .*

In real-world implementations of RSA, the modulus  $m$  is a product of two very large primes  $p$  and  $q$ . If  $w$  is a randomly chosen word with  $1 \leq w < m$ , the probability that  $w$  is coprime to  $m$  is

$$\frac{\phi(m)}{m} = \frac{(p-1)(q-1)}{pq}.$$

For  $p$  and  $q$  of  $n$  digits, that number is approximately

$$\left(\frac{10^n - 1}{10^n}\right)^2 \sim 1 - \frac{2}{10^n}.$$

If, say,  $n$  is 50, then the likelihood of encrypting a random word that is not coprime to  $m$  is approximately  $2/(10^{50})$ . But the point of Proposition 9.3 is that RSA works even if the word is not coprime to the modulus.

## 9.2 Why Is RSA Effective?

Now suppose Eve eavesdrops on the messages between Alice and Bob. Then she knows  $m$  and  $e$  and each encrypted word  $c$ .

To decrypt the encrypted word  $c$ , Eve needs to undo the encryption,  $c = w^e \pmod{m}$  by finding some decrypting exponent  $d$ . She could do so by solving the congruence  $ed \equiv 1 \pmod{\phi(m)}$  to find  $d$ . But that requires knowing  $\phi(m)$ , and that is as hard a problem as factoring  $m$ . For if she can factor  $m$  she can find  $\phi(m)$ , but conversely, if she knows  $m$  and  $\phi(m)$ , then she can factor  $m$  (see Exercise 9.7).

More generally, as seen in Exercise 9.6, there is more than one decrypting exponent  $d$  so that  $w^{ed} \equiv 1 \pmod{m}$ . But if Eve can find some decrypting exponent  $d$ , then Eve can factor  $m$ : this is a result of D. Boneh that we'll prove in Section 14.6.

So the security of RSA is based entirely on the difficulty of factoring the modulus.

But Bob has kept the factorization of  $m$  secret. So Eve would need to figure out the factorization of  $m$  by herself.

And factoring large numbers into products of primes is a hard problem.

The security of an RSA cryptosystem lies in the assumption that Eve, who knows  $m$  but not its factorization, will be unable to determine the factorization of  $m$  in a reasonable amount of time.

How large should  $m$  be? The recommended size of  $m$  has increased over time with improvements in computer power and in factoring algorithms. A public measure of progress is illustrated by the RSA Factoring Challenge, posed by RSA Laboratories in 1991. The challenge was a published list of numbers that are products of two primes that were offered as factoring challenges. (See [RSA15] for the list and a summary of results.) The smallest  $m$ , called RSA-100, a number of 100 digits, was factored within two weeks of the challenge. Subsequently, RSA-129 was factored in 1994 by A. Lenstra and a team involving 1600 computers over a period of eight months, and RSA-155 was factored in 1999 by a team of 17 researchers from six countries managed by H. Te Riele, a computation requiring about 8400 MIPS years (“One MIPS year is the equivalent of a computation during one full year at a sustained speed of one million instructions per second.” [CDL00]).

The largest number on the list that has been factored (as of 2015) is RSA-768, of 232 decimal digits (= 768 binary digits), factored by a thirteen member team from six countries led by T. Kleinjung [KAF10]. That effort was in four phases: half a year on 80 processors setting up the Number Field Sieve algorithm; then sieving, “which was done on many hundreds of computers and took almost two years”. The matrix step took “a couple of weeks on a few processors”, and the final factorization of RSA-768 took less than a half day.

The RSA-768 authors speculated that a 1024-bit RSA modulus could reasonably be expected to be factored well before 2020 by an academic consortium, and so they recommended phasing out usage of 1024-bit RSA moduli by 2014.

Thus by 2013, sources on the web suggested that for adequate long-term security, a modulus  $m$  should have at least 616 decimal digits, or 2048 bits, a product of two 308 digit primes.

In 2015, sources on the web (e.g. [Cs15]) recommended that for moderately high security, involving information that needs to be secure for weeks or months, a 2048 bit modulus was viewed as acceptable. But for high security, information that should remain secure for years, the minimum size modulus is recommended to have 3072 bits, or 924 decimal digits, a product of two 462 digit prime numbers. An example of the latter might be information on secret agents embedded in a hostile nation, information that should remain secret for decades.

Those estimates are based on the assumption that quantum computing is not available. However, if (when?) large quantum computers become viable, then RSA (and the other cryptosystems described in this book) will become insecure. An algorithm due to Peter Shor [Sh97] can factor numbers quickly (in “polynomial time”) on a quantum computer. As of 2014, the only numbers known to have been factored on a quantum computer are very small, such as 15, 21 and 143 (and apparently also 56153 – see [Zy14]), numbers that factor into a product of two primes whose base 2 representations differ in only two bits:

$$\begin{aligned} 143 &= 11 \cdot 13 = (1011) \cdot (1101); \\ 56153 &= 233 \cdot 241 = (11101001) \cdot (11110001). \end{aligned}$$

For a 2016 news article, “Quantum computer comes closer to cracking RSA encryption”, see [No16], which speculates that current RSA encryption will be safe from quantum computer attacks for perhaps 15 to 30 years. See also Section 13.5.

See also [IBM17], an announcement from IBM of a universal quantum computing processor, with 16 superconducting qubits, that is available for public use. The magazine *Nature*, reporting on this computer on May 24, 2017 [Na17] stated that “IBM is one of several companies and academic labs racing to build the first quantum machine that could outperform any existing classical computer, a threshold expected to be passed at around 50 qubits.” Since 2017, interest in quantum computing has increased greatly, and the above information will be obsolete by the time you read this.

### 9.3 Signatures

RSA cryptosystems can be used for signatures.

Suppose Alice is a reporter who is about to visit a region of the world where the communication network to the outside world is under the control of an authority, call it Malus, that may find it convenient to send out false messages under her name. When Alice sends a message home to Bob, she wants Bob to know that the message is actually from her.

So before she goes on her trip, she broadcasts an RSA cryptosystem  $(m, e)$  to Bob, where  $m$  is the modulus and  $e$  is an encrypting exponent. She knows the factorization of  $m$  and so knows the corresponding decrypting exponent  $d$ , but she keeps  $d$  secret.

When she wants to send a message  $w$  to Bob, she takes the message and encrypts it using the modulus  $m$  and her secret exponent  $d$  to get  $c = (w^d \bmod m)$ . When Bob receives the encrypted message, he decrypts using the known exponent  $e$ .

Since everyone knows  $m$  and  $e$ , everyone can read Alice's message. But in order to send out a fraudulent message  $w$  in Alice's name, Malus would need to encrypt his fraudulent message  $w$  just as Alice would: so that the resulting encrypted message  $c$  would decrypt by  $w = c^e \pmod{m}$ . Thus Malus would need to find an exponent  $d$  with the property that for all  $w$ ,

$$w^{ed} \equiv w \pmod{m}.$$

Thus Malus would have to crack the RSA code  $(m, e)$ .

Of course, the signature feature can be added to a secure message, so that when Alice sends a message to Bob, Alice will know that only Bob can read it, and Bob will know that only Alice could have sent it.

To illustrate how that feature works, suppose Bob is a stock broker in New York City and Alice is a wealthy client, day-trading on her wireless laptop on the beach at Phuket, 9000 miles away. Alice wants to send buy and sell orders to Bob. Bob wants to be certain that when he receives an order from Alice, it is authentic.

For authenticity, Alice sets up an RSA cryptosystem  $(m_A, e_A)$ , and for security, Bob sets up a different RSA system  $(m_B, e_B)$ . Both RSA systems could be published or broadcast. But only Bob would know the secret decrypting exponent  $d_B$  for his system, and only Alice would know the secret decrypting exponent  $d_A$  for her system.

To send an order to Bob, Alice encrypts her order twice: first by using her pair  $(m_A, d_A)$  with the secret  $d_A$  to create a signature, then by using the pair  $(m_B, e_B)$  with the public  $e_B$  for secrecy. When Bob receives the encrypted order, he first decrypts it with the secret  $d_B$  that only he knows, then he uses the public  $e_A$  to recover Alice's plaintext order.

Since Alice encrypted the message using the secret exponent  $d_A$ , which broker Bob was able to decrypt, Bob would know that only Alice could have sent the message.

Since only Bob knows the secret exponent  $d_B$ , Alice would know that only Bob could decrypt the message.

In particular, Eve can't decrypt the order because she would need the secret  $d_B$  that only Bob knows, and Malus can't impersonate Alice because he would need the secret  $d_A$  that only Alice knows.

Thus both Alice and Bob are assured of the authenticity and secrecy of the order Alice sent Bob.

In Section 11.3 we'll discuss some implementation issues for RSA: how to decrypt more efficiently, and how to avoid known pitfalls in the choice of primes. In Chapter 17 we'll describe a modern factoring algorithm. Later in this chapter we'll discuss how to find large primes.

## 9.4 Symmetric Versus Asymmetric Cryptosystems

Prior to the mid-1970s, every publicly known cryptosystem was a symmetric cryptosystem. That means, whatever special knowledge was needed by Alice to encrypt a message was also needed by Bob to decrypt the message, and vice versa.

The additive and multiplicative Caesar ciphers, and the Vigenère and Vernam ciphers of Chapters 1 and 2, are examples of symmetric cryptosystems. For example, in the original additive Caesar cipher, to encrypt a message (in words made up of letters), replace each letter by the letter three positions to the right in the alphabet. The key is “three”. To decrypt an encrypted message, replace each letter by the letter three positions to the left in the alphabet.

To use any of those systems, Alice and Bob need to have the same key  $k$ .

Modern symmetric cryptosystems are enormously useful—they are computationally very fast, and given sufficiently long keys, secure. So they are in common use today.

One system, the Data Encryption Standard (DES), developed in 1977, uses a 56 bit key to encrypt and decrypt. So there are  $2^{56} \sim 10^{17}$  possible keys. For a number of years it was the standard cryptosystem used by the US Government for encrypting sensitive but unclassified documents. But with the increase in computing power, a “brute force” attack (try every key) became possible and was in fact used in 1997 to decrypt a DES message in response to a challenge from the inventors of RSA.

So around the turn of the century, DES was phased out in favor of AES, the Advanced Encryption Standard (known as Rijndael prior to adoption by the National Institute of Standards and Technology, U.S. Department of Commerce, in 2001). AES is a symmetric key cryptosystem that uses 256 bit keys. (We’ll discuss AES very briefly in Section 18.5.)

The major problem with symmetric cryptosystems is key sharing. If Alice and Bob are physically separated and want to use a symmetric cryptosystem, how can they agree on the key without an eavesdropper learning about it?

RSA solves that problem. To set up a symmetric cryptosystem, Alice can send Bob the key, or instructions on how to find the key, using RSA. For example, Alice can use RSA to encrypt a 256 bit key  $k$ . She sends the encrypted key to Bob. Bob can decrypt Alice’s message and learn the key  $k$ , and then Alice and Bob will be ready to send messages by a symmetric cryptosystem that requires a shared 256 bit key.

So public key cryptosystems such as RSA solve the problem of key exchange for use in a symmetric key cryptosystem.

## 9.5 There are Many Large Primes

An RSA cryptosystem requires large primes. How many are there?

The ancient Greeks knew the answer—it is in Euclid ([Eu00], Book IX, Proposition 20).

**Theorem 9.4** *There are infinitely many primes.*

*Proof* (Euclid) Suppose the set of primes is finite in number: let us denote them by  $p_1, p_2, \dots, p_r$ . Consider the number

$$m = p_1 p_2 \cdots p_r + 1.$$

It must have a prime divisor  $q$ . If  $q$  were one of the primes  $p_1, p_2, \dots, p_r$ , then  $q$  would divide  $m - 1 = p_1 p_2 \cdots p_r$ , and so  $q$  would divide  $m - (m - 1) = 1$ , impossible. So  $q$  cannot be one of the primes  $p_1, p_2, \dots, p_r$ . Thus  $q$  must be a new prime. This contradicts the assumption that  $p_1, \dots, p_r$  were all the primes. So the number of primes cannot be finite.  $\square$

But for RSA, far more interesting is an estimate of how many primes there are of a certain size. For example, how many primes are less than some given number  $n$ ?

**Definition** Let  $\pi(x)$  be the function defined for all real numbers  $x > 0$  by

$$\pi(x) = \text{the number of prime numbers } < x.$$

The sequence of primes begins

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \dots$$

$$\text{so } \pi(3) = 2, \pi(10) = 4, \pi(\sqrt{200}) = 6, \pi(25) = 9, \pi(100) = 25.$$

The celebrated Prime Number Theorem, proved in 1896 independently by Hadamard and de la Vallée Poussin, is

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln(x)} = 1.$$

Here  $\ln(x)$  is the natural logarithm of  $x$ .

For estimating  $\pi(x)$  for a fixed real number  $x$ , such as  $x = 10^{100}$  (that is, to estimate the number of primes of at most 100 digits), fairly precise numerical results have been found. Chebyshev in 1850 proved that  $\pi(x) < 1.10555(x / \ln x)$  for all  $x$ , and in 1962 Rosser and Schoenfeld proved that  $x / \ln(x) \leq \pi(x)$  for all  $x > 17$ . Thus the number of primes  $< x$  is squeezed between two easily computable bounds: for all  $x > 17$ ,

$$\frac{x}{\ln(x)} \leq \pi(x) \leq (1 + \epsilon) \frac{x}{\ln(x)}$$

where  $1 + \epsilon < 1.10555$  for all  $x$ , and  $\epsilon$  approaches 0 as  $x$  goes to infinity.

Dividing these inequalities by  $x$  yields

$$\frac{1}{\ln(x)} \leq \frac{\pi(x)}{x} \leq (1 + \epsilon) \frac{1}{\ln(x)}.$$

This says that on average, one of every  $\ln x$  numbers less than  $x$  is prime. In particular, if  $x = 10^d$ , then on average, one of every  $\ln 10^d = d \ln 10$  numbers of at most  $d$  digits is prime.

For example, if we let  $x = 10^{10}$ , then since  $\ln 10 = 2.3026$ , among all the numbers less than  $10^{10}$ , one of every  $10 \ln(10) = 23$  numbers is prime.

For  $x = 10^{100}$ , among numbers of 100 digits or less, one of every  $100 \ln 10 = 230$  numbers is prime.

These results (whose proofs are well beyond the scope of this book) show that large primes are not at all scarce. Thus if we need some prime numbers of around 100 digits (for example, for cryptography) and have a method for quickly checking whether a given large number is prime or not (we'll show soon that such a method exists), then if we randomly select numbers of 100 digits or less, we should expect that about 1 of every 230 numbers we select will in fact be prime.

If we want to find primes of exactly  $d$  digits, one can adapt the Chebyshev and Rosser-Schoenfeld bounds (see [Ch09], Chapter 4) to show that the number of primes of exactly  $d$  digits is

$$> \frac{C}{d \ln 10} 10^d$$

where the constant  $C$  satisfies

$$1 > C > .9883 - .1228 \frac{1}{d-1}.$$

For  $d = 100$ ,  $C \geq .987$ . So the proportion of primes among 100 digit numbers is at least

$$\frac{.987}{100 \ln 10} > \frac{1}{234}.$$

We noted that 308 digit primes are recommended for modern RSA systems. For  $d = 308$ ,  $C \geq .9879$ . So the proportion of primes among 308-digit numbers is at least

$$\frac{.9879}{308 \ln 10} > \frac{1}{718}.$$

So it is helpful to know that primes of 308 digits are not hard to find. In fact, the number

$$\pi(10^{308}) - \pi(10^{307})$$

of primes of exactly 308 digits is

$$\geq 9 \cdot 10^{307} \frac{.9879}{308 \ln(10)} > 10^{305}.$$

## 9.6 Finding Large Primes

There are many large primes available, as we just saw. But how do we find some?

To start, pick a random number  $n_0$  of  $d$  digits. For concreteness, let's assume  $d = 100$ . Then look at the next five thousand numbers. Since 5000 is roughly 20 times 234, we would expect around 20 prime numbers among those thousand numbers.

But how do we decide which among those numbers are prime?

The basic idea is to look at each of the 5000 numbers and try to show it is composite. If we fail to show that the number is composite, then we will decide it is prime. And we'll be extremely unlucky if we're wrong.

We begin by removing numbers easily seen to be composite, using trial division, or equivalently, the Sieve of Eratosthenes. Starting with  $n_0$ , we cross out all the multiples of 2 and 5, and then, starting with the first multiple of 3 that is  $\geq n_0$ , we cross out every third number. Then repeat that with each prime  $p < 1000$ : find the first multiple of  $p$  in the set of 5000 numbers, then cross out every  $p$ th number beyond that until we have crossed out every multiple of  $p$  in the set of 5000 numbers. (You should try that with the numbers from 1 to 50, crossing out all multiples of 2, 3, 5 and 7. The numbers not crossed out are prime.)

If we want, we could then try dividing the remaining numbers by primes  $< B$  where  $B$  is as large as the computer available to us can handle quickly.

What we have left are numbers that are not divisible by any primes  $< B$ . That set includes all the primes among our 5000 numbers.

But we're likely to miss many composite numbers by trial division.

*Example 9.5* For a small example, let us look for primes among the one hundred numbers between 2508001 and 2508100.

Trial division by primes  $< 50$  eliminates 82 composite numbers in this set. The remaining numbers are:

2508001				
	2508013	2508017		2508029
2508031				
2508041	2508043	2508047	2508049	2508059
	2508053			
		2508067		
2508071	2508073			2508089
	2508083			
2508091		2508097		

It turns out that 13 of these 18 numbers are prime.

Trial division is hopelessly inefficient for primality testing or factoring for large numbers  $n$ .

Suppose, for example, that  $n$  is a number of 308 digits. If  $n$  happened to be prime, we would need to trial divide  $m$  by all primes of 154 digits or less to be sure by trial division that  $n$  is prime. But by the Prime Number Theorem there are approximately  $10^{154}/154 \ln 10 = 2.82 \cdot 10^{151}$  primes of 154 or fewer digits. To get a sense of size, the world's fastest computer (as of November 2013) can only do around  $33 \cdot 10^{15}$  floating point operations per second. There were (as of 2010) around 2 billion computers in the world. The sun is projected to burn itself out within  $10^{19}$  seconds. So even if every computer in the world were as fast as the world's fastest, and all worked on the trial division, by the time the sun died they could do trial division on  $n$  only by around  $10^{44}$  primes.

We cannot determine if a large number  $m$  is prime by the test of failing to find a factor of  $m$  by trial division. We need another test.

## 9.7 The $a$ -Pseudoprime Test

One of the simplest tests involves Fermat's Theorem.

Fermat's Theorem says that if  $p$  is a prime number, then for any integer  $a$  relatively prime to  $p$ ,

$$a^{m-1} \equiv 1 \pmod{p}.$$

The contrapositive of Fermat's theorem is the following:

*Given a number  $m > 1$ , suppose that  $a^{m-1} \not\equiv 1 \pmod{m}$  for some  $a$  with  $1 \leq a < m$ . Then  $m$  is composite.*

So Fermat's Theorem gives a collection of compositeness tests, one for each  $a$  with  $1 \leq a \leq m$ :

**Definition** Given a number  $m$ , suppose  $a$  is a number with  $1 < a < m$ . Then  $m$  passes the  $a$ -pseudoprime test if  $a^{m-1} \equiv 1 \pmod{m}$ .

If  $m$  fails the  $a$ -pseudoprime test for some  $a$  with  $1 < a < m$ , then  $m$  is composite.

For example, we can use the 2-pseudoprime test to show that 9 is not prime, by observing that  $2^8 \equiv 4 \not\equiv 1 \pmod{9}$ . By Fermat's theorem: if 9 were prime, then  $2^8$  would be congruent to 1 ( $\pmod{9}$ ): since it isn't, 9 can't be prime.

On the other hand, the 2-pseudoprime test is not a primality test. We can't conclude that 561 is prime by determining that  $2^{560} \equiv 1 \pmod{561}$  (which is true), because in fact 561 is not prime—it is clearly divisible by 3.

But as a test for compositeness of a number  $m$ , seeing if  $2^{m-1} \equiv 1 \pmod{m}$  can be done rather quickly and is surprisingly effective.

*Example 9.6* Let us look for composite numbers among the eighteen numbers between 2508001 and 2508100 that survived our trial division in Example 9.5:

$$\begin{aligned} & 2508001, 2508013, 2508017, 2508029, 2508031, 2508041, \\ & 2508043, 2508047, 2508049, 2508053, 2508059, 2508067, \\ & 2508071, 2508073, 2508083, 2508089, 2508091, 2508097. \end{aligned}$$

Every prime between 2508001 and 2508100 must be among these 18 numbers.

To test these numbers, we try the 2-pseudoprime test. We find that four of the numbers fail that test, and so are composite:

$$\begin{aligned} 2^{2508028} &\equiv 974611 \pmod{2508029} \\ 2^{2508030} &\equiv 907491 \pmod{2508031} \\ 2^{2508058} &\equiv 2404842 \pmod{2508059} \\ 2^{2508070} &\equiv 2324206 \pmod{2508071}. \end{aligned}$$

Thus 2508029, 2508031, 2508059, and 2508071 are composite.

We are left with fourteen potential primes out of the original 100 numbers.

(The factorizations of the candidates that failed the 2-pseudoprime test are:

$$\begin{aligned} 2508029 &= 1151 \cdot 2179 \\ 2508031 &= 59 \cdot 42509 \\ 2508059 &= 137 \cdot 18307 \\ 2508071 &= 463 \cdot 5417. \end{aligned}$$

Of course, there is nothing special about  $a = 2$ . We could apply the 3-pseudoprime test on the 13 remaining potential primes.

If we do, we find that they all pass the 3-pseudoprime test. We can also try the 5-pseudoprime test, etc.

**Definition** A composite number  $m$  for which  $2^{m-1} \equiv 1 \pmod{m}$  is called a 2-pseudoprime.

A composite number  $m$  for which  $a^{m-1} \equiv 1 \pmod{m}$  is called an  $a$ -pseudoprime.

Is it possible for a number  $m$  to pass many  $a$ -pseudoprime tests and be composite?

It turns out that the answer is “yes”:

**Definition** A Carmichael number is a composite number  $m$  with the property that

$$a^{m-1} \equiv 1 \pmod{m}$$

for all numbers  $a$  coprime to  $m$ .

Carmichael numbers are numbers  $m$  that are  $a$ -pseudoprimes for every number  $a$  coprime to  $m$ . And although rare, they exist. The seven Carmichael numbers  $< 10,000$  are 561, 1105, 1729, 2465, 2821, 6801 and 8911. By comparison, there are 1229 prime numbers  $< 10,000$ . In 1992 it was proved [AGP94] that there are infinitely many Carmichael numbers. (See [PSW80] for counts and lists of 2-pseudoprimes, strong 2-pseudoprimes and Carmichael numbers  $< 25 \cdot 10^9$ .)

Given the existence of Carmichael numbers, we need to strengthen our test.

## 9.8 The Strong $a$ -Pseudoprime Test

Suppose we have a number  $m$  that we think might be prime because it has no small prime divisors. We start doing  $a$ -pseudoprime tests. But how do we actually do an  $a$ -pseudoprime test?

The XS binary algorithm was presented in Section 8.5. We review it here.

We write  $m - 1$  in base 2:  $m - 1 = (a_d, a_{d-1}, a_{d-2}, \dots, a_2, a_1, a_0)_2$ , where each  $a_i$  is 0 or 1. For example, to find 560 in base 2, we see that

$$\begin{aligned} 560 &= 512 + 32 + 16 \\ &= 1 \cdot 2^9 + 0 \cdot 2^8 + 0 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 \\ &= (1, 0, 0, 0, 1, 1, 0, 0, 0, 0)_2. \end{aligned}$$

To obtain the sequence of instructions on how to find  $a^{m-1} \pmod{m}$ , we take the base two representation of  $m - 1$ , replace each comma by S, replace each bit that is 1 by X, and slash all the bits that are 0. We then think of X as the instruction “multiply by  $a$  and reduce modulo  $m$ ”, S as the instruction “square and reduce modulo  $m$ ”, and  $\emptyset$  as the instruction “do nothing”.

So our sequence of instructions for finding  $a^{560} \pmod{m}$  is

$$XS\emptyset S\emptyset SXSXS\emptyset S\emptyset S\emptyset$$

or since  $\emptyset$  means “do nothing”, we omit every  $\emptyset$ , to leave

$$XSSSXSSXSSS.$$

Without reducing modulo  $m$ , we would start with 1 and compute  $a^{560}$  by following the sequence of instructions from left to right:

$$\begin{aligned} 1 &\rightarrow a \rightarrow a^2 \rightarrow a^4 \rightarrow a^8 \rightarrow a^{16} \rightarrow a^{17} \\ &\rightarrow a^{34} \rightarrow a^{35} \rightarrow a^{70} \rightarrow a^{140} \rightarrow a^{280} \rightarrow a^{560}. \end{aligned}$$

To compute  $a^{560} \pmod{561}$  we should reduce each number modulo 561 after each computation, to keep the numbers less than  $561^2 = 314721$ .

Now it turns out that by doing the  $a$ -pseudoprime test in this way, we are also testing the primality of  $m$  in a different way.

Since any potential prime number  $m$  is odd,  $m - 1 = 2^e f$  for some  $e > 0$  and some odd number  $f$ . For example, for  $m = 561$ ,  $m - 1 = 2^4 \cdot 35$ , so  $e = 4$  and  $f = 35$ . Looking at the sequence of instructions for  $m - 1 = 560$ , you can see that the instructions starting with 1 at the left and ending with the last X is the set of instructions for computing  $a^f = a^{35} \pmod{m}$ , and the remaining instructions consist of squaring  $e = 4$  times. That fact, together with the next proposition, gives us a stronger primality test almost for free.

**Proposition 9.7** If there exists a number  $b$  not congruent to 1 or  $-1$  modulo  $m$  so that  $b^2 \equiv 1 \pmod{m}$ , then  $m$  is composite.

*Proof* Suppose  $b^2 \equiv 1 \pmod{m}$ . Then  $m$  divides  $b^2 - 1 = (b+1)(b-1)$ . If  $b$  is not congruent to 1 or  $-1$  modulo  $m$ , then  $m$  does not divide  $b+1$  and  $m$  does not divide  $b-1$ . But the Coprime Divisibility Lemma (from Chapter 3) implies that if  $m$  is a prime and  $m$  divides a product  $rs$  of integers, then  $m$  divides  $r$  or  $m$  divides  $s$ . So  $m$  cannot be prime.  $\square$

Incorporating this idea into the computations gives a more subtle test for primeness.

*The strong  $a$ -pseudoprime test.* For  $m$  odd, let  $m = 2^e f$  with  $f$  odd. Compute  $a^{m-1}$  modulo  $m$  by the XS-binary algorithm above:

$$a \rightarrow a^2 \rightarrow \dots \rightarrow a^f \rightarrow a^{2f} \rightarrow \dots \rightarrow a^{2^{e-1}f} \rightarrow a^{2^e f} = a^{m-1} \pmod{m}$$

Then:

- If  $a^{m-1} \not\equiv 1 \pmod{m}$ , then  $m$  is composite (by Fermat's Theorem).

Suppose  $a^{m-1} = a^{2^e f} \equiv 1 \pmod{m}$ . Look at the sequence

$$(a^f, a^{2f}, \dots, a^{2^{e-1}f}, a^{2^e f} = 1) \pmod{m}.$$

There are four possibilities for this sequence modulo  $m$ :

$$\begin{aligned} & (1, 1, \dots, 1) \\ & (\dots, -1, 1, \dots, 1) \\ & (\dots, b, 1, \dots, 1) \\ & (\dots, c) \end{aligned}$$

where  $b$  is not  $\equiv 1$  or  $-1 \pmod{m}$ , and  $c \not\equiv 1 \pmod{m}$ .

In the first two cases,  $m$  passes the strong  $a$ -pseudoprime test.

In the third case  $m$  is an  $a$ -pseudoprime but fails the strong  $a$ -pseudoprime test, so is provably composite, by Proposition 9.7.

In the last case  $m$  fails the  $a$ -pseudoprime test, so is provably composite by Fermat's Theorem.

**Definition** An odd number  $m$  is a *strong  $a$ -pseudoprime* if  $m$  is composite but passes the strong  $a$ -pseudoprime test.

To restate the definition:  $m$  is a strong  $a$ -pseudoprime if and only if  $m$  is composite,  $a^{m-1} \equiv 1 \pmod{m}$ , and one of two things occurs.

- (1)  $a^f \equiv 1 \pmod{m}$ , or
- (2) The rightmost number in the sequence that is not  $\equiv 1 \pmod{m}$  is  $\equiv -1 \pmod{m}$ .

If  $m$  is prime, either (1) or (2) always occurs.

*Example 9.8* Consider  $m = 29$ ,  $m-1 = 7 \cdot 2^2$ : trying  $a = 2, 5$  and  $7$  we find:

$$2^7 \equiv 12; \quad 2^{14} \equiv 28 \equiv -1, \quad 2^{28} \equiv 1 \pmod{29},$$

so we get the sequence  $(12, -1, 1)$  modulo 29.

$$5^7 \equiv 28 \equiv -1, \quad 5^{14} \equiv 1 \pmod{29},$$

so we get the sequence  $(-1, 1, 1)$  modulo 29.

$$7^7 \equiv 1 \pmod{29},$$

so we get the sequence  $(1, 1, 1)$ .

So  $m = 29$  passes the strong 2-, 5- and 7-pseudoprime tests.

*Example 9.9* Let  $m = 561$ . We look at the sequence

$$(a^{35}, a^{70}, a^{140}, a^{280}, a^{560}) \pmod{561}.$$

For  $a = 2$ , this sequence is  $(263, 166, 67, 1, 1)$ , so 561 fails the strong 2-pseudoprime test.

For  $a = 7$ , this sequence is  $(241, 298, 166, 67, 1)$ , so 561 fails the strong 7-pseudoprime test.

In both cases we see that

$$67^2 \equiv 1 \pmod{561},$$

so 561 cannot be prime. In fact, 561 divides

$$67^2 - 1 = (67 - 1)(67 + 1) = 66 \cdot 68$$

and doesn't divide either factor.

The example generalizes to give a stronger version of Proposition 9.7: if  $m$  is an  $a$ -pseudoprime but fails the strong  $a$ -pseudoprime test, not only is  $m$  necessarily composite, but  $m$  is easy to factor:

**Proposition 9.10** *Given a number  $m$ , suppose there is a number  $b$  so that  $b^2 \equiv 1 \pmod{m}$  but  $b$  is not congruent to 1 or  $-1$  modulo  $m$ . Then the greatest common divisors  $(m, b - 1)$  and  $(m, b + 1)$  are non-trivial factors of  $m$ .*

*Proof* If  $m$  does not divide  $b - 1$  or  $b + 1$ , then  $(m, b + 1) < m$  and  $(m, b - 1) < m$ . But  $(m, b - 1)$  must also be  $> 1$ . For  $m$  divides  $b^2 - 1 = (b - 1)(b + 1)$ . If  $(m, b - 1) = 1$ , then  $m$  must divide  $b + 1$  (by the Coprime Divisibility Lemma). But that contradicts the assumption on  $b$ . Similarly,  $(m, b + 1) > 1$ . So  $(m, b - 1)$  and  $(m, b + 1)$  are proper divisors of  $m$ .  $\square$

In our example of  $m = 561$ , we have  $(561, 66) = 33$  and  $(561, 68) = 17$ . In fact,  $561 = 33 \cdot 17$ .

The main point of this section is that the strong  $a$ -pseudoprime test takes no more computation than the  $a$ -pseudoprime test, and yields a stronger compositeness test.

How much stronger?

**Theorem 9.11** (M. Rabin) *Let  $m$  be a Carmichael number. Then for at least  $3/4$  of all numbers  $a$  with  $1 < a < m$ , the strong  $a$ -pseudoprime test shows that  $m$  is composite.*

Proof of a weak version of this theorem (with  $3/4$  replaced by  $1/2$ ) is in Chapter 14.

Rabin's Theorem yields the following test for primeness.

*Probabilistic Primality Test.* To test an odd number  $m$  for primeness, pick 100 random numbers  $a$  with  $1 < a < m$  and subject  $m$  to the strong  $a$ -pseudoprime test for each  $a$ . If  $m$  is not proven composite by one of those tests, then conclude  $m$  is prime.

The chance of  $m$  being composite but a strong  $a$ -pseudoprime for a single randomly chosen number  $a$  is  $\leq 1/4$ . Then the chance of  $m$  being composite but a strong  $a$  pseudoprime for 100 randomly chosen numbers  $a$  is less than or equal to the probability of picking 100 red balls in 100 trials out of an urn with  $m$  balls, 25% of them red balls and 75% of them black balls. That probability is only slightly larger than  $(1/4)^{100} = 2^{-200}$  (slightly larger because we're drawing without replacement). (Since  $2^{100} \sim 10^{30}$  and the number of seconds in 100 years is slightly more than  $3 \cdot 10^9$ , you could be confident that you would not make a single mistake in your lifetime assuming that a number is prime if the number is not proved composite by Rabin's test.)

*Example 9.12* Returning to Example 9.6, it turns out that thirteen of the fourteen numbers that passed the 2-pseudoprime test are prime. The other one, 2508013, is a Carmichael number. We can see that it is composite if we try a few strong  $a$ -pseudoprime tests.

We first write  $2508013 - 1 = 2508012 = 4 \cdot 627003$ . To perform the strong  $a$ -pseudoprime test, we compute the sequence

$$(a^{627003}, a^{1254006}, a^{2508012}) \pmod{2508013}.$$

For  $a = 7$ , we obtain

$$(2508012, 1, 1),$$

so (since  $2508012 \equiv -1 \pmod{2508013}$ ),  $m$  passes the strong 7-pseudoprime test. For  $a = 13$ , we obtain

$$(1, 1, 1),$$

so  $m$  passes the strong 13-pseudoprime test. But for  $a = 2$ , we obtain

$$(1750878, 1892841, 1).$$

For  $a = 3$ , we obtain

$$(1528649, 1892841, 1).$$

For  $a = 5$ , we obtain

$$(141964, 1892841, 1).$$

For  $a = 11$ , we obtain

$$(222228, 1, 1).$$

So 2508013 is not a strong 2-, or 3-, or 5, or 11-pseudoprime. Just one of these last four computations suffices to prove that 2508013 is composite.

In fact, we can factor 2508013 using that  $1892841^2 \equiv 1 \pmod{2508013}$ . For 2508013 divides  $(1892841 + 1)(1892841 - 1)$  and doesn't divide either factor. So we can compute  $(2508013, 1892842) = 53$  by Euclid's algorithm. Then

$$2508013 = 53 \cdot 79 \cdot 599.$$

As it turned out, we could have found that 2508013 was composite by a bit more trial division. But Rabin's Theorem implies that repeated strong  $a$ -pseudoprime tests can with very high probability prove compositeness of numbers that are much too big for trial division to be useful.

*Remark 9.13* RSA is one of the two public key cryptosystems that are in wide use throughout the world. The other is the Diffie-Hellman cryptosystem. Diffie-Hellman is mathematically more versatile,

because it can be based on any finite cyclic group. So Chapters 10 and 12 contain an introduction to finite abelian groups, to prepare the way for the Diffie-Hellman system in Chapter 13. But we won't ignore RSA. Chapter 11 studies systems of congruences and the Chinese Remainder Theorem, which will yield some useful information related to RSA—in particular, a method to improve the efficiency of decrypting. Section 14.6 has a result on the security of RSA, and Chapter 17 presents a factoring algorithm created to try to factor an RSA modulus.

## Exercises

- 9.1. Encrypt the message OK using the cryptosystem of Example 9.1.
- 9.2. Encrypt the message YES using the cryptosystem of Example 9.2.
- 9.3. Suppose you send Alice the modulus  $m = 143$  and the exponent  $e = 7$ . She wants to send you a letter. She replaces the letter by its number  $w$  in the alphabet ( $A = 1, \dots, Z = 26$ ), encrypts it by finding  $c \equiv w^7 \pmod{143}$  and sends you  $c = 106$ . You know that  $m$  factors as  $m = 11 \cdot 13$ . Find Alice's letter.
- 9.4. In Example 9.1, show that  $(607^{43} \pmod{3131}) = 1415$ , recovering Alice's original message  $w$  from the encrypted word  $c$  Bob received.
- 9.5. In Example 9.1 could Bob have used  $d' = 43$  instead of  $d = 2143$  as a general decrypting exponent on every encrypted message  $w$  with  $m = 3131$  and  $e = 7$ ? Explain.
- 9.6. Let  $p, q$  be distinct odd primes,  $m = pq$  and  $e$  be an encrypting exponent for an RSA cryptosystem. Show that any exponent  $d'$  satisfying

$$\begin{aligned} ed' &\equiv 1 \pmod{p-1} \\ ed' &\equiv 1 \pmod{q-1} \end{aligned}$$

is a suitable decrypting exponent for  $e$ .

- 9.7. If  $m = pq$ , a product of distinct primes, then  $\phi(m) = (p-1)(q-1)$ . So  $m$  and  $\phi(m)$  are known functions of  $p$  and  $q$ .
  - (i) Show that  $p$  and  $q$  can be written as functions of  $m$  and  $\phi(m)$ , as follows: Write

$$(x-p)(x-q) = x^2 - ax + b,$$

then  $b = pq = m$  and  $a = p + q$ . Show that  $a = m + 1 - \phi(m)$ .

- (ii) Having found  $a$  and  $b$  from  $m$  and  $\phi(m)$ , show that the primes  $p$  and  $q$  can be found by the quadratic formula.
  - (iii) Suppose  $m = 684161$ , a product of two prime numbers, and  $\phi(m) = 682500$ . Find the two prime factors of  $m$ .
- 9.8. Suppose Alice, in Phuket, sends signed secret orders to Bob, on Wall Street, using  $(m_A, d_A)$ , then  $(m_B, e_B)$ , to encrypt, where  $d_A$  and  $d_B$  are secret, and  $e_A$  and  $e_B$  are public. Would it be reasonable to use  $m_A = m_B$ ?
- 9.9. In the last exercise, would there be any issues if  $m_A$  is much smaller, or much larger, than  $m_B$ ?
- 9.10. Design an RSA cryptosystem in which the modulus  $m = p_1 p_2 p_3$  is the product of three distinct primes.

- 9.11. Suppose you look for a prime of 462 decimal digits to use as a factor of an RSA modulus. If you choose a random number  $n$  of 462 digits, how many primes would you expect between  $n$  and  $n + 10,000$ ?
- 9.12. Find a number  $a$  with  $2 \leq a \leq 45$  so that 91 is an  $a$ -pseudoprime.
- 9.13. Show that  $2^{560} \equiv 1 \pmod{561}$ .
- 9.14. (i) Suppose  $m$  is a product of distinct prime numbers and  $a$  is coprime to  $m$ . Suppose  $a^{m-1} \equiv 1 \pmod{p}$  for each prime divisor  $p$  of  $m$ . Show that then  $a^{m-1} \equiv 1 \pmod{m}$ , so  $m$  is an  $a$ -pseudoprime.  
(ii) Suppose  $m = p_1 p_2 p_3$ , a product of three primes, and  $p_1 - 1$ ,  $p_2 - 1$  and  $p_3 - 1$  all divide  $m - 1$ . Show that then  $m$  is a Carmichael number.
- 9.15. Suppose  $k$  is a number with the property that  $6k + 1$ ,  $12k + 1$  and  $18k + 1$  are all prime numbers. Show that  $m = (6k + 1)(12k + 1)(18k + 1)$  is a Carmichael number. (Example:  $k = 1$ ,  $m = 1729$ .) (Use Exercise 9.14 (ii).)
- 9.16. (i) Verify that 341 is a 2-pseudoprime. Is 341 a strong 2-pseudoprime?  
(ii) Show that 341 is not a Carmichael number.
- 9.17. Show that 2821 is composite by finding some number  $a$  so that 2821 is not a strong  $a$ -pseudoprime.
- 9.18. In Example 9.12, verify that  $(1892841 - 1, 2508013)$  is a non-trivial divisor of 2508013.

# Chapter 10

## Groups, Cosets and Lagrange's Theorem



In Chapter 8 we introduced the order of an element of a finite group, and, in particular, the order of a unit of  $\mathbb{Z}_m$ . We stated Euler's Theorem, that if  $a$  is a unit modulo  $m$ , then  $a^{\phi(m)} \equiv 1 \pmod{m}$ . As we saw in Chapter 9, Euler's Theorem lies behind RSA cryptography, because it makes decrypting possible for those who know  $\phi(m)$ .

In this chapter, we look at subgroups of a group, in several settings. The main result of the chapter is Lagrange's Theorem, a result in finite group theory that implies that the number of elements in a subgroup  $H$  of a finite group  $G$  divides the number of elements of  $G$ . To obtain this result, we introduce the idea of cosets of  $H$  in  $G$ . The concept of coset here extends the ideas of Chapter 5, where we constructed  $\mathbb{Z}_m$  as cosets of the ideal  $m\mathbb{Z}$ .

Euler's Theorem is a simple consequence of Lagrange's Theorem.

Lagrange's Theorem is a very general counting result. In that form, it shows up often later in the book. Sections 14.1 and 14.2 relate the ideas of this chapter, and, in particular, cosets, to solutions of homogeneous and non-homogeneous linear equations in several settings, and to decoding in Hamming codes. The ideas are used to gain insight into testing large numbers for primeness (for cryptography) (Section 14.5). They are also used to obtain results about the security of the RSA cryptosystem (Section 14.6) and of the Blum–Goldwasser cryptosystem (in Section 16.6).

In this book we need to work only with groups that are abelian, that is, groups in which the operation is commutative. But Lagrange's Theorem and its proof in Section 10.5 are valid for all finite groups, not just finite abelian groups. Non-abelian groups are discussed briefly in Section 10.6.

### 10.1 Groups

Recall from Sections 5.1 and 8.1 that a group  $G$  is a set together with an associative operation

$$*: G \times G \rightarrow G$$

and a unique identity element, and every element of  $G$  has a unique inverse. If the operation on  $G$  is commutative, then the group is called *abelian*.

This book focuses on three classes of examples of abelian groups.

- A ring is an abelian group when viewed with just the operation of addition. Examples:  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{Z}_m$ ,  $F[x]$  for  $F$  a commutative ring.
- The set of units (invertible elements) of a commutative ring is an abelian group under the operation of multiplication. Examples: The subset  $\{1, -1\}$  of  $\mathbb{Z}$ ; the group  $U_m$  of units of  $\mathbb{Z}_m$ ; the set of all non-zero elements of a field.

- A vector space is a group with the operation of addition. Similarly, an ideal of a commutative ring is a group under addition. (Vector space examples will show up in Chapter 14.)

## 10.2 Subgroups

Many groups may be described as subgroups of known groups.

**Definition** Let  $G$  be a group with operation  $*$  and identity element  $e$ , and where the inverse of an element  $a$  is denoted  $a'$ . A *subgroup*  $H$  of  $G$  is a non-empty subset of  $G$  with two properties:

- (i) if  $a, b$  are in  $H$ , then  $a * b$  is in  $H$ ; and
- (ii) if  $a$  is in  $H$ , so is  $a'$ .

In words,  $H$  is a subgroup of  $G$  if  $H$  is a subset of  $G$  that is closed under the operations of  $*$  and taking inverses (in  $G$ ).

Many of the groups we will work with in this book are groups with a finite number of elements, or for short, “finite groups”. If a subset  $S$  of a group  $G$  is a finite set, then checking if  $S$  is a subgroup is easier:

**Proposition 10.1** *Let  $G$  be a group with operation  $*$ . Let  $S$  be a finite non-empty subset of  $G$ . If  $S$  is closed under  $*$ , then  $S$  is a subgroup of  $G$ .*

Notation: for  $a$  in  $G$ , let  $a^r = a * a * \dots * a$  ( $r$  factors).

*Proof* Assume  $S$  is a subset of  $G$  and  $S$  contains  $n$  elements. Suppose  $S$  is closed under  $*$ . We show that  $S$  is also closed under inverses. Let  $a$  be an element of  $S$ . Then  $a, a^2, a^3, \dots, a^n, a^{n+1}$  are  $n+1$  elements of  $S$ . Since  $S$  has  $n$  elements, there must be exponents  $s$  and  $t > s$  so that

$$a^t = a^s.$$

Since  $S$  is a subset of  $G$  and the operation  $*$  is the operation in  $G$ , this last equation holds in  $G$ . Set  $d = t - s$  and cancel  $a^s$  from both sides of the equation to obtain  $a^d = e$ , the identity element of  $G$ . Then  $a * a^{d-1} = a^d = e$ . So  $a^{d-1}$  is the inverse of  $a$  in  $G$ , and is in  $S$ , so is the inverse of  $a$  in  $S$ . Thus  $S$  is closed under inverses.  $\square$

We've seen this argument before, in Chapter 8. We used it there to show that every element  $a$  of a finite group has an order  $d$ , the smallest positive integer so that  $a^d = e$ .

Before giving many examples of subgroups of groups, we should note that most subsets of groups are not subgroups. A quick test: given a subset  $H$  of  $G$ , is the identity element of  $G$  in  $H$ ? If not,  $H$  cannot be a subgroup. For if  $H$  were closed under products and inverses, then starting with any element  $a$  of  $H$ , we can find  $a^{-1}$  in  $H$ , and then  $a * a^{-1} = e$  is in  $H$ .

But containing the identity element of  $G$  is not sufficient to show that  $H$  is a subgroup.

*Example 10.2* Let  $G = \mathbb{Z}$  and let  $H = \mathbb{Z}_{\geq 0}$ , the set of non-negative integers, with operation  $+$ . Then  $H$  is not a subgroup of  $G$ . For while the additive identity element 0 is in  $\mathbb{Z}_{\geq 0}$  and the sum of two non-negative integers is a non-negative integer, the negative of a natural number is not in  $\mathbb{Z}_{\geq 0}$ . Since  $\mathbb{Z}_{\geq 0}$  is not closed under taking negatives,  $\mathbb{Z}_{\geq 0}$  is not a subgroup of  $G$ .

*Example 10.3* Let  $G = (\mathbb{Z}_5, +) = \{0, 1, 2, 3, 4\}$ . Here are some subsets containing the identity element 0 that are not subgroups of  $G$ :

$$\{0, 1\}, \{0, 1, 2\}, \{0, 1, 4\}, \{0, 2, 3\}, \{0, 3\}.$$

In fact, there are sixteen subsets of  $G$  that contain the identity 0, and only two of them are subgroups:  $\{0\}$  and  $G$  itself. (For a generalization of this observation, see Proposition 10.33 below.)

Every group  $G$  has at least two “trivial” subgroups: the entire group  $G$  itself, and the set  $\{e\}$  consisting of only the identity element.

**Subgroups via generators.** To find subgroups of a group, one approach is to specify a set of generators for the subgroup.

**Definition** For elements  $a_1, \dots, a_r$  of a group  $G$ , the *subgroup of  $G$  generated by  $a_1, a_2, \dots, a_r$* , denoted  $\langle a_1, a_2, \dots, a_r \rangle$ , is the set of all products in  $G$  whose factors are elements of the set consisting of the elements  $a_1, a_2, \dots, a_r$  and their inverses.

It is not hard to see that a product of products of elements of a set  $a_1, a_2, \dots, a_r$  and their inverses is also a product of elements of the set  $a_1, \dots, a_r$  and their inverses. Also, the inverse of such a product is such a product. So the set of all such products is a subgroup of  $G$ .

When writing a subgroup as a group generated by elements  $a_1, \dots, a_r$ , we generally seek a minimal set of generators, so that if we omit any listed generator, we get a smaller subgroup. For example,  $U_5 = \{1, 2, 3, 4\} = \langle 2, 3 \rangle$  (because  $2 \cdot 2 = 4$  and  $2 \cdot 3 \equiv 1 \pmod{5}$ ). But 2 and 3 do not form a minimal set of generators for  $U_5$  because  $3 \equiv 2^3 \pmod{5}$ . So we can omit 3 and write  $U_5 = \langle 2 \rangle$ , a description of  $U_5$  using a minimal set of generators.

**Definition** A subgroup of a group  $G$  that is generated by a single element of  $G$  is called a *cyclic* subgroup. A group  $G$  is a cyclic group if  $G$  is generated by a single element.

The group  $\mathbb{Z}$  under addition (which we’ll often denote by  $(\mathbb{Z}, +)$ ) is a cyclic group: in fact,  $\mathbb{Z} = \langle 1 \rangle$ , because every positive integer  $n = 1 + 1 + \dots + 1$  ( $n$  summands), every negative integer  $-m = (-1) + (-1) + \dots + (-1)$  ( $m$  summands), and  $0 = 1 + (-1)$ . Also,  $\mathbb{Z} = \langle -1 \rangle$ .

The group  $\mathbb{Z}_m$  under addition is a cyclic group, generated by 1.

In this chapter we’ll look at subgroups of additive groups of commutative rings, and subgroups of groups of units of commutative rings. Many, but not all, of these groups will be cyclic groups.

**Subgroups of additive groups.** Let’s begin with the additive group of the integers,  $(\mathbb{Z}, +)$  or just  $\mathbb{Z}$ , for short.

*Example 10.4* For an integer  $m$ , the cyclic subgroup  $\langle m \rangle$  generated by  $m$  consists of  $0 = m + (-m)$ , all elements of the form  $sm = m + m + \dots + m$  ( $s$  summands), and all elements of the form  $-(tm) = t(-m) = (-m) + (-m) + \dots + (-m)$  ( $t$  summands). Since  $-(tm) = (-t)m$ , the subgroup generated by  $m$  is the set of all integer multiples of  $m$ .

The subgroup  $\langle m \rangle$  of the additive group  $\mathbb{Z}$  generated by  $m$  is the same as the ideal  $m\mathbb{Z}$  generated by  $m$ . So we’ll usually use the notation  $m\mathbb{Z}$  to refer to this subgroup.

The subgroups  $m\mathbb{Z}$  for  $m \geq 0$  are the only subgroups of  $\mathbb{Z}$ . This follows from the fact that  $\mathbb{Z}$  is cyclic and

**Proposition 10.5** *Every subgroup of a cyclic group is cyclic.*

*Proof* Suppose  $(G, +) = \langle g \rangle$  is a cyclic group, with additive identity 0. The inverse of any element is its negative. Then every non-zero element of  $G$  is of the form

$$g + g + g + \cdots + g \text{ (r summands)} = rg$$

or

$$(-g) + (-g) + \cdots + (-g) \text{ (s summands)} = s(-g).$$

Then  $s(-g) = -(sg)$  since the negative of a sum is the sum of the negatives. If we define  $(-s)g = -(sg)$ , then we may view  $G$  as the set  $\{tg|t \in \mathbb{Z}\}$ .

Now suppose  $H$  is a subgroup of  $G$ . Then  $H$  consists of elements  $rg$  for certain integers  $r$  in  $\mathbb{Z}$ . Let  $J \subset \mathbb{Z}$  be the set

$$J = \{r \in \mathbb{Z} : rg \text{ is in } H\}.$$

Now  $H$  is a subgroup of  $G$ , so  $rg + sg = (r+s)g$  and  $-rg = (-r)g$  are in  $H$  for any  $rg, sg$  in  $H$ . Thus the set  $J$  is an ideal of  $\mathbb{Z}$ .

We proved in Chapter 5 (Theorem 5.13) that every non-zero ideal of  $\mathbb{Z}$  is a principal ideal, generated by the smallest positive integer in the ideal.

Let  $d$  be the smallest positive integer in the ideal  $J$ . Then

$$J = \{rd : r \in \mathbb{Z}\} :$$

$J$  consists of all integer multiples of  $d$ . So the subgroup  $H$  of  $G = \langle g \rangle$  consists of all integer multiples of  $dg$ :

$$H = \{(rd)g : rd \in J\} = \{r(dg) : r \in \mathbb{Z}\}.$$

Thus the subgroup  $H = \langle dg \rangle$  is a cyclic subgroup of  $G$ , where  $d$  is the smallest positive integer so that  $dg$  is in  $H$ .  $\square$

**Corollary 10.6** Every subgroup of  $\mathbb{Z}_m$  is cyclic.

This follows because  $\mathbb{Z}_m$  is cyclic, generated by 1.

*Example 10.7* Let  $G = \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$  with the operation addition modulo 8. Here are some cyclic subgroups of  $G$ :

$$\langle 2 \rangle = \{2, 2+2, 2+2+2, 2+2+2+2\} = \{2, 4, 6, 0\}.$$

$$\langle 4 \rangle = \{4, 0\}.$$

$$\langle 6 \rangle = \{6, 12, 18, 24\} = \{6, 4, 2, 0\} = \langle 2 \rangle.$$

$$\langle 5 \rangle = \{5, 10, 15, 20, 25, 30, 35, 40\} = \{5, 2, 7, 4, 1, 6, 3, 0\} = G.$$

**Subgroups as solutions of equations.** Another useful way to define a subgroup is to define the subgroup to be the set of all solutions of one or more “homogeneous linear equations” in  $G$ .

Here are some examples:

*Example 10.8* The set of solutions (in  $\mathbb{Z}$ ) of

$$4x \equiv 0 \pmod{22}$$

is a subgroup of  $(\mathbb{Z}, +)$  (and hence is cyclic). It is the subgroup  $11\mathbb{Z}$  consisting of all integers that are multiples of 11.

*Example 10.9* The set of solutions in  $\mathbb{Z}_{24}$  of

$$3x = 0$$

is the same as the set of solutions in  $\mathbb{Z}_{24}$  to the congruence

$$3x \equiv 0 \pmod{24},$$

namely the subgroup  $\langle 8 \rangle = \{0, 8, 16\}$  of  $\mathbb{Z}_{24}$ .

*Example 10.10* The set of integers  $x$  that satisfy the two homogeneous equations

$$\begin{aligned} x &\equiv 0 \pmod{22}, \\ x &\equiv 0 \pmod{24} \end{aligned}$$

is a subgroup of  $(\mathbb{Z}, +)$ . It is the subgroup  $264\mathbb{Z}$  consisting of all integers that are multiples of  $264 = [22, 24]$ , the least common multiple of 22 and 24.

On the other hand, the set of solutions of the non-homogeneous equations

$$\begin{aligned} x &\equiv 13 \pmod{22}, \\ x &\equiv 11 \pmod{24} \end{aligned}$$

is not a subgroup of  $\mathbb{Z}$  because the set of solutions is not closed under addition (and also doesn't contain the identity element 0). For example,  $x = 35$  is a solution, but  $35 + 35 = 70$  is not a solution, because

$$\begin{aligned} 70 &\equiv 4 \pmod{22} \\ 70 &\equiv -2 \pmod{24}. \end{aligned}$$

**Subgroups of groups of units via generators.** As with additive groups, we can describe a subgroup of the group  $U_m$  of units modulo  $m$  as a group generated by a set of elements, or as a group of solutions to equations.

In contrast to  $\mathbb{Z}_m$ , it is not true for every number  $m$  that the group  $U_m$  is cyclic: for example,  $U_8 = \{1, 3, 5, 7\}$  is not cyclic because the square of each element = 1.

Since  $U_m$  is a finite group, finding subgroups generated by elements of  $U_m$  is made easier by

**Proposition 10.11** *Let  $G$  be a finite group. Then the subgroup  $\langle a_1, \dots, a_r \rangle$  of  $G$  generated by the elements  $a_1, \dots, a_r$  of  $G$  is the set of products in  $G$  whose factors come from the set  $\{a_1, \dots, a_r\}$ .*

The idea here is that if  $G$  is finite, then we don't need to worry about inverses, because the inverse of any element is some positive power of the element. See Proposition 10.1.

Here are some examples of subgroups of  $U_m$  generated by sets of units.

*Example 10.12* For  $p$  prime, the group of units  $U_p$  is cyclic (as we'll prove in Chapter 13). So all subgroups of  $U_p$  are cyclic, by Proposition 10.5. Here are all the subgroups of  $U_{17}$ :

$$\begin{aligned}
\langle 3 \rangle &= U_{17}; \\
\langle 9 \rangle &= \{9, 9^2, \dots, 9^8\} = \{9, 13, 15, 16, 8, 4, 2, 1\} \\
\langle 13 \rangle &= \{13, 16, 4, 1\} \\
\langle 16 \rangle &= \{16, 1\} \text{ (note: } 16 = -1 \text{ in } \mathbb{Z}_{17}) \\
\langle 1 \rangle &= \{1\}.
\end{aligned}$$

*Example 10.13* We find minimal sets of generators for all of the subgroups of

$$U_{24} = \{1, 5, 7, 11, 13, 17, 19, 23\}.$$

Since all computations are modulo 24, we can replace 13, 17, 19 and 23 by  $-11, -7, -5$  and  $-1$ , respectively, if we prefer.

The group  $U_{24}$  is not cyclic. To see this, we first list the cyclic subgroups of  $U_{24}$ :

One is the trivial group  $\langle 1 \rangle = \{1\}$ , the subgroup of  $U_{24}$  consisting of the identity element 1. The others are:

$$\begin{aligned}
\langle 5 \rangle &= \{5, 1\} \\
\langle 7 \rangle &= \{7, 1\} \\
\langle 11 \rangle &= \{11, 1\} \\
\langle -1 \rangle &= \{-1, 1\} \\
\langle -5 \rangle &= \{-5, 1\} \\
\langle -7 \rangle &= \{-7, 1\} \\
\langle -11 \rangle &= \{-11, 1\}.
\end{aligned}$$

Each of these seven subgroups has two elements, because every element of  $U_{24}$  other than 1 has order 2.

Now we look at non-cyclic subgroups.

The subgroup  $\langle 7, 11 \rangle$  of  $U_{24}$  consists of all elements of  $U_{24}$  that are products involving the numbers 7 and 11. It contains 7, 11,  $7 \cdot 7 = 1$  and  $7 \cdot 11 = 5$ . To see that  $\{1, 5, 7, 11\}$  is closed under multiplication, we write down its multiplication table:

.	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

So

$$\langle 7, 11 \rangle = \{1, 5, 7, 11\}.$$

It turns out that  $U_{24}$  has seven subgroups with four elements, each of which can be described in several ways as the subgroup generated by two elements of  $U_{24}$ :

$$\begin{aligned}
\{1, 5, 7, 11\} &= \langle 5, 7 \rangle = \langle 5, 11 \rangle = \langle 7, 11 \rangle \\
\{1, 5, -5, -1\} &= \langle 5, -5 \rangle = \langle 5, -1 \rangle = \langle -5, -1 \rangle \\
\{1, 7, -7, -1\} &= \langle 7, -7 \rangle = \langle 7, -1 \rangle = \langle -7, -1 \rangle \\
\{1, 11, -11, -1\} &= \langle 11, -11 \rangle = \langle 11, -1 \rangle = \langle -11, -1 \rangle \\
\{1, 5, -7, -11\} &= \langle 5, -7 \rangle = \langle 5, -11 \rangle = \langle -7, -11 \rangle \\
\{1, -5, -7, 11\} &= \langle -5, -7 \rangle = \langle -5, 11 \rangle = \langle -7, 11 \rangle \\
\{1, -5, 7, -11\} &= \langle -5, 7 \rangle = \langle -5, -11 \rangle = \langle 7, -11 \rangle.
\end{aligned}$$

The only other subgroup of  $U_{24}$  is  $U_{24}$  itself. We could view it as the subgroup  $\langle 5, 7, -1 \rangle$  (or in many other ways).

**Subgroups of units defined by equations: “roots of unity” in  $\mathbb{Z}_m$ .** For groups of units modulo  $m$  under multiplication, the congruence analogous to  $ax \equiv 0 \pmod{m}$  is  $x^a \equiv 1 \pmod{m}$ .

**Proposition 10.14** *Let  $U_R$  be the group of units of a commutative ring  $R$ . For a fixed positive integer  $e$ , let  $U_R(e)$  be the subset*

$$U_R(e) = \{a \in U_R : a^e = 1\}.$$

*Then  $U_R(e)$  is a subgroup of  $U_R$ .*

*Proof* We need to show that  $U_R(e)$  is closed under products and inverses.

For products: suppose  $a$  and  $b$  are in  $U_R(e)$ . Then  $a^e = 1$  and  $b^e = 1$ . So

$$(ab)^e = a^e \cdot b^e = 1 \cdot 1 = 1.$$

Hence  $ab$  is in  $U_R(e)$ .

For inverses: suppose  $a$  is in  $U_R(e)$ . If  $b$  is the inverse of  $a$ , then  $ab = 1$ , so  $1 = (ab)^e = a^e b^e$ . But  $a^e = 1$ , so  $b^e = 1$ . So the inverse  $b$  of  $a$  is in  $U_R(e)$ .

Hence  $U_R(e)$  is a subgroup of  $U_R$ .  $\square$

**Definition** The group  $U_R(e)$  is called *the group of  $e$ -th roots of unity of  $R$* .

The traditional use of the term “roots of unity” is with elements of the field  $\mathbb{C}$  of complex numbers. Here are some small examples, where we omit  $\mathbb{C}$  in the notation  $U_{\mathbb{C}}(e)$ .

*Example 10.15*

$$\begin{aligned} U(2) &= \{\alpha \in \mathbb{C} : \alpha^2 = 1\} = \{1, -1\}; \\ U(3) &= \{\alpha \in \mathbb{C} : \alpha^3 = 1\} = \left\{ \frac{-1 + \sqrt{-3}}{2}, \frac{-1 - \sqrt{-3}}{2}, 1 \right\}; \\ U(4) &= \{\alpha \in \mathbb{C} : \alpha^4 = 1\} = \{1, i, -1, -i\}. \end{aligned}$$

In general, the group of  $n$ th roots of unity in  $\mathbb{C}$  is the set

$$U(n) = \{e^{2\pi ik/n} = \cos(2\pi k/n) + i \sin(2\pi k/n) : k = 1, 2, \dots, n\}.$$

Groups of roots of unity are of interest also for groups of units modulo  $m$ . They will be particularly useful for Reed–Solomon codes in Chapter 19.

*Example 10.16* Let  $G = U_m$ , the group of units of  $\mathbb{Z}_m$  under multiplication. For any number  $e$ , let

$$U_m(e) = \{b \in U_m | b^e = 1\}.$$

Then  $U_m(e)$ , the group of  $e$ th roots of unity in  $U_m$ , is a subgroup of  $U_m$ .

By Euler’s Theorem,  $U_m(\phi(m)) = U_m$ : every unit is a  $\phi(m)$ -th root of unity in  $U_m$ .

In particular, for a prime  $p$ , we have  $U_p = U_p(p-1)$  by Fermat’s Theorem.

For  $p$  prime,  $U_p(2) = \{1, -1\}$ .

$U_8(2) = \{1, 3, -3, -1\} = U_8$ .

As we saw in Example 10.13,  $U_{24}(2) = U_{24}$ : every unit modulo 24 has order 1 or 2.

*Example 10.17* Let  $m$  be an odd composite number. Then  $m$  is an  $a$ -pseudoprime if  $a^{m-1} = 1$ , which means that  $a$  is in  $U_m(m - 1)$ .

Recall from Chapter 9 that a Carmichael number  $m$  is an odd composite number which is an  $a$ -pseudoprime for all units  $a$ . Thus  $m$  is Carmichael if  $U_m(m - 1) = U_m$ . For example,  $U_{561}(560) = U_{561}$ . (The number 561 is the smallest Carmichael number.)

### 10.3 Subgroups of Finite Cyclic Subgroups

The main result of this chapter will be that if  $G$  is a finite group and  $H$  is a subgroup of  $G$ , then the number of elements of  $H$  divides the number of elements of  $G$ . In this section we show the main result for subgroups of finite cyclic groups.

**Theorem 10.18** *Let  $G$  be a finite cyclic group with operation  $*$  and identity  $e$ , and denote  $a * a * \dots * a$  ( $r$  factors) as  $a^r$ . Let  $H$  be a subgroup of  $G$ . Then the number of elements of  $H$  divides the number of elements of  $G$ .*

*Example 10.19* Let  $G = U_{13}$ , the group of units of  $\mathbb{Z}_{13}$ . Then  $G$  is a cyclic group with 12 elements, and is generated by 2, because 2 has order 12 modulo 13.

Now  $3 = 2^4$  has order 3, so the cyclic subgroup  $\langle 3 \rangle$  generated by 3 has three elements: 3, 9 and  $27 = 1$ , and 3 divides 12.

Also,  $5 = 2^9$  has order 4 =  $\frac{12}{(12, 9)}$ , so the cyclic subgroup  $\langle 5 \rangle$  generated by 5 has four elements: 5,  $-1$ ,  $-5$  and 1, and 4 divides 12.

To prove Theorem 10.18, we first observe

**Proposition 10.20** *For a finite cyclic group  $G = \langle a \rangle$ , the number of elements of  $G$  is equal to the order of the element  $a$ .*

The argument here uses ideas in Proposition 10.1.

*Proof* Let  $a$  have order  $n$ . Then  $a^n = e$  and  $a^k \neq e$  for  $1 \leq k < n$ . So

$$G = \{a, a^2, \dots, a^n\}$$

We show that  $a, a^2, \dots, a^n$  are all different. For suppose  $a^r = a^{r+k}$  for some  $r \geq 1$  and  $k > 0$ . Canceling  $a^r$  gives  $a^k = e$ . Since  $a$  has order  $n$ ,  $n \leq k$ . So  $r + k > n$ . Thus  $a, a^2, \dots, a^n$  are  $n$  different elements of  $G$ .  $\square$

*Proof of Theorem 10.18* If  $G = \langle a \rangle$  is cyclic where  $a$  has order  $n$ , then every subgroup of  $G$  is also cyclic (Proposition 10.5), so is generated by a power of  $a$ . Let  $H = \langle a^r \rangle$ . If  $a$  has order  $n$ , then  $a^r$  has order  $s = n/(n, r)$ . By Proposition 10.20, the number of elements of  $G$  is the order of  $a$ , namely  $n$ , and the number of elements of  $H$  is equal to the order of the element  $a^r$ , namely  $s = n/(n, r)$ . Since  $s$  divides  $n$ , the proof is done.  $\square$

### 10.4 Cosets

Closely related to the concept of subgroup is the concept of a *coset* of a subgroup.

**Definition** Let  $G$  be a group with operation  $*$ , and  $H$  a subgroup. For  $b$  in  $G$ , the *left coset* of  $b$ , denoted  $b * H$ , is the set of elements  $b * h$ , where  $h$  runs through all elements of  $H$ . In symbols,

$$b * H = \{b * h \mid h \text{ in } H\}.$$

Why is  $b * H$  a “left coset”? Because it consists of elements obtained by multiplying elements of  $H$  by  $b$  on the left. We could also define a right coset  $H * b$ . If the group  $G$  is abelian, then  $b * h = h * b$  for all  $b, h$  in  $G$ , so  $H * b = b * H$ . All of the groups we will work with in this book are abelian, so we will usually omit the word “left” and just talk about cosets. (But see the last section of this chapter.)

Given  $G$  and a subgroup  $H$ , we have a coset  $b * H$  for every element  $b$  of  $G$ . But for  $b$  and  $b'$  in  $G$ , the cosets  $b * H$  and  $b' * H$  might be the same set. We'll need to explore this issue.

*Example 10.21* Let  $G = \mathbb{Z}$  (the operation is  $+$ ),  $H = 2\mathbb{Z}$ . Then the coset  $1 + 2\mathbb{Z}$  is the set of integers of the form  $1 + 2k$  where  $k$  runs through all elements of  $\mathbb{Z}$ . Thus  $1 + 2\mathbb{Z}$  is the set of all integers congruent to 1 (mod 2) (the odd integers). Similarly, the coset  $0 + 2\mathbb{Z}$  is just the set of elements in the subgroup  $2\mathbb{Z}$ , that is, the set of multiples of 2 (the even integers).

Any integer is either even or odd, so is either in  $0 + 2\mathbb{Z}$  or in  $1 + 2\mathbb{Z}$ . So there are two cosets of the subgroup  $2\mathbb{Z}$  in  $\mathbb{Z}$ ; every integer is in one of the two cosets, and the cosets have no elements in common (no integer is both even and odd).

If we look at the coset  $3 + 2\mathbb{Z}$ , we see that that set consists of all the odd integers. So  $3 + 2\mathbb{Z} = 1 + 2\mathbb{Z}$ .

More generally, it's easy to see that if  $k$  is any integer, then  $k + 2\mathbb{Z} = 0 + 2\mathbb{Z}$  if  $k$  is even, and  $k + 2\mathbb{Z} = 1 + 2\mathbb{Z}$  if  $k$  is odd. So we have just two cosets of the subgroup  $2\mathbb{Z}$ , but each coset can be labeled in many ways.

*Example 10.22* More generally, let  $G = \mathbb{Z}$  (a group under  $+$ ) and  $H = m\mathbb{Z}$  for some  $m > 1$ , the modulus. For an integer  $a$ , the coset  $a + m\mathbb{Z}$  of  $a$  is the set of integers of the form  $a + mk$  for  $k$  any integer, that is, the set of integers congruent to  $a$  (mod  $m$ ). Then the coset  $a + m\mathbb{Z}$  is equal to the coset  $b + m\mathbb{Z}$  if and only if  $a$  is congruent to  $b$  (mod  $m$ ). There are  $m$  different cosets, namely,  $0 + m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \dots, (m - 1) + m\mathbb{Z}$ . This is because any integer is congruent (mod  $m$ ) to exactly one of the numbers  $0, 1, 2, \dots, m - 1$ .

These last two examples should be familiar. In Chapter 5 we identified  $\mathbb{Z}_m$  as  $\mathbb{Z}/m\mathbb{Z}$ , the cosets of the ideal  $m\mathbb{Z}$  in  $\mathbb{Z}$ . If we forget that  $\mathbb{Z}$  has multiplication, and think of  $\mathbb{Z}$  just as a group under addition, then the cosets of the subgroup  $m\mathbb{Z}$  in  $\mathbb{Z}$  are identical to the cosets of the ideal  $m\mathbb{Z}$  in the ring  $\mathbb{Z}$ .

*Example 10.23* Let  $G = (\mathbb{Z}_8, +) = \{0, 1, 2, 3, 4, 5, 6, 7\}$ , with operation addition modulo 8. Let  $H = \langle 2 \rangle = \{0, 2, 4, 6\}$ . Then the cosets of  $H$  are

$$\begin{aligned} 0 + H &= \{0 + 0, 0 + 2, 0 + 4, 0 + 6\} = \{0, 2, 4, 6\} = H; \\ 1 + H &= \{1 + 0, 1 + 2, 1 + 4, 1 + 6\} = \{1, 3, 5, 7\}; \\ 2 + H &= \{2 + 0, 2 + 2, 2 + 4, 2 + 6\} = \{2, 4, 6, 0\} = H; \\ 3 + H &= \{3 + 0, 3 + 2, 3 + 4, 3 + 6\} = \{3, 5, 7, 1\} = 1 + H; \\ &\quad \text{etc.} \end{aligned}$$

We have  $H = (0 + H) = (2 + H) = (4 + H) = (6 + H)$ , and  $(1 + H) = (3 + H) = (5 + H) = (7 + H)$ . So there are two cosets of  $H$  in  $G$ , and each may be written in four different ways.

*Example 10.24* Let  $G = U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$  with operation multiplication modulo 15. Let  $H = \langle 4 \rangle = \{4, 1\}$ . Then the cosets are

$$\begin{aligned}
 1 \cdot H &= \{1 \cdot 4, 1 \cdot 1\} = \{4, 1\} = H \\
 2 \cdot H &= \{2 \cdot 4, 2 \cdot 1\} = \{8, 2\} = 8 \cdot H \\
 4 \cdot H &= \{4 \cdot 4, 4 \cdot 1\} = \{1, 4\} = H \\
 7 \cdot H &= \{7 \cdot 4, 7 \cdot 1\} = \{13, 7\} = 13 \cdot H \\
 8 \cdot H &= \{8 \cdot 4, 8 \cdot 1\} = \{8, 2\} = 2 \cdot H \\
 11 \cdot H &= \{11 \cdot 4, 11 \cdot 1\} = \{14, 11\} = 14 \cdot H \\
 13 \cdot H &= \{13 \cdot 4, 13 \cdot 1\} = \{7, 13\} = 7 \cdot H \\
 14 \cdot H &= \{14 \cdot 4, 14 \cdot 1\} = \{11, 14\} = 11 \cdot J
 \end{aligned}$$

So there are four cosets of  $H$  in  $G$ , and each may be written in two different ways.

Each element of the coset yields a different way to write the coset: for example, with  $H = \{1, 4\}$ , the coset  $\{7, 13\} = 7 \cdot H = 13 \cdot H$ .

**Cosets and group tables.** For small finite groups we can visualize cosets by looking at parts of the group table of the group.

*Example 10.25* Let  $G$  be the group  $\mathbb{Z}_8$  with the operation of addition. Here is the group table for  $G$  (= the addition table for  $\mathbb{Z}_8$ ):

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Let us look at the subgroup generated by 2. The table tells us that  $2 + 2 = 4$ ,  $2 + 4 = 6$ ,  $2 + 6 = 0$ ,  $2 + 0 = 2$ . So the subgroup  $\langle 2 \rangle = \{2, 4, 6, 0\}$ . To find the group table for the subgroup, we just omit all the rows and columns not headed by 2, 4, 6 and 0:

+	0	-	2	-	4	-	6	-
0	0	-	2	-	4	-	6	-
-	-	-	-	-	-	-	-	-
2	2	-	4	-	6	-	0	-
-	-	-	-	-	-	-	-	-
4	4	-	6	-	0	-	2	-
-	-	-	-	-	-	-	-	-
6	6	-	0	-	2	-	4	-
-	-	-	-	-	-	-	-	-

Now suppose we want to look at the cosets in  $\mathbb{Z}_8$  of the subgroup  $\langle 2 \rangle$  generated by 2. To do so, we omit just the columns of the group table for  $\mathbb{Z}_8$  headed by elements of the group not in the subgroup:

$+$	0	-	2	-	4	-	6	-
0	0	-	2	-	4	-	6	-
1	1	-	3	-	5	-	7	-
2	2	-	4	-	6	-	0	-
3	3	-	5	-	7	-	1	-
4	4	-	6	-	0	-	2	-
5	5	-	7	-	1	-	3	-
6	6	-	0	-	2	-	4	-
7	7	-	1	-	3	-	5	-

Then the row headed by  $a$  consists of the elements of the form ( $a + \text{element of the subgroup}$ ). Those elements make up the coset  $a + \langle 2 \rangle$ . For example, the row headed by 3 contains the elements

$$3 + 0, 3 + 2, 3 + 4, 3 + 6.$$

So the coset  $3 + \langle 2 \rangle$  of 3 is the set  $\{3, 5, 7, 1\}$ . The row headed by 6 contains the elements

$$6 + 0, 6 + 2, 6 + 4, 6 + 6.$$

So the coset  $6 + \langle 2 \rangle$  of 6 is the set  $\{6, 0, 2, 4\}$ . The row headed by 5 contains the elements

$$5 + 0, 5 + 2, 5 + 4, 5 + 6.$$

So the coset  $5 + \langle 2 \rangle$  of 5 is the set  $\{5, 7, 1, 3\}$ .

Notice that the cosets  $2 + \langle 2 \rangle$ ,  $4 + \langle 2 \rangle$ ,  $6 + \langle 2 \rangle$ , and  $0 + \langle 2 \rangle$  are the same, and the cosets  $1 + \langle 2 \rangle$ ,  $3 + \langle 2 \rangle$ ,  $5 + \langle 2 \rangle$ , and  $7 + \langle 2 \rangle$  are the same. That's because 2, 4, 6 and 0 are all in the subgroup  $\langle 2 \rangle$  generated by 2 (which is the coset of 0), and 1, 3, 5 and 7 are all in the same coset of  $\langle 2 \rangle$ . This illustrates a general fact that we'll prove shortly:

*If two elements  $a$  and  $b$  are in the same coset of a subgroup  $H$  of a group  $G$ , then the coset of  $a$  is equal to the coset of  $b$ .*

In our example, we have a subgroup  $\langle 2 \rangle$  with 4 elements, and there are 2 distinct cosets. Since each element of the group is in exactly one of the two cosets, we see that the number of elements of the subgroup (4), multiplied by the number of cosets (2), is equal to the number of elements of the group (8).

*Example 10.26* Here is the group table for the group  $U_{20}$  of units of  $\mathbb{Z}_{20}$ , a group under multiplication:

$\cdot$	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

If  $H = \langle 9 \rangle = \{1, 9\}$ , then the cosets of  $H$  are

$$\begin{aligned} H &= \{1, 9\} = 9 \cdot H \\ 3 \cdot H &= \{3, 7\} = 7 \cdot H \\ 11 \cdot H &= \{11, 19\} = 19 \cdot H \\ 13 \cdot H &= \{13, 17\} = 17 \cdot H. \end{aligned}$$

We can look at the group table for the subgroup  $\langle 9 \rangle$  generated by 9. It consists of just 9 and  $9 \cdot 9 = 81 = 1$ . So the group table is

.	1	-	-	9	-	-	-	-
1	1	-	-	9	-	-	-	-
-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-
9	9	-	-	1	-	-	-	-
-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-

Now let's look at the cosets of the subgroup generated by 9. We delete all columns of the group table except those headed by elements of the subgroup:

.	1	-	-	9	-	-	-	-
1	1	-	-	9	-	-	-	-
3	3	-	-	7	-	-	-	-
7	7	-	-	3	-	-	-	-
9	9	-	-	1	-	-	-	-
11	11	-	-	19	-	-	-	-
13	13	-	-	17	-	-	-	-
17	17	-	-	13	-	-	-	-
19	19	-	-	11	-	-	-	-

We have a coset for each element of the group. Each coset has two elements in it, one element for each element of the subgroup  $\langle 9 \rangle$ . For example, the coset  $3 \cdot \langle 9 \rangle$  of 3 contains  $3 = 3 \cdot 1$  and  $7 = 3 \cdot 9$ ; the coset  $17 \cdot \langle 9 \rangle$  of 17 contains  $17 = 17 \cdot 1$  and  $13 = 17 \cdot 9$ .

There are four distinct cosets. Every element of the group is in exactly one of those four cosets. So the number of distinct cosets (4), multiplied by the number of elements in any coset (2), is equal to the number of elements of the group (8).

**Properties of cosets.** Based on these examples, the following fact about cosets of a subgroup in a group should be reasonable:

**Proposition 10.27** *Let  $H$  be a subgroup of a group  $G$ , with operation  $*$ . For all  $a, b$  in  $G$ , if  $b$  is in  $a * H$ , then  $b * H = a * H$ . Thus two left cosets of  $H$  in  $G$  are either disjoint or equal.*

*Proof* If  $b$  is in  $a * H$ , then  $b = a * h$  for some  $h$  in  $H$ . Then for all  $h'$  in  $H$ ,  $b * h' = a * (h * h')$  is in  $a * H$ , so  $b * H$  is contained in  $a * H$ . Conversely, if  $b = a * h$ , then  $a = b * k$  for  $k = h^{-1}$  in  $H$ , so  $a$  is in  $b * H$ , and then the same argument shows that  $a * H$  is contained in  $b * H$ . So  $a * H = b * H$ .

Finally, if  $c$  is some element in both  $a * H$  and  $b * H$ , then we just showed that  $c * H = a * H$  and  $c * H = b * H$ . So  $a * H = b * H$ .  $\square$

**Definition** Given the coset  $a * H$ , we call  $a$  a *representative* of the coset  $a * H$ . The proof of Proposition 10.27 shows that every element of a coset may be chosen as a representative of the coset: an element  $b$  is in a coset  $a * H$  if and only if  $b * H = a * H$ .

Since every element  $a$  of  $G$  is in the coset  $a * H$ , we have

**Proposition 10.28** *Let  $H$  be a subgroup of a group  $G$ . Then every element  $a$  of  $G$  is in exactly one coset of  $H$  in  $G$ .*

*Proof* The element  $a$  is in the coset  $a * H$ . If  $a$  were in another coset  $b * H$ , then  $a * H$  and  $b * H$  would both contain  $a$ . But then the cosets  $a * H$  and  $b * H$  would be equal.  $\square$

These two results say that given a subgroup  $H$  of  $G$ , the set of cosets of  $H$  in  $G$  form a partition of  $G$  into a union of pairwise non-intersecting subsets. We saw that in the examples above.

For the group  $G = \mathbb{Z}_8$ , with subgroup  $H = \{2, 4, 6, 0\}$ , we found that

$$G = H \cup (1 + H),$$

that is,

$$\{0, 1, 2, 3, 4, 5, 6, 7\} = \{2, 4, 6, 0\} \cup \{1, 3, 5, 7\}.$$

For the group  $G = U_{20}$  with subgroup  $H = \langle 11 \rangle = \{11, 1\}$ , we found that

$$G = H \cup (3 \cdot H) \cup (7 \cdot H) \cup (9 \cdot H),$$

that is,

$$\{1, 3, 7, 9, 11, 13, 17, 19\} = \{1, 11\} \cup \{3, 13\} \cup \{7, 17\} \cup \{9, 19\}.$$

## 10.5 Lagrange's Theorem

The main result of this chapter is the following famous theorem:

**Theorem 10.29** (Lagrange's Theorem) *Let  $G$  be a finite group,  $H$  a subgroup of  $G$ . Then the number of elements of  $H$ , multiplied by the number of cosets of  $H$  in  $G$ , is equal to the number of elements of  $G$ .*

Lagrange's Theorem implies immediately that if  $G$  is a finite group and  $H$  a subgroup of  $G$ , then the number of elements of  $H$  divides the number of elements of  $G$ .

To prove Lagrange's Theorem we need one preliminary fact.

**Proposition 10.30** *Let  $G$  be a group and  $H$  a subgroup of  $G$ . The number of elements in a left coset  $a * H$  is equal to the number of elements in  $H$ .*

*Proof* Define a function  $f$  from  $H$  to  $a * H$  by  $f(h) = a * h$ . Then  $f$  obviously maps onto  $a * H = \{a * h : h \in H\}$ . It is almost as obvious that  $f$  is a one-to-one function. For if  $f(h) = f(h')$ , then  $a * h = a * h'$ . By cancellation,  $h = h'$ . So  $f$  defines a one-to-one correspondence between  $H$  and  $a * H$ . Hence  $H$  and  $a * H$  have the same number of elements.  $\square$

Now for the proof of Lagrange's Theorem.

*Proof* Let  $G$  have  $n$  elements, and  $H$  have  $r$  elements. We want to write  $G$  as a disjoint union of left cosets:

$$G = (a_1 * H) \cup (a_2 * H) \cup \dots \cup (a_s * H).$$

We can do this as follows: every  $b$  in  $G$  is in the left coset  $b * H$ . So we let  $b_1, b_2, \dots, b_n$  be the elements of  $G$ . Then

$$G = (b_1 * H) \cup (b_2 * H) \cup \dots \cup (b_n * H).$$

Unless  $H$  contains only one element, this is not a disjoint union—there will be cosets in this union that are equal. We want to toss out duplicates. So starting with  $k = 1$ , look at each coset  $b_{k+1} * H$  to see if it has an element in common with one of the earlier cosets  $b_1 * H, \dots, b_k * H$ . If so, then  $b_{k+1} * H$  is equal to the coset it has an element in common with. So toss  $b_{k+1} * H$  out. Once we toss out all the duplicates, we're left with  $G$  as the disjoint union of the remaining cosets. Call the non-duplicative cosets  $a_1 * H, a_2 * H, \dots, a_s * H$ . Then  $G$  is the disjoint union of those non-duplicative cosets:

$$G = (a_1 * H) \cup (a_2 * H) \cup \dots \cup (a_s * H).$$

Now we count the elements of  $G$ .

We see that  $n$ , the number of elements of  $G$ , is equal to the number of elements in the coset  $a_1 * H$  plus the number of elements of  $a_2 * H$  plus  $\dots$  plus the number of elements of  $a_s * H$ .

But Proposition 10.30 tells us that each coset in the disjoint union has  $r$  elements, where  $r$  is the number of elements in  $H$ . Thus if  $G$  has  $n$  elements and  $s$  cosets, then  $n = rs$ . To state this formula in words, the number of elements in  $G$  is equal to the number of elements in  $H$  times the number of left cosets of  $H$  in  $G$ .

This completes the proof of Lagrange's theorem. □

We can obtain Euler's Theorem from Lagrange's Theorem easily.

**Corollary 10.31** *For every element  $b$  of a finite group  $G$ , the order of  $b$  divides the number of elements of  $G$ .*

*Proof* Let  $H = \langle b \rangle$  be the subgroup of  $G$  generated by  $b$ . Then the order of  $b$  is the number of elements of  $H$  by Proposition 10.20. The corollary then follows immediately from Lagrange's theorem. □

**Corollary 10.32** *Euler's theorem.*

*Proof* Let  $G = U_m$ , the group (under multiplication) of units of  $\mathbb{Z}_m$ , and let  $a$  be a number coprime to  $m$ . Then the order  $d$  of  $a$  is equal to the number of elements of the subgroup  $\langle a \rangle$  of  $U_m$ . Hence the order  $d$  divides the number of elements of  $U_m$ , namely  $\phi(m)$ , so  $\phi(m) = ds$  for some number  $s$ . But then, since  $a$  has order  $d$  and  $\phi(m) = ds$ , we have  $a^{\phi(m)} \equiv 1 \pmod{m}$ . □

The number of elements in a finite group  $G$ , or the cardinality of  $G$ , is called the *order* of  $G$ . The number of cosets of  $H$  in  $G$  is called the *index* of  $H$  in  $G$ . Thus Lagrange's Theorem states that

$$(\text{the order of } H) \times (\text{the index of } H \text{ in } G) = (\text{the order of } G).$$

A note on this terminology: The use of “order of a group” as the number of elements of the group is different from the notion of the “order of an element  $a$ ” as the smallest positive exponent  $d$  so that  $a^d$  is the identity element.

But the two notions of order are compatible. For if  $a$  is an element of  $G$ , then the order of  $a$  = the order of the subgroup  $\langle a \rangle$  generated by  $a$ , by Proposition 10.20. So the statement, “the order of an element divides the order of the group”, which uses both versions of the word “order”, is correct.

For a final observation on subgroups, we show:

**Proposition 10.33** *If  $G$  is a group with operation  $*$  and identity  $e$ , then  $G$  has no non-trivial subgroups if and only if the order of  $G$  is a prime number  $p$ .*

*Proof* If  $G$  has order  $p$ , prime, then every subgroup  $H$  of  $G$  has order 1 or  $p$  by Lagrange's Theorem. If  $H$  has order  $p$ , then  $H = G$ ; if  $H$  has order 1, then  $H = \langle e \rangle$ , so  $G$  has no non-trivial subgroups.

If  $G$  has order  $n$ , composite, let  $a \neq e$  be an element of  $G$  and look at the cyclic subgroup  $\langle a \rangle$ . If  $a$  has order  $r$  with  $1 < r < n$ , then  $\langle a \rangle$  is a non-trivial subgroup of  $G$ . If  $a$  has order  $n$  and  $n$  factors as  $n = rs$  with  $1 < r, s < n$ , then  $\langle a^r \rangle$  is a subgroup of  $G$  of order  $s$ , so  $G$  contains a non-trivial subgroup.  $\square$

## 10.6 Non-abelian Groups

A group  $(G, *)$  is abelian if  $a * b = b * a$  for all  $a, b$  in  $G$ , and non-abelian otherwise. For large composite numbers  $n$ , the number of non-abelian groups of order  $n$  (up to isomorphism) greatly exceeds the number of abelian groups of order  $n$ . For example, there are 5 abelian and 9 non-abelian groups of order 16, 5 abelian and 47 non-abelian groups of order 48, and 11 abelian and 256 non-abelian groups of order 64 [<http://oeis.org/wiki/Number> of groups of order  $n$ ].

The smallest example of a non-abelian group is a group of order 6, which is perhaps most easily described as the group of  $2 \times 2$  invertible matrices with entries in  $\mathbb{F}_2 = \{0, 1\}$  with operation matrix multiplication. An  $n \times n$  matrix  $\mathbf{A}$  is invertible if there is an  $n \times n$  matrix  $\mathbf{B}$  so that  $\mathbf{AB} = \mathbf{I}$ , the  $n \times n$  identity matrix.

The  $2 \times 2$  invertible matrices with entries in  $\mathbb{F}_2$  are

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

To see that multiplication is non-commutative, consider

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \end{aligned}$$

For every field  $F$  and every  $n > 1$ , the set of invertible  $n \times n$  matrices with entries in  $F$  is a non-abelian group, called the general linear group and denoted by  $GL_n(F)$ . For every group  $G$  of order  $n$ , then there is a subgroup of  $GL_n(F)$  that looks like (is isomorphic to)  $G$ . So for large  $n$ ,  $GL_n(F)$  has enormous numbers of subgroups, nearly all of them non-abelian.

Non-abelian groups do not arise in the applications presented in this book, so we refer to standard textbooks on abstract algebra or group theory for more about non-abelian groups, except for two points.

First, if we specify that “coset” in this chapter means “left coset”, then nothing we did in proving Lagrange's Theorem depended on the group being abelian. We stated Lagrange's Theorem for  $G$  any finite group and  $H$  any subgroup, and the proof holds in that level of generality. In fact, there is a “left coset” version of Lagrange's Theorem and a “right coset” version. But since the order of the subgroup  $H$  is independent of leftness or rightness of cosets, one can conclude that the index of  $H$  in  $G$  is the same, whether we count left cosets or right cosets.

Second, given a group  $G$  and a subgroup  $H$ , we can ask if for every  $a$  in  $G$ , the left coset  $a * H$  is equal to the right coset  $H * a$ . If  $a * H = H * a$  for all  $a$  in  $G$ , then the subgroup  $H$  is called a *normal* subgroup of  $G$ .

If  $H$  is a normal subgroup of  $G$ , then the left cosets of  $H$  in  $G$  form a group, denoted  $G/H$  (“ $G$  mod  $H$ ”) where the operation is by  $(a * H) * (b * H) = (a * b) * H$ . Verifying that the operation, defined using representatives of cosets, is in fact independent of the choice of representatives, is essentially the same argument used in Section 5.5.

If  $G$  is abelian, then every subgroup of  $G$  is a normal subgroup. But most non-abelian groups have subgroups that are not normal. For a single example, the subgroup

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

of  $GL_2(\mathbb{F}_2)$  is not a normal subgroup of  $GL_2(\mathbb{F}_2)$ , as the interested reader can show.

See Chapter 14, Remark 14.8 for further discussion on normal subgroups.

## Exercises

- 10.1. Let  $N$  be the set of natural numbers (positive integers), and define an operation  $*$  on  $\mathbb{N}$  by  $a * b = [a, b]$ , the least common multiple of  $a$  and  $b$ . In Exercise 5.4 we observed that the operation  $*$  is associative and commutative, and the identity element is the number 1.
  - (i) Which elements of  $N$  have inverses?
  - (ii) For which  $a$  and  $b$  is there a solution of  $a * x = b$ ?
  - (iii) Does cancellation hold in  $\mathbb{N}$  under the operation  $*$ ?
- 10.2. Show that  $\{a : 15a \equiv 18 \pmod{24}\}$  is not a subgroup of the group  $\mathbb{Z}_{24}$  (with operation  $+$ ).
- 10.3. Let  $G = (\mathbb{Z}_p, +)$  where  $p$  is prime.
  - (i) Show that the only non-zero subgroup of  $G$  is all of  $G$ . (Hint: let  $a$  be a non-zero element of  $G$ . What is the order of  $\langle a \rangle$ .)
  - (ii) Show that  $G$  has  $2^{p-1}$  subsets that contain the identity element 0 of  $G$ . (Only two of these subsets of  $G$  that contain 0 are subgroups of  $G$ .)
- 10.4. Example 10.7 described the cyclic subgroups  $\langle a \rangle$  of  $\mathbb{Z}_8$  for  $a = 2, 4, 5$  and 6. Find the cyclic subgroups  $\langle a \rangle$  for  $a = 1, 3, 7$  and 0.
- 10.5. Show that a subset  $S$  of a group  $(G, \cdot)$  is a subgroup of  $G$  if and only if for all  $a$  and  $b$  in  $S$ ,  $a \cdot b^{-1}$  is in  $S$ .
- 10.6. Let  $G = U_{19}$ , the group of units mod 19 (with operation multiplication mod 19).
  - (i) Find the cyclic subgroup of  $G$  generated by 7.
  - (ii) Find the cyclic subgroup of  $G$  generated by 8.
- 10.7. Let  $G = \mathbb{Z}_m$  (the operation is addition) and let  $b$  be some number with  $1 \leq b < m$ . Show that the cyclic subgroup  $H$  generated by  $b$  is all of  $G$  if and only if there is a solution to the congruence  $bx \equiv 1 \pmod{m}$ , if and only if  $(b, m) = 1$ .
- 10.8. (i) Show that the number of subgroups of  $(\mathbb{Z}_m, +)$  is equal to the number of positive divisors of  $m$ .
  - (ii) If  $m = p_1^{e_1} p_2^{e_2} \cdots p_g^{e_g}$ , find a formula for the number of subgroups of  $(\mathbb{Z}_m, +)$  involving the exponents  $e_1, \dots, e_g$ .
- 10.9. Show that the subgroup of  $(\mathbb{Z}, +)$  consisting of all solutions  $x$  in  $\mathbb{Z}$  of  $ax \equiv 0 \pmod{m}$  is the cyclic subgroup  $r\mathbb{Z}$  where  $r = m/(a, m)$ . (See Section 3.7.)

- 10.10. Find a generator of the cyclic subgroup of  $(\mathbb{Z}_{66}, +)$  consisting of the solutions to  $30x \equiv 0 \pmod{66}$ .
- 10.11. Describe all of the subgroups of  $(U_{21}, \cdot)$  by finding a minimal set of generators for each subgroup.
- 10.12.  $U_m(2)$  is the set of  $a$  in  $U_m$  with  $a^2 \equiv 1 \pmod{m}$ .
- For  $m > 2$ , find two elements of  $U_m(2)$ .
  - Show that if  $U_m(2)$  has more than two elements, then  $m$  is a composite number.
- 10.13. Find the four elements of  $U_{28}(2)$ .
- 10.14. Let  $m = 41 \cdot 43 = 1763$ . Show that  $1, 42, -1$  and  $-42$  are four elements of  $U_{1763}(2)$ .
- 10.15. Generalize the last exercise: if  $p$  and  $q = p + 2$  are twin primes (that is, both are primes), find four elements of  $U_{pq}(2)$ .
- 10.16. Which of  $1, 2, 3, 4, 5, 6$  are in  $U_{91}(90)$ ? (Hint: use Lemma 16 in Chapter 8.)
- 10.17. (i) Why is it that the subgroup  $\langle m \rangle$  of the group  $(\mathbb{Z}, +)$  is equal to the ideal  $m\mathbb{Z}$  of the commutative ring  $\mathbb{Z}$ ?
- (ii) In the commutative ring  $\mathbb{R}[x]$  of polynomials with real coefficients, is the ideal  $x\mathbb{R}[x]$  equal to the subgroup  $\langle x \rangle$  of the additive group  $(\mathbb{R}[x], +)$ ? (Hint: look at  $\sqrt{3}x$ , or  $x^2$ .)
- 10.18. Let  $G = U_{27}$ .
- List the elements of the cyclic subgroup of  $G$  generated by 4.
  - List the elements of the cyclic subgroup of  $G$  generated by 10.
- 10.19. In Example 10.19, describe the elements of the cyclic subgroup  $\langle 2^r \rangle$  of  $U_{13}$  for  $r = 1, 2, 3, 4, 6$  and 12, and verify Theorem 10.18 in every case.
- 10.20. Let  $G$  be the group  $(\mathbb{Z}_6, +)$ .
- Write down the group table for  $G$ .
  - Write down all the cosets of the subgroup  $\langle 2 \rangle$  of  $G$ . Then write  $G$  as a disjoint union of some of those cosets.
  - Write down all the cosets of the subgroup  $\langle 3 \rangle$  of  $G$ . Then write  $G$  as a disjoint union of some of those cosets.
- 10.21. Let  $G$  be the group  $(U_{20}, \cdot)$ . The group table is in Example 10.26. Display the cosets of the subgroup  $\langle 3 \rangle$  of  $G$  as part of the group table. Then cross out duplicate cosets as in the beginning of the proof of Lagrange's theorem, to show  $G$  as a disjoint union of the remaining cosets.
- 10.22. Let  $G = (U_{24}, \cdot)$ , the group of units of  $\mathbb{Z}_{24}$ . Write down all the distinct cosets of  $\langle 13 \rangle$  in  $G$ .
- 10.23. Let  $G = (U_{24}, \cdot)$ , the group of units of  $\mathbb{Z}_{24}$ . Let  $H = \langle 7, 13 \rangle = \{1, 7, 13, 19\}$ . Write down the portion of the group table for  $G$  involving the columns headed by 1, 7, 13 and 19. Then write down all the distinct cosets of  $\langle 7, 13 \rangle$  in  $G$ .
- 10.24. Let  $G = U_{12}$ . Does it make sense to write down the cosets of the subgroup of  $G$  generated by 3?
- 10.25. Explain why Fermat's Theorem is a consequence of Lagrange's Theorem.
- 10.26. Why does the order of  $U_{91}(90)$  divide  $\phi(91)$ ? Can you explain why just using Euler's Theorem?
- 10.27. (i) Verify that 3 is a primitive root modulo 17
- Find some  $r$  so that the element  $3^r$  of  $U_{17}$  is a generator of  $U_{17}(12)$
  - Notice that  $2^{12} \equiv -1 \pmod{17}$ . Write all solutions to the congruence

$$x^{12} \equiv -1 \pmod{17}$$

as a coset of  $U_{17}(12)$ .

# Chapter 11

## Solving Systems of Congruences



In Section 3.7 we showed how to solve a single linear congruence. In this chapter we solve systems of two or more linear congruences. For systems where the moduli are pairwise coprime, the main theorem is that solutions always exist. The theorem is known as the Chinese Remainder Theorem (CRT), because special cases of the theorem were known to the ancient Chinese.

In modern mathematics the Chinese Remainder Theorem is a useful tool in a variety of settings. For one example, use of the CRT can help shorten the computational effort of finding high powers modulo composite moduli. This has immediate application to improving the efficiency of decrypting in an RSA cryptosystem, as we'll see in Section 11.3.

*Example 11.1* Suppose we want to find  $123^{211} \pmod{247}$ . We can do it by the usual XS binary algorithm from Chapter 8, writing the exponent 211 in base 2. But the numbers are fairly large, and not something one would want to do by hand. But if we observe that  $247 = 13 \cdot 19$ , then we can proceed in three steps:

- Find  $a = (123^{211} \pmod{13})$ .
- Find  $b = (123^{211} \pmod{19})$ .
- Find a number  $c < 247$  so that

$$c \equiv a \pmod{13}$$

$$c \equiv b \pmod{19}.$$

Then

$$c \equiv 123^{211} \pmod{13},$$

$$c \equiv 123^{211} \pmod{19},$$

and  $(13, 19) = 1$ , so (by Lemma 8.32)

$$c \equiv 123^{211} \pmod{247}.$$

To do the first two steps is relatively easy: we have already seen how to proceed in Section 8.5.

For the first step, observe that  $123 \equiv 6 \pmod{13}$  and the exponent  $211 = 12 \cdot 17 + 7 \equiv 7 \pmod{12}$ , so by Fermat's Theorem,

$$123^{211} \equiv 6^{211} \equiv 6^7 \pmod{13}.$$

Then it is easy to see that  $6^7 \equiv 7 \pmod{13}$ .

For the second step, observe that  $123 \equiv 9 \pmod{19}$  and the exponent  $211 \equiv 13 \pmod{18}$ , so, again using Fermat's Theorem,

$$123^{211} \equiv 9^{211} \equiv 9^{13} \equiv 3^{26} \equiv 3^8 \equiv 6 \pmod{19}$$

(using that  $3^{18} = 1 \pmod{19}$  to reduce  $3^{26}$  to  $3^8$ ).

The third step becomes: find a number  $c < 247 = 13 \cdot 19$  so that

$$\begin{aligned} c &\equiv 7 \pmod{13} \\ c &\equiv 6 \pmod{19}. \end{aligned}$$

Finding solutions of systems of congruences such as this, is what this chapter is about.

One could try to find the smallest solution of

$$\begin{aligned} c &\equiv 7 \pmod{13} \\ c &\equiv 6 \pmod{19}, \end{aligned}$$

by the crude approach of just writing down the list of numbers that are  $7 + (\text{multiple of } 13)$  and less than  $13 \cdot 19 = 247$ :

$$7, 20, 33, 46, 59, 72, 85, 98, 111, 124, 137, 150, 163, 176, 189, 202, 215, 228, 241,$$

and also the list of numbers that are  $6 + (\text{multiple of } 19)$  and less than 247:

$$6, 25, 44, 63, 82, 101, 120, 139, 158, 177, 196, 215, 234,$$

and observing that 215 is in both lists. Then 215 satisfies both congruences, so

$$123^{211} \equiv 215 \pmod{247}.$$

This approach is analogous to looking for the greatest common divisor of two numbers by listing all the divisors of each number and comparing the two lists. We found that Euclid's algorithm was a much faster method for finding greatest common divisors. As it turns out, Bezout's Identity (obtained by Euclid's algorithm) will give us a much faster method for solving pairs of congruences.

## 11.1 Two Congruences: The “Linear Combination” Method

This section gives a general method for solving a system of two congruences when the moduli are pairwise coprime, using Bezout's Identity. The theorem is the Chinese Remainder Theorem for two congruences.

**Theorem 11.2** *Let  $m$  and  $n$  be coprime numbers. Then for all integers  $a$  and  $b$ , there is a solution of*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

If  $x_0$  is a solution of the congruences, then the set of all solutions of the congruences is the set of solutions of

$$x \equiv x_0 \pmod{mn}.$$

We note that the condition that  $m$  and  $n$  are coprime is needed to be certain that the pair of congruences has a solution. For example, 6 and 4 are not coprime, and the pair of congruences

$$\begin{aligned} x &\equiv 1 \pmod{6} \\ x &\equiv 2 \pmod{4}. \end{aligned}$$

has no solution. See Section 11.5 below for the full story on systems of two congruences.

For coprime moduli, the idea of the solution method is to solve two special systems and then obtain a solution of the original congruence as a linear combination of the solutions of the special systems. To solve the special systems, it suffices to determine Bezout’s Identity for  $m$  and  $n$ .

**Proposition 11.3** *Let  $m$  and  $n$  be coprime numbers and let*

$$ms + nt = 1$$

*be a solution of Bezout’s Identity for  $m$  and  $n$ . Then  $e_1 = nt$  is a solution of*

$$\begin{aligned} e_1 &\equiv 1 \pmod{m} \\ e_1 &\equiv 0 \pmod{n}, \end{aligned}$$

*and  $e_2 = ms$  is a solution of*

$$\begin{aligned} e_2 &\equiv 0 \pmod{m} \\ e_2 &\equiv 1 \pmod{n}. \end{aligned}$$

Notice that Bezout’s identity,  $ms + nt = 1$  becomes

$$e_2 + e_1 = 1,$$

where  $e_2$  is a multiple of  $m$ , and  $e_1$  a multiple of  $n$ . Also,  $e_2 = 1 - e_1$ , so once we find  $e_1$ , we get  $e_2$  immediately.  $\square$

*Proof* Clearly  $nt \equiv 0 \pmod{n}$ . Also

$$1 = ms + nt \equiv nt \pmod{m}.$$

So  $e_1 = nt$  satisfies the first pair of congruences. The same observations show that  $e_2 = ms$  satisfies the second pair.  $\square$

*Proof of Theorem 11.2* Let  $e_1, e_2$  be as in Proposition 11.3. Let  $x = ae_1 + be_2$ . Then by direct substitution,

$$\begin{aligned} x &= ae_1 + be_2 = ant + bms \equiv a \cdot 1 + b \cdot 0 \equiv a \pmod{m} \\ x &= ae_1 + be_2 = ant + bms \equiv a \cdot 0 + b \cdot 1 \equiv b \pmod{n}. \end{aligned}$$

In words, given the numbers  $e_1$  and  $e_2$  of the proposition, we obtain a solution to the pair of congruences of Theorem 11.2 as a linear combination of  $e_1$  and  $e_2$  where the coefficients of  $e_1$  and  $e_2$  are the numbers on the right sides of the pair of congruences.

For uniqueness of the solution, suppose  $x_0$  and  $x_1$  are two solutions to the pair of congruences. Then

$$\begin{aligned}x_1 - x_0 &\equiv a - a = 0 \pmod{m} \\x_1 - x_0 &\equiv b - b = 0 \pmod{n}.\end{aligned}$$

So  $x_1 - x_0 = z$  is a divisible by both  $m$  and  $n$ , so is a common multiple of  $m$  and  $n$ . Any common multiple of  $m$  and  $n$  is divisible by the least common multiple  $[m, n]$  of  $m$  and  $n$ . Since  $m$  and  $n$  are coprime, the least common multiple of  $m$  and  $n$  is the product  $mn$ . So  $x_1 - x_0 = z$  is divisible by  $mn$ . Conversely, if  $x_0$  is a solution to the pair of congruences, and  $z$  is any multiple of  $mn$ , then  $x_0 + z$  is also a solution to the pair of congruences. So the set of solutions to the pair of congruences is the set of solutions to the single congruence

$$x \equiv x_0 \pmod{mn}. \quad \square$$

*Example 11.4* Suppose we want to solve

$$\begin{aligned}c &\equiv 7 \pmod{13} \\c &\equiv 4 \pmod{17}.\end{aligned}$$

We find Bezout's identity for 13 and 17. Euclid's Algorithm is

$$\begin{aligned}17 &= 13 \cdot 1 + 4 \\13 &= 4 \cdot 3 + 1.\end{aligned}$$

So using the EEA method:

$$\begin{aligned}17 &\longleftrightarrow (17, 1, 0) \\13 &\longleftrightarrow (13, 0, 1) \\4 &\longleftrightarrow (17, 1, 0) - (13, 0, 1) = (4, 1, -1) \\1 &\longleftrightarrow (13, 0, 1) - 3(4, 1, -1) = (1, -3, 4).\end{aligned}$$

That is,

$$1 = 4 \cdot 13 + (-3) \cdot 17 = e_2 + e_1.$$

Thus

$$\begin{aligned}e_1 &\equiv (-3) \cdot 17 = -51 \\e_2 &\equiv 4 \cdot 13 = 52,\end{aligned}$$

and a solution to the pair of congruences is

$$x = 7e_1 + 4e_2 = 7 \cdot (-51) + 4 \cdot (52) = -357 + 208 = -149.$$

Since  $13 \cdot 17 = 221$ , the set of all solutions of the two congruences is the set of numbers satisfying

$$x \equiv -149 \pmod{221}.$$

The smallest positive solution is  $-149 + 221 = 72$  (which we check:  $72 = 13 \cdot 5 + 7 = 17 \cdot 4 + 4$ ).

The hardest part of this solution method is remembering how to use  $e_1$  and  $e_2$ . But if you notice that  $e_1$  is a multiple of 17, then any multiple of  $e_1$  must be congruent to zero modulo 17, and  $e_1$  has been

chosen to congruent to 1 modulo 13. Similarly,  $e_2$  is a multiple of 13, so any multiple of  $e_2$  must be congruent to zero modulo 13, and  $e_2$  has been chosen to be congruent to 1 modulo 17. So  $ae_1 + be_2$  must be congruent to  $a$  modulo 13 because  $e_1$  is congruent to 1 modulo 13 and  $be_2$  is a multiple of 13. Similarly modulo 17.

*Example 11.5* Consider the pair of congruences

$$\begin{aligned}x &\equiv 15 \pmod{20} \\x &\equiv 3 \pmod{17}.\end{aligned}$$

We know there is a solution, since 20 and 17 are coprime. Bezout’s identity is

$$1 = 120 - 119 = 20 \cdot 6 + 17 \cdot (-7).$$

Then  $e_1 = -119$ ,  $e_2 = 120$ . Thus a solution to the pair of congruences is

$$x = 15 \cdot (-119) + 3 \cdot 120 = -1785 + 360 = -1425.$$

The general solution is the set of  $x$  satisfying

$$x \equiv -1425 \pmod{340}.$$

The smallest positive solution is

$$x = -1425 + 5 \cdot 340 = 275 (= 20 \cdot 13 + 15 = 17 \cdot 16 + 3).$$

Suppose we wish to find several systems of congruences to the same moduli. A useful property of the solution method using Bezout’s Identity is that once we have found  $e_1$  and  $e_2$ , we can find solutions to all of the systems by simply writing down  $ae_1 + be_2$  where  $(a, b)$  runs through the right sides of the congruences.

*Example 11.6* Continuing the last example, suppose now we wish to solve

$$\begin{aligned}x &\equiv 8 \pmod{20} \\x &\equiv 11 \pmod{17}.\end{aligned}$$

We’ve done all the work: knowing  $e_1$  and  $e_2$  for these moduli from the previous example, we simply set

$$x_0 = 8e_1 + 11e_2 = 8 \cdot (-119) + 11 \cdot 120 = 368.$$

The general solution is then

$$x \equiv 368 \pmod{340}$$

and the smallest positive solution is  $x = 28$ .

To solve

$$\begin{aligned}x &\equiv 9 \pmod{20} \\x &\equiv 13 \pmod{17},\end{aligned}$$

we obtain  $x_0 = 9e_1 + 13e_2 = 9 \cdot (-119) + 13 \cdot 120 = -1071 + 1560 = 489$ ; the smallest positive solution is then  $x = 489 - 340 = 149$ .

## 11.2 More Than Two Congruences

Suppose we have a system of  $n$  congruences in which the moduli are pairwise coprime. Built into the statement of the Chinese Remainder Theorem for two congruences is the method for solving  $n > 2$  congruences: we solve the first two congruences by replacing the two congruences by a single congruence. Then our system of  $n$  congruences becomes a system of  $n - 1$  congruences. Repeating  $n - 2$  times gives us a single congruence, whose set of solutions is the set of solutions to the system of  $n$  congruences.

More formally:

**Theorem 11.7** (Chinese Remainder Theorem) *Let  $m_1, m_2, \dots, m_n$  be pairwise coprime natural numbers  $> 1$  (the moduli), and let  $a_1, a_2, \dots, a_n$  be any integers. Then there is a solution to the set of simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n}. \end{aligned}$$

If  $x_0$  is a solution, then the set of all solutions is the set of integers congruent to  $x_0$  modulo  $M = m_1 m_2 \cdots m_n$ .

*Proof* The proof is by induction on  $n$ . The case for two congruences was Theorem 11.2.

For  $n > 2$  we assume that any set of  $n - 1$  congruences whose moduli are pairwise coprime has a solution. Suppose we have a set of  $n$  congruences as in the statement of the theorem. We use the theorem for two congruences to replace the first two congruences by a single congruence, of the form

$$x \equiv x_0 \pmod{m_1 m_2}.$$

To show that there is a solution to the original set of  $n$  congruences, we need to show that there is a solution to the set of  $n - 1$  congruences consisting of all but the first two of the  $n$  original congruences, together with the congruence

$$x \equiv x_0 \pmod{m_1 m_2}.$$

To apply the induction hypothesis, the only thing we need to observe is that the new last modulus,  $m_1 m_2$  is coprime to  $m_j$  for  $j = 3, \dots, n$ . But if  $(m_j, m_1) = 1$  and  $(m_j, m_2) = 1$ , then  $m_j$  has no prime factors in common with  $m_1 m_2$ , and so  $(m_j, m_1 m_2) = 1$ . Thus the set of  $n - 1$  congruences has a solution by the induction hypothesis, and that solution will be a solution to the original  $n$  congruences.

The last statement of the theorem is a consequence of the facts, easily proved by uniqueness of factorization in Section 4.1, that if  $m_1, \dots, m_n$  are pairwise coprime, then their least common multiple is their product, and divides any common multiple.  $\square$

*Example 11.8* Suppose we wish to solve the system:

$$\begin{aligned} x &\equiv 7 \pmod{13} \\ x &\equiv 4 \pmod{17} \\ x &\equiv 1 \pmod{21}. \end{aligned}$$

The three moduli, 13, 17 and 21, are pairwise coprime, so we know there is a unique solution modulo  $13 \cdot 17 \cdot 21 = 4641$ .

We first replace the first two congruences by a congruence modulo  $[13, 17] = 221$ . In Example 2 we found Bezout's identity:

$$1 = 13 \cdot 4 + 17 \cdot (-3) = e_2 + e_1,$$

so

$$e_1 = -17 \cdot 3 = -51$$

$$e_2 = 13 \cdot 4 = 52.$$

Then

$$x = 7e_1 + 4e_2 = -357 + 208 = -149 \equiv 72 \pmod{221}.$$

To solve the original system of three congruences, we are reduced to solving the pair of congruences

$$x \equiv 72 \pmod{221}$$

$$x \equiv 1 \pmod{21}.$$

We find Bezout's identity for 221 and 21 (we omit the calculations, using Euclid's algorithm and the EEA):

$$1 = 2 \cdot 221 - 21 \cdot 21 = 442 - 441 = e_2 + e_1.$$

So  $e_1 = -441$ ,  $e_2 = 442$  and

$$x = 72 \cdot e_1 + 1 \cdot e_2 = 72 \cdot (-441) + 1 \cdot 442 = -31310.$$

Since  $221 \cdot 21 = 4641$ , the general solution is

$$x \equiv -31310 \pmod{4641}.$$

The smallest positive solution is  $x = -31310 + 7 \cdot 4641 = 1177$  (which we check:  $1177 = 221 \cdot 5 + 72 = 21 \cdot 56 + 1$ ).

### 11.3 Some Applications to RSA Cryptography

**i. RSA Decrypting.** Suppose Bob constructs an RSA cryptosystem for Alice to use to send messages to Bob. Recall that Bob does this as follows: he finds two large primes  $p$  and  $q$  and sets  $m = pq$  (the modulus). He picks an encrypting exponent  $e$  that is coprime to  $\phi(m) = (p-1)(q-1)$ , finds a decrypting exponent  $d$  satisfying  $ed \equiv 1 \pmod{\phi(m)}$ , and sends  $m$  and  $e$  to Alice. To make computations easy for Alice, he chooses  $e$  to be a small number (such as  $e = 3$ , or 7).

To send the message  $w$  to Bob, Alice computes  $c = w^e$  modulo  $m$  and sends Bob  $c$ . To determine  $w$ , Bob must compute  $c^d$  modulo  $m$ . But  $c$  is going to be a number of almost the same number of digits as  $m$ , and since  $e$  is small,  $d$  will have almost the same number of digits as  $m$ . Thus determining  $c^d$  modulo  $m$  takes a bit of effort.

But Bob has the advantage that he knows that  $m = pq$ . So he can proceed as follows:

- (i) Compute  $y \equiv c^d \pmod{p}$  and  $z \equiv c^d \pmod{q}$  where  $y < p$  and  $z < q$ .
- (ii) Find  $x < m = pq$  so that

$$x \equiv y \pmod{p}$$

$$x \equiv z \pmod{q}.$$

Then

$$\begin{aligned}x &\equiv c^d \pmod{p} \\x &\equiv c^d \pmod{q},\end{aligned}$$

so

$$x \equiv c^d \pmod{pq},$$

and  $pq = m$ . Since  $w \equiv c^d \pmod{m}$  and  $0 < w < m$ , we must have  $x = w$ .

*Example 11.9* To illustrate how this works, suppose the modulus  $m = 187 = 11 \cdot 17$ , the encrypting exponent is  $e = 3$  and Alice wants to send  $w = 127$  to Bob. Alice encrypts  $w$  to get  $c = 127^3 \equiv 172 \pmod{187}$ , and sends  $c$  to Bob. The decrypting exponent is  $d = 107$ , so Bob needs to find  $w \equiv c^d \equiv 172^{107} \pmod{187}$ . He begins the decrypting by computing

$$172^{107} \pmod{11}$$

and

$$172^{107} \pmod{17}.$$

Now  $172 \equiv 7 \pmod{11}$ , so  $172^{107} \equiv 7^{107}$ , and this is congruent to  $7^7$ , since  $7^{10} \equiv 1 \pmod{11}$  by Fermat's Theorem. One can check easily that  $7^7 \equiv 6 \pmod{11}$ .

Also,  $172 \equiv 2 \pmod{17}$ , and again using Fermat's Theorem,  $172^{107} \equiv 2^{107} \equiv 2^{11} \pmod{17}$ . But  $2^4 \equiv -1 \pmod{17}$ , so  $2^{11} \equiv 2^3 = 8 \pmod{17}$ .

Thus  $w \equiv c^d \equiv 172^{107} \pmod{187}$  satisfies

$$\begin{aligned}w &\equiv 6 \pmod{11} \\w &\equiv 8 \pmod{17}.\end{aligned}$$

If Bob had previously found Bezout's identity for 17 and 11:

$$1 = (-3) \cdot 11 + 2 \cdot 17 = e_2 + e_1,$$

then he knows that

$$\begin{aligned}e_1 &= 17 \cdot 2 = 34 \equiv 1 \pmod{11}, \\&\equiv 0 \pmod{17}\end{aligned}$$

and

$$\begin{aligned}e_2 &= 11 \cdot -3 = -33 \equiv 0 \pmod{11}, \\&\equiv 1 \pmod{17}.\end{aligned}$$

Having found that  $w \equiv 6 \pmod{11}$ ,  $w \equiv 8 \pmod{17}$ , Bob can write down

$$w \equiv 6e_1 + 8e_2 = 6 \cdot 34 + 8 \cdot (-33) = 204 - 264 = -60 \pmod{187}.$$

Since  $0 < w < 187$ , he finds the smallest positive number satisfying  $w \equiv -60 \pmod{187}$ , namely,

$$w = -60 + 187 = 127.$$

If Alice sends a long message to Bob, she would break up the message into words  $w_1, \dots, w_g$  of numbers  $< m$  and encrypt all of them with the same encrypting exponent  $e$  to get encrypted words  $c_1, \dots, c_g$ . Bob would decrypt each of them with the decrypting exponent  $d$  as above, finding  $c_k$  modulo

$p$  and  $c_k$  modulo  $q$  for each  $k$  and then solving

$$\begin{aligned} w_k &\equiv c_k^d \pmod{p} \\ w_k &\equiv c_k^d \pmod{q} \end{aligned}$$

for  $w_k < pq$ . To do this efficiently, Bob could use the method of Proposition 11.3: in anticipation of Alice's message, Bob finds Bezout's identity for  $p$  and  $q$ :

$$1 = ap + bq = e_2 + e_1,$$

where  $-q < a < q$  and  $-p < b < p$ . Then

$$e_1 = bq \equiv 1 \pmod{p}, \quad e_1 \equiv 0 \pmod{q},$$

and

$$e_2 = ap \equiv 0 \pmod{p}, \quad e_2 \equiv 1 \pmod{q}.$$

Then, for each  $1 \leq k \leq g$ , having reduced Alice's  $k$ th encrypted word modulo  $p$  and modulo  $q$  to find

$$y_k = c_k^d \pmod{p}$$

and

$$z_k = c_k^d \pmod{q},$$

Bob can find  $w_k$  modulo  $m = pq$  by

$$w_k \equiv e_1 y_k + e_2 z_k \pmod{pq}.$$

The right side of this congruence is the difference of two numbers  $< m^2$ , so it is easy to reduce the right side modulo  $m = pq$  to a number  $< m$ .

As we've just seen, finding  $e_1$  and  $e_2$  from Bezout's identity enables Bob to quickly solve a sequence of pairs of congruences modulo  $p$  and  $q$ .

It has been estimated that decrypting using the Chinese Remainder Theorem in this way requires somewhere between 1/4 and 1/3 of the time needed to compute  $c^d$  modulo  $m$  directly. Note however, that only someone who knows the factorization of the modulus  $m$  can use this method. That's why, if Bob designed the cipher, then the exponent used by Alice should be small to minimize her computations, since she cannot use the Chinese Remainder Theorem to encrypt.

**ii. RSA moduli with more than two factors.** In 1997 a US patent was issued for an RSA cryptosystem using a modulus with more than two primes [CH97].

There is some benefit for doing RSA with a modulus of the form  $m = p_1 p_2 \cdots p_g$ , where  $p_1, p_2, \dots, p_g$  are distinct primes of  $d$  digits. The reason is that as of 2015 the recommended size of an RSA modulus for long-term security is 3072 binary bits, or 924 decimal digits. This recommendation is based on the fact that the time required for the best known factoring algorithms to factor a modulus depends on the size of the modulus.

But the time required for factoring algorithms does not depend so much on the size of the prime factors of the modulus. So one way to increase the modulus without severely affecting the efficiency of an RSA cryptosystem is to use a modulus with more than two prime factors.

For example, using a 924 digit modulus that is a product of six 154 digit primes would be far more secure than using a 308 digit modulus with two 154 digit prime factors. On the other hand, using the

Chinese Remainder Theorem, decrypting would be significantly faster with the six-prime 924 digit modulus than it would be for a 924 digit modulus that is a product of two 462 digit primes.

So how would Bob design an RSA system with a modulus that is a product of more than two primes? We'll do the case of three primes.

Bob picks distinct primes  $p_1, p_2, p_3$  at random, and sets  $m = p_1 p_2 p_3$ . He knows  $\phi(m) = (p_1 - 1)(p_2 - 1)(p_3 - 1)$ . He picks a small encrypting exponent  $e$  and verifies that it is coprime to  $\phi(m)$  by finding  $d$ , the decrypting exponent, so that  $ed \equiv 1 \pmod{\phi(m)}$ . He sends  $(m, e)$  to Alice. For subsequent decrypting, he also finds integers  $e_1, e_2, e_3$  that satisfy

$$\begin{aligned} e_1 &\equiv 1 \pmod{p_1}, & e_1 &\equiv 0 \pmod{p_2 p_3}; \\ e_2 &\equiv 1 \pmod{p_2}, & e_2 &\equiv 0 \pmod{p_1 p_3}; \\ e_3 &\equiv 1 \pmod{p_3}, & e_3 &\equiv 0 \pmod{p_1 p_2}. \end{aligned}$$

Alice has a message  $w$ , a number  $< m$ . She encrypts by computing  $c = (w^e \pmod{m})$ , using the XS-binary algorithm, which won't be too onerous if  $e$  is small. She sends  $c$  to Bob.

To decrypt, Bob computes  $(c^d \pmod{m})$  using the Chinese Remainder Theorem, by first computing

$$\begin{aligned} w_1 &= (c^d \pmod{p_1}), \\ w_2 &= (c^d \pmod{p_2}), \\ w_3 &= (c^d \pmod{p_3}). \end{aligned}$$

Then he finds

$$w_0 = ((w_1 e_1 + w_2 e_2 + w_3 e_3) \pmod{m}).$$

Then  $w_0 \equiv c^d \pmod{m}$  and  $w_0 < m$ , so  $w_0 = w$ , Alice's plaintext word.

The extension to a modulus  $m$  with more than three distinct primes should be clear.

With a modulus  $m$  of 1024 bits that is a product of three 342-bit primes, all computations except the final determination of  $w$  from reducing  $w_1 e_1 + w_2 e_2 + w_3 e_3$  modulo  $m$  involve numbers no larger than  $p_i^2$ , or about 684 bits. By contrast, if  $m$  is the product of two 512 bit primes  $q_1$  and  $q_2$ , computing  $c^d \pmod{q_i}$  would involve numbers of size as large as  $q_j^2$ , or about 1024 bits. Boneh and Shacham [BS02] considered that situation and found that decrypting the two-prime RSA took 1.73 as much time as the three-prime RSA for moduli of the same size. (The authors warned against using more than three primes, because at the time, numbers with prime factors of under 256 bits could be factored with a sufficiently dedicated effort. Presumably both the warning and the speed of computation are applicable to larger moduli.) Boneh and Shacham [BS02] also considered moduli of the form  $m = p^2 q$  with  $p, q$  primes and found a larger speedup in decrypting compared to a modulus  $m' = p' q'$  of the same size.

**iii. Common encrypting exponents.** Suppose Alice, a financial advisor, has three clients, Bill, Bob and Brian, with whom she communicates using RSA. Each client has his own modulus,  $m_1, m_2$  and  $m_3$ , respectively. Alice wants to send privileged information about a particular stock to all three of them. For convenience, Alice uses the encrypting exponent  $e = 3$  for each client. So Alice sends the same message  $w$  to each of them, as follows: To Bill she sends  $c_1 \equiv w^3 \pmod{m_1}$ . To Bob she sends  $c_2 \equiv w^3 \pmod{m_2}$ . To Brian she sends  $c_3 \equiv w^3 \pmod{m_3}$ .

Eve (perhaps an agent looking for violations of insider trading laws) intercepts  $c_1, c_2, c_3$  and knows  $m_1, m_2, m_3$  and  $e = 3$ . She doesn't know  $w$  or  $w^3$ , but she knows  $c_1, c_2$  and  $c_3$ , and that

$$\begin{aligned} w^3 &\equiv c_1 \pmod{m_1} \\ w^3 &\equiv c_2 \pmod{m_2} \\ w^3 &\equiv c_3 \pmod{m_3}. \end{aligned}$$

So she solves

$$\begin{aligned} t &\equiv c_1 \pmod{m_1} \\ t &\equiv c_2 \pmod{m_2} \\ t &\equiv c_3 \pmod{m_3} \end{aligned}$$

for some number  $t < m_1 m_2 m_3$ . Then

$$t \equiv w^3 \pmod{m_1 m_2 m_3}.$$

But  $w < m_i$  for  $i = 1, 2, 3$ , so  $w^3 < m_1 m_2 m_3$ . Thus  $t = w^3$ .

Once Eve finds  $t$ , she can simply compute the cube root of  $t$  to decrypt the message  $w$ .

The point of this example is that one should not send the same message with the same small encrypting exponent  $e$  to  $e$  or more different recipients.

Before returning to general systems of congruences, we note that the Chinese Remainder Theorem will also show up in Chapter 13. We'll discuss discrete logarithms and cryptography based on them in Chapter 13. The CRT is at the core of a method for finding discrete logarithms.

## 11.4 Solving General Systems of Congruences

The methods so far in this chapter have dealt with systems of congruences to coprime moduli. Those methods suffice for decrypting in RSA, as we have just seen. But for completeness, we now describe whether and how we can solve systems of congruences where the moduli need not be pairwise coprime. In those cases the method of finding solutions as a linear combination of terms in Bezout's identity doesn't work well, because the greatest common divisor in Bezout's identity may be  $> 1$ . So in the next two sections we present two methods for solving general systems of congruences. We begin by recalling how to solve one congruence.

**One congruence.** Consider the congruence

$$ax \equiv b \pmod{m}.$$

We looked at single congruences in Section 3.7. There are two ways to solve them, a systematic way and an ad hoc way.

The systematic way to solve a single linear congruence is to translate the congruence into the linear diophantine equation

$$ax + my = b.$$

If the greatest common divisor of  $a$  and  $m$  does not divide  $b$ , then there is no solution to this equation with  $x, y$  integers, because if there were, then the left side would be a multiple of  $(a, m)$ , but the right side,  $b$ , would not be.

On the other hand, if  $d = (a, m)$  does divide  $b$ , say  $b = b'd$  for some integer  $b'$ , then we can solve the equation by using Bezout's identity: find integers  $r, s$  so that

$$ar + ms = d.$$

Then

$$arb' + msb' = db' = b,$$

so  $x_0 = rb'$ ,  $y_0 = sb'$  is a solution to the equation.

Once a solution  $x = x_0$  is found for  $ax \equiv b \pmod{m}$ , then the set of solutions of  $ax \equiv b \pmod{m}$  can be expressed as the congruence

$$x \equiv x_0 \pmod{m/(a, m)},$$

as shown in Corollary 3.36.

The ad hoc way to approach a congruence  $ax \equiv b \pmod{m}$  is to use properties of congruence, as shown in Section 3.7. Reversible things we can do to any congruence include:

- we can replace numbers by other numbers they are congruent to modulo  $m$ ,
- we can multiply both sides by a number coprime to  $m$ .
- we can cancel from both sides a number coprime to  $m$ .
- we can cancel from the modulus and from both sides any number that is a common factor of all three.

We can try to use these to turn the congruence into one that is easier to solve.

For congruences involving small numbers, manipulations often yield solutions fairly quickly.

*Example 11.10* We solve

$$82x \equiv 1 \pmod{103}.$$

Replace 82 by  $-21$ :

$$-21x \equiv 1 \pmod{103}$$

Multiply by 5:

$$-105x \equiv 5 \pmod{103}$$

Replace  $-105$  by  $-2$ , then replace 5 by 108:

$$-2x \equiv 108 \pmod{103}$$

Canceling 2 and multiplying by  $-1$  gives:

$$x \equiv -54 = 49 \pmod{103}.$$

Manipulations other than what are shown will also work. You can be creative (as long as you follow the rules)!

## 11.5 Solving Two Congruences

Here is the general theorem on solutions of systems of two congruences. It generalizes the Chinese Remainder Theorem (which covers the case when the moduli are coprime).

**Theorem 11.11** *Let  $m$  and  $n$  be natural numbers  $> 1$  (the moduli) and  $a, b$  be any integers. Then there is a solution  $x = x_0$  to*

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n},$$

*if and only if the greatest common divisor of  $m$  and  $n$  divides  $b - a$ . If  $x = x_0$  is a solution, then the set of integers  $x$  that satisfy the two congruences is the same as the set of  $x$  that satisfy*

$$x \equiv x_0 \pmod{[m, n]}$$

*where  $[m, n]$  is the least common multiple of  $m$  and  $n$ .*

Before proving the theorem, we look at three examples, which illustrate in two ways how to solve the pair of congruences when a solution exists.

### The systematic method.

*Example 11.12* Consider the pair of congruences

$$\begin{aligned} x &\equiv 2 \pmod{24} \\ x &\equiv 8 \pmod{39}. \end{aligned}$$

If  $x$  is a solution, then

$$x = 2 + 24r$$

for some integer  $r$ , and

$$x = 8 + 39s$$

for some integer  $s$ . Setting the two expressions for  $x$  equal to each other, we obtain

$$2 + 24r = 8 + 39s$$

or, collecting the constants,

$$24r - 39s = 6,$$

a linear diophantine equation studied in Chapter 3. Since the greatest common divisor of 24 and 39, namely 3, divides 6, this equation is solvable using the extended Euclidean algorithm to solve Bezout's identity. Doing so, we get  $24 \cdot 5 - 39 \cdot 3 = 3$ , so

$$24 \cdot 10 - 39 \cdot 6 = 6.$$

So  $r = 10, s = 6$ . Substituting  $r$  and  $s$  in the expressions for  $x$  gives a solution  $x = 2 + 240 = 8 + 234 = 242$  to the two congruences.

Once we find a particular solution  $x = 242$  to

$$\begin{aligned} x &\equiv 2 \pmod{24} \\ x &\equiv 8 \pmod{39}. \end{aligned}$$

we can find the general solution by adding to the particular solution  $x = 242$  the general solution to the homogeneous system of congruences,

$$\begin{aligned} x &\equiv 0 \pmod{24} \\ x &\equiv 0 \pmod{39}, \end{aligned}$$

which is the same as the set of integers  $x$  such that

$$x \equiv 0 \pmod{[24, 39] = 312}.$$

So the set of all solutions to the set of congruences

$$\begin{aligned}x &\equiv 2 \pmod{24} \\x &\equiv 8 \pmod{39},\end{aligned}$$

is the set of all integers  $x$  so that

$$x = 242 + 312k$$

for some integer  $k$ . This is the same as the set of integers  $x$  that satisfy the congruence

$$x \equiv 242 \pmod{312}.$$

**Solving by reducing to a single congruence.** An alternative method for solving a system of two congruences is to reduce the problem to a problem to solve a single congruence. If we have

$$\begin{aligned}x &\equiv b \pmod{m} \\x &\equiv d \pmod{n},\end{aligned}$$

where  $m < n$ , observe that the second congruence has solutions

$$x = d + nt$$

where  $t$  can be any integer. Put that expression for  $x$  into the first congruence:

$$d + nt \equiv b \pmod{m}.$$

Then solve this congruence for  $t$  by one of the methods above.

*Example 11.13* Repeating Example 8, we seek all solutions to

$$\begin{aligned}x &\equiv 2 \pmod{24} \\x &\equiv 8 \pmod{39}.\end{aligned}$$

To turn this into a single congruence, we write  $x = 8 + 39t$  and substitute for  $x$  in the first congruence to get

$$8 + 39t \equiv 2 \pmod{24}.$$

Simplifying gives

$$39t \equiv -6 \pmod{24}.$$

Reduce 39 to 15 modulo 24 and then divide everything by  $3 = (39, 24)$  to get

$$5t \equiv -2 \pmod{8}.$$

Now  $-2 \equiv 30 \pmod{8}$ , so  $t \equiv 6 \pmod{8}$ . Then  $x = 8 + 39 \cdot 6 = 242$ . The general solution to the two congruences is

$$x \equiv 242 \pmod{[24, 39]}$$

or

$$x \equiv 242 \pmod{312}.$$

*Example 11.14* Consider

$$\begin{aligned}x &\equiv 5 \pmod{20} \\x &\equiv 15 \pmod{16}.\end{aligned}$$

We set  $x = 5 + 20r$  and put it into the second congruence to get

$$5 + 20r \equiv 15 \pmod{16},$$

or

$$4r \equiv 10 \pmod{16}.$$

But this has no solution, because  $(4, 16) = 4$  does not divide 10. So there is no solution to the pair of congruences.

The proof of Theorem 11.11 follows the systematic (Bezout's identity) method of Example 11.12.

*Proof* Recall that Theorem 11.11 states that the pair of congruences  $x \equiv a \pmod{m}$ ,  $x \equiv b \pmod{n}$  has a solution if and only if  $(m, n)$  divides  $b - a$ .

We suppose  $x$  is a solution to the two congruences

$$\begin{aligned}x &\equiv a \pmod{m} \\x &\equiv b \pmod{n}.\end{aligned}$$

Since  $x$  is a solution to the first congruence,  $x = a + my$  for some integer  $y$ . Also,  $x = b + nz$  for some integer  $z$ . Setting the two expressions equal yields the equation

$$a + my = b + nz.$$

This is equivalent to the linear diophantine equation

$$my - nz = b - a.$$

Now:

- if the greatest common divisor  $d$  of  $m$  and  $n$  does not divide  $b - a$ , then there is no integer solution to the linear diophantine equation. Thus there is no integer  $x$  that solves the original pair of congruences.
- if  $d = (m, n)$  divides  $b - a$ , so that  $b - a = qd$ , then Bezout's identity solves the equation as follows: we find integers  $t$  and  $w$  so that  $mt + nw = d$ . Multiplying both sides by  $q$  gives  $m(tq) + n(wq) = b - a$ . Hence  $y = tq$ ,  $z = -wq$  solves  $my - nz = b - a$ , and so  $x = a + my = b + nz$  is a solution to the original pair of congruences.

These two cases prove the first part of Theorem 11.11.

For the second part, we assume that  $x_0$  is a solution to  $x \equiv a \pmod{m}$ ,  $x \equiv b \pmod{n}$ , and we want to show that all other solutions to the congruences are congruent to  $x_0$  modulo  $[m, n]$ .

First, observe that if  $x_0$  is a solution to the pair of congruences and  $x$  satisfies  $x \equiv x_0 \pmod{[m, n]}$  for some integer  $k$ , then  $x \equiv x_0 \pmod{m}$  and  $x \equiv x_0 \pmod{n}$ . So  $x$  is also a solution to the original pair of congruences.

Now suppose  $x_0$  and  $x_1$  are solutions to the pair of congruences. Then  $x_1 - x_0$  is a solution to the “homogeneous” pair of congruences

$$\begin{aligned}u &\equiv 0 \pmod{m} \\u &\equiv 0 \pmod{n}.\end{aligned}$$

That means  $x_1 - x_0$  is a common multiple of  $m$  and  $n$ . Hence  $x_1 - x_0$  is a multiple of the least common multiple  $[m, n]$ . Hence  $x_1 - x_0 = [m, n]k$  for some  $k$ , and so

$$x_1 = x_0 + [m, n]k$$

for some  $k$ .

To sum up what we have found, once we have some solution  $x = x_0$  to the pair of congruences, all solutions to the pair of congruences are of the form  $x = x_0 + u$ , where  $u$  is any solution to the pair of homogeneous congruences

$$\begin{aligned} u &\equiv 0 \pmod{m} \\ u &\equiv 0 \pmod{n}. \end{aligned}$$

The solutions are  $u = [m, n]t$  for all integers  $t$ . Thus the set of solutions to the original pair of congruences is the set of integers  $x$  satisfying  $x = x_0 + [m, n]t$  for all  $t$ .

We can express the set of solutions to the two original congruences as the set of  $x$  satisfying the single congruence

$$x \equiv x_0 \pmod{[m, n]},$$

thus replacing the two original congruences by a single congruence.  $\square$

## 11.6 Three or More Congruences

As we saw earlier, the key to solving systems of more than two simultaneous congruences is the observation that we can express the set of integers that solve two simultaneous congruences as the set of integers that satisfy one congruence.

*Example 11.15* We find all solutions to

$$\begin{aligned} x &\equiv 2 \pmod{12} \\ x &\equiv 8 \pmod{10} \\ x &\equiv 9 \pmod{13}. \end{aligned}$$

We first solve the first two: we find  $x$  of the form  $x = 2 + 12r = 8 + 10s$ . It's easy enough to see that  $x = 38$  is a solution. Since  $[12, 10] = 60$ , the general solution to the first two congruences is  $x = 38 + 60k$  for  $k$  any integer. Thus to solve the three congruences is the same as to solve

$$\begin{aligned} x &\equiv 38 \pmod{60} \\ x &\equiv 9 \pmod{13}. \end{aligned}$$

In this pair of congruences, the modulus 13 is smaller than the modulus 60 arising from the first two original congruences. Hence the congruence method of solution is particularly helpful.

So we set  $x = 38 + 60t$ , coming from the congruence involving the larger modulus, and substitute into the congruence with the smaller modulus, to get

$$38 + 60t \equiv 9 \pmod{13}$$

which reduces modulo 13 to

$$-1 - 5t \equiv 9 \pmod{13}$$

or

$$-5t \equiv 10 \pmod{13}.$$

Thus

$$t \equiv -2 \equiv 11 \pmod{13}.$$

Having found  $t$ , we substitute for  $t$  in the expression for  $x$  to get

$$x = 38 + 60 \cdot 11 = 698.$$

The general solution to the original three congruences is then

$$x \equiv 698 \pmod{780}$$

since  $[10, 12, 13] = 60 \cdot 13 = 780$ .

## 11.7 Systems of Non-monic Linear Congruences

In Chapter 3 we determined all solutions to the congruence  $ax \equiv b \pmod{m}$ . We finish this chapter by looking briefly at linear systems of the form

$$\begin{aligned} ax &\equiv b \pmod{m} \\ cx &\equiv d \pmod{n}, \end{aligned}$$

where the coefficients  $a$  and  $c$  are any integers. We illustrate by an example.

*Example 11.16* To solve

$$6x \equiv 14 \pmod{20}$$

$$9x \equiv 11 \pmod{25},$$

we can first solve the first congruence, to get  $x \equiv -1 \pmod{10}$ . We then set  $x = -1 + 10t$  into the second congruence to get

$$9(-1 + 10k) \equiv 11 \pmod{25}$$

and simplify to get

$$15k \equiv 20 \pmod{25},$$

which has a solution  $k = 3$ ,  $x = -1 + 30 = 29$ .

Once we find one solution, then, since  $[25, 20] = 100$ , the general solution is

$$x \equiv 29 \pmod{100}.$$

Extending this to systems of three or more linear congruences is a matter of successively reducing a system of two congruences to a single congruence.

We've completed the story on how to solve systems of linear congruences.

## Exercises

- 11.1. (i) Find  $e_1$  and  $e_2$  so that

$$\begin{aligned} e_1 &\equiv 1 \pmod{15} \\ e_1 &\equiv 0 \pmod{22} \end{aligned}$$

and

$$\begin{aligned} e_2 &\equiv 0 \pmod{15} \\ e_2 &\equiv 1 \pmod{22}. \end{aligned}$$

Then use  $e_1$  and  $e_2$  to find all solutions to

$$\begin{aligned} x &\equiv a \pmod{15} \\ x &\equiv b \pmod{22} \end{aligned}$$

for

- (ii)  $(a, b) = (3, 7)$ ;
- (iii)  $(a, b) = (11, 18)$ ;
- (iv)  $(a, b) = (13, 20)$ ;

- 11.2. Use the Bezout's identity method to solve

$$\begin{aligned} x &\equiv a \pmod{41} \\ x &\equiv b \pmod{59} \end{aligned}$$

for

- (i)  $(a, b) = (1, 0)$ , (ii)  $(a, b) = (0, 1)$ , (iii)  $(a, b) = (11, 80)$ .

- 11.3. Find all solutions to

$$\begin{aligned} x &\equiv 13 \pmod{99} \\ x &\equiv 8 \pmod{101}. \end{aligned}$$

- 11.4. Find  $w < 323 = 17 \cdot 19$  so that

$$w \equiv 36^{200} \pmod{323}$$

by the method in the introduction to this chapter.

- 11.5. To find an integer  $e_2 \equiv 0 \pmod{221}$ ,  $e_2 \equiv 1 \pmod{21}$  in Example 11.8, we can write  $e_2 = 221t$  and substitute it into the congruence  $e_2 \equiv 1 \pmod{21}$ . Do so and solve for  $t$  to get  $e_2$ . Then find  $e_1$  by a simple subtraction.
- 11.6. (i) Solve Bezout's Identity for 20 and 23.  
(ii) Using (i), find all solutions to

$$\begin{aligned} x &\equiv 6 \pmod{20} \\ x &\equiv 14 \pmod{23}. \end{aligned}$$

- (iii) Using (i), find all solutions to

$$\begin{aligned} x &\equiv 15 \pmod{20} \\ x &\equiv 2 \pmod{23}. \end{aligned}$$

- 11.7. (i) Write the set of solutions to

$$\begin{aligned}x &\equiv 6 \pmod{20} \\x &\equiv 14 \pmod{23}.\end{aligned}$$

as the set of solutions to a single congruence modulo 460. (c.f. Exercise 11.6).

- (ii) Using (i), find all solutions to

$$\begin{aligned}x &\equiv 6 \pmod{20} \\x &\equiv 14 \pmod{23} \\x &\equiv 5 \pmod{27}.\end{aligned}$$

Write the set of solutions as a set of solutions to a single congruence modulo  $m$ . What is  $m$ ?

- 11.8. A Chinese problem dating from around 270 AD is equivalent to solving

$$\begin{aligned}x &\equiv 2 \pmod{3} \\x &\equiv 3 \pmod{5} \\x &\equiv 2 \pmod{7}.\end{aligned}$$

Find the smallest positive solution.

- 11.9. Find the least non-negative residue of

$$95^{1000} \pmod{217}$$

by setting the problem up as that of solving a system of two congruences, as in Example 11.1.

- 11.10. Find

$$30^{40} \pmod{143}.$$

- 11.11. Note that  $391 = 17 \cdot 23$ . Is 391 a 100-pseudoprime?

- 11.12. Find

$$500^{500} \pmod{391}.$$

- 11.13. Solve  $82x \equiv 1 \pmod{103}$  by the Bezout's Identity method.

- 11.14. Solve  $81x \equiv 40 \pmod{101}$ .

- 11.15. Solve  $80x \equiv 41 \pmod{100}$ .

- 11.16. Solve, if possible,

$$\begin{aligned}x &\equiv 13 \pmod{24} \\x &\equiv 23 \pmod{27}.\end{aligned}$$

- 11.17. Solve, if possible,

$$\begin{aligned}x &\equiv 11 \pmod{24} \\x &\equiv 23 \pmod{27}.\end{aligned}$$

- 11.18. Solve, if possible,

$$\begin{aligned}x &\equiv 11 \pmod{24} \\x &\equiv 3 \pmod{10} \\x &\equiv 8 \pmod{15}.\end{aligned}$$

- 11.19. In Example 11.9 with  $e = 3, d = 107$ , suppose you receive  $w^3 = c = 93$  from Alice. Knowing the factorization of 187, find  $93^{107} \pmod{187}$  and determine Alice's message  $w$ .

- 11.20. (i) Find Bezout's Identity for 53 and 61.

Using RSA, you send Alice the modulus  $m = 3233 (= 53 \cdot 61)$  and the encrypting exponent  $e = 7$ . Alice has a two-letter message that she turns into a number  $\leq 2626$  and encrypts and sends to you. You receive  $c = 1067$ . You have already determined that the decrypting exponent is  $d = 1783$ .

(ii) Find  $1067^{1783} \pmod{53}$  and  $1067^{1783} \pmod{61}$ .

(iii) Then use Bezout's identity from (i) to find Alice's plaintext message.

- 11.21. Let  $m = rs$  with  $r, s$  odd and coprime.

(i) Show that any  $w$  so that  $w^2 \equiv 1 \pmod{m}$  must satisfy

$$\begin{aligned} w^2 &\equiv 1 \pmod{r} \\ w^2 &\equiv 1 \pmod{s}. \end{aligned}$$

(ii) Show that if  $b^2 \equiv 1 \pmod{r}$  and  $c^2 \equiv 1 \pmod{s}$ , then the unique solution  $x = w$  modulo  $m$  of

$$x \equiv b \pmod{r}$$

$$x \equiv c \pmod{s}$$

satisfies  $w^2 \equiv 1 \pmod{m}$ .

(iii) Noting that  $(-1)^2 = (1)^2 \equiv 1 \pmod{r}$  and  $\pmod{s}$ , show that the congruence

$$x^2 \equiv 1 \pmod{m}$$

has at least four solutions  $x$  with  $0 < x < m$ .

(iv) Show that if  $m = pq$  where  $p$  and  $q$  are odd primes, then the congruence

$$x^2 \equiv 1 \pmod{m}$$

has exactly four solutions  $x$  with  $0 < x < m$ . (Hint: what are the solutions to  $x^2 \equiv 1 \pmod{p}$  for  $p$  a prime.)

- 11.22. Suppose we set up a demonstration RSA cryptosystem for students with  $m = 55$ , and assume that the encrypting exponent is  $e = 3$ . Show that there are exactly nine numbers  $w$  with  $0 \leq w < m$  with

$$w^e \equiv w \pmod{m},$$

so that  $w$  is unchanged under encryption. (It would be embarrassing to use one of those numbers as a plaintext message!)

- 11.23. Suppose we set up an RSA cryptosystem with  $m = pq$ , a product of distinct odd primes, and assume that the encrypting exponent  $e$  is coprime to  $\phi(m)$ .

(i) Show that the group  $U_p(e - 1)$  of  $(e - 1)$ -th roots of unity in  $\mathbb{Z}/p\mathbb{Z}$  has order at least 2. Show that  $U_q(e - 1)$  also has order at least 2.

(ii) Show that there are exactly nine solutions  $w$  with  $0 \leq w < m$  of the congruence

$$w^e \equiv w \pmod{m}.$$

(The solutions are plaintext messages that are unchanged under encryption by  $e$ .)

- 11.24. Let  $p_1 = 11$ ,  $p_2 = 17$ ,  $p_3 = 23$ ,  $m = p_1 p_2 p_3 = 4301$ . Then  $\phi(m) = 3520$ . Bob sends  $(e, m) = (7, 4301)$  to Alice. Alice has a message  $w < 4301$  that she encrypts as

$$w^7 \equiv c = 3328 \pmod{m}.$$

(i) Help Bob find the decrypting exponent by solving  $7d \equiv 1 \pmod{\phi(m)}$ .

Then compute  $3328^d \pmod{4301}$  as follows:

(ii) Find  $e_1, e_2$  and  $e_3$  satisfying

$$\begin{aligned} e_1 &= 17 \cdot 23t_1 \equiv 1 \pmod{11} \\ e_2 &= 11 \cdot 23t_2 \equiv 1 \pmod{17} \\ e_3 &= 11 \cdot 17t_3 \equiv 1 \pmod{23}. \end{aligned}$$

(iii) Find  $3328^{e_1} \pmod{11}$ ,  $\pmod{17}$  and  $\pmod{23}$ .

(iv) Then find Alice's message  $w$ .

- 11.25. Let  $p$  be a prime number. Show that

$$\begin{aligned} x &\equiv a \pmod{p^e} \\ x &\equiv b \pmod{p^{e+r}} \end{aligned}$$

with  $e > 0$ ,  $r \geq 0$  has the solution  $x \equiv b \pmod{p^{e+r}}$  if  $a \equiv b \pmod{p^e}$ , and has no solution otherwise.

Here is an alternative way to approach a system of congruences to non-coprime moduli.

Consider

$$\begin{aligned} x &\equiv a \pmod{20} \\ x &\equiv b \pmod{24}. \end{aligned}$$

Factor the moduli and split each congruence into a system of congruences to coprime moduli:

$$\begin{aligned} x &\equiv a \pmod{5} \\ x &\equiv a \pmod{4} \\ x &\equiv b \pmod{8} \\ x &\equiv b \pmod{3}. \end{aligned}$$

Then apply Exercise 11.25 to the middle two congruences: there is a solution if and only if  $a \equiv b \pmod{4}$ , in which case the set of four congruences is

$$\begin{aligned} x &\equiv a \pmod{5} \\ x &\equiv b \pmod{8} \\ x &\equiv b \pmod{3}, \end{aligned}$$

which reduces to

$$\begin{aligned} x &\equiv a \pmod{5} \\ x &\equiv b \pmod{24}. \end{aligned}$$

11.26. Using Exercise 11.25, decide if there is a solution to the system

$$\begin{aligned}x &\equiv a \pmod{24} \\x &\equiv b \pmod{27},\end{aligned}$$

where

- (i)  $a = 7, b = 10;$
- (ii)  $a = 4, b = 14.$  In each case, if there is a solution, find all solutions.

11.27. Repeat the last exercise for the system

$$\begin{aligned}x &\equiv a \pmod{112} \\x &\equiv b \pmod{72},\end{aligned}$$

where

- (i)  $a = 7, b = 21;$
- (ii)  $a = 7, b = 31.$

11.28. V. Katz ([Kat98], p. 199f) describes a taxation problem from a nearly 800 year old Chinese treatise. In congruence notation, the problem is: find the smallest positive solution to

$$\begin{aligned}x &\equiv 10 \pmod{12} \\x &\equiv 0 \pmod{11} \\x &\equiv 0 \pmod{10} \\x &\equiv 4 \pmod{9} \\x &\equiv 6 \pmod{8} \\x &\equiv 0 \pmod{7} \\x &\equiv 4 \pmod{6}.\end{aligned}$$

(i) Show that the problem reduces to solving

$$\begin{aligned}x &\equiv -2 \pmod{[12, 8, 6]} \\x &\equiv 0 \pmod{[11, 10, 7]} \\x &\equiv 4 \pmod{9}.\end{aligned}$$

(ii) Find the smallest positive solution to this system of congruences.

(iii) Using Exercise 11.25, rewrite the original system of seven congruences to get a system of congruences to pairwise coprime moduli, and then describe the solutions of the system as the set of solutions to a single congruence.

11.29. Solve  $8x \equiv 15 \pmod{39}.$

11.30. Solve, if possible,

$$21x \equiv 35 \pmod{51}.$$

11.31. Solve, if possible,

$$65x \equiv 38 \pmod{101}.$$

11.32. Solve, if possible,

$$\begin{aligned} 3x &\equiv 13 \pmod{23} \\ 5x &\equiv 17 \pmod{32}. \end{aligned}$$

A prime number  $p$  is called a *safeprime* if  $p = 2q + 1$  where  $q$  is also prime. Examples:  $p = 5, 7, 11, 23, 47, 59, 83, 107, \dots$  Safeprimes are useful primes for cryptography. They are useful for RSA because there are some factoring algorithms (such as the Pollard  $p - 1$  algorithm) that factor large numbers  $m$  more efficiently when one of the prime factors  $p$  of  $m$  has the property that  $p - 1$  is a product of only small primes. They are also useful for Diffie–Hellman key exchange and the Blum–Goldwasser cryptosystem that we'll study later.

11.33. Show that if  $p > 20$  is a safeprime, then using that both  $p$  and  $q$  are prime numbers  $> 10$ , show that

- (i)  $p \equiv 2 \pmod{3}$ ,
- (ii)  $p \equiv 3 \pmod{4}$ ,
- (iii)  $p \equiv 2, 3$  or  $4 \pmod{5}$ .

(iv) Find the set of solutions to the system of congruences

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv b \pmod{5}. \end{aligned}$$

for  $b = 2, 3$  and  $4$ . In each case, write the set of solutions in the form  $x \equiv a \pmod{60}$  for some number  $a < 60$ .

(v) Use (iv) to find all safeprimes  $p$  with  $60 < p < 240$ .

11.34. A prime  $p$  is *special* if  $p = 2p_1 + 1$  and both  $p$  and  $p_1$  are safeprimes.

- (i) Show that a special prime must be congruent to 7 modulo 8;
- (ii) If  $p$  is a special prime  $> 25$ , list all of the possibilities for  $p \pmod{120}$ . (For example, 167 is a special prime and  $(167 \pmod{120}) = 47$ .)

11.35. A Sophie Germain prime is a prime  $q$  so that  $2q + 1 = q_1$  is prime (hence  $q_1$  is a safeprime). For  $n \geq 1$ , let's call  $q$  an  $n$ -SG prime if all of

$$q, 2q + 1 = q_1, 2q_1 + 1 = q_2, 2q_2 + 1 = q_3, \dots, 2q_{n-1} + 1 = q_n$$

are prime. (So every  $n$ -SG prime is a Sophie Germain prime.) Example: 83 is a 1-SG prime; 2 is a 4-SG prime but not a 5-SG prime. Show that

- (i) A 1-SG prime cannot be  $\equiv 7 \pmod{10}$ .
- (ii) A 2-SG prime  $> 5$  must be congruent to 1 or 9  $\pmod{10}$ .
- (iii) A 3-SG prime  $> 5$  must be congruent to 9  $\pmod{10}$ .
- (iv) A Sophie Germain prime  $> 5$  must be  $\equiv 11, 23$  or  $29 \pmod{30}$ .
- (v) A 2-SG prime  $> 5$  must be  $\equiv 11$  or  $29 \pmod{30}$ .
- (vi) A 3-SG prime  $> 5$  must be  $\equiv 29 \pmod{30}$ .
- (vii) Find a 5-SG prime.

# Chapter 12

## Homomorphisms and Euler’s Phi Function



In this chapter we introduce homomorphisms, functions from a ring to a ring (or a group to a group) that “respect” the algebraic operations of the domain and codomain in a sense we shall make precise. A homomorphism is analogous to a linear transformation from a vector space to a vector space in linear algebra.

It should not be surprising that functions show up in algebra. Calculus is almost entirely devoted to the study of functions, and functions of functions (such as the derivative and the definite integral). Elementary linear algebra is predominantly devoted to the study of linear transformations and matrices that represent linear transformations. Functions show up in virtually every area of advanced mathematics.

In this chapter we primarily use homomorphisms to help us better understand the commutative rings  $\mathbb{Z}_m$  and their groups  $U_m$  of units for  $m$  a composite number. Using homomorphisms will provide a “natural” setting for understanding the Chinese Remainder Theorem, and will also yield a proof of the multiplication formula for Euler’s phi function.

The ideas in this chapter will be useful in Chapter 14 to help us understand better the effectiveness of the strong pseudoprime test for testing a number for compositeness, and for understanding the security of RSA. The ideas show up in Chapter 16 in connection with understanding the security of the Blum–Goldwasser cryptosystem. As an introduction to how results in this chapter can be used, we finish the chapter with a characterization of odd Carmichael numbers (Proposition 12.31).

Section 18.5 hints at how homomorphisms can help describe all fields with a finite number of elements.

### 12.1 The Formulas for Euler’s Phi Function

Euler’s phi function  $\phi(m)$  counts the number of units of  $\mathbb{Z}/m\mathbb{Z}$ . Thus  $\phi(m)$  is equal to the number of numbers  $a$  with  $1 \leq a \leq m$  that are coprime to  $m$ .

As noted in the chapter on Euler’s Theorem, the properties of Euler’s phi function are:

- Theorem 12.1** (i) If  $p$  is a prime number, then  $\phi(p) = p - 1$ .  
(ii) If  $p$  is a prime number and  $e \geq 1$ , then  $\phi(p^e) = p^e - p^{e-1}$ .  
(iii) If  $a$  and  $b$  are coprime numbers, then  $\phi(ab) = \phi(a)\phi(b)$ .

These three properties imply that if  $m$  is any number that we know how to factor, then we can find  $\phi(m)$ . For example, to find  $\phi(21000)$ , we observe that

$$21000 = 2^3 \cdot 3 \cdot 5^3 \cdot 7,$$

so

$$\begin{aligned}\phi(21000) &= \phi(2^3)\phi(3)\phi(5^3)\phi(7) \\ &= (8-4)(3-1)(125-25)(7-1) \\ &= 4 \cdot 2 \cdot 100 \cdot 6 = 4800.\end{aligned}$$

Properties (i) and (ii) of Theorem 12.1 are easy: for  $p$  prime, to get the formula  $\phi(p^e) = p^e - p^{e-1}$ , just count the number of numbers  $\leq p^e$  that are multiples of  $p$ . The remaining numbers  $\leq p^e$  are coprime to  $p^e$ .

One purpose of this chapter is give a new proof of (iii): if  $a$  and  $b$  are coprime, then  $\phi(ab) = \phi(a)\phi(b)$ . Knowing this property of  $\phi(m)$  is essential for knowing how to find a decrypting exponent for RSA.

As we shall see, the proof relates to the Chinese Remainder Theorem from Chapter 11:

**Theorem 12.2** (Chinese Remainder Theorem) *Let  $m, n$  be coprime natural numbers  $> 1$ , and  $a, b$  be any integers. Then there is a solution of the set of simultaneous congruences*

$$\begin{aligned}x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}.\end{aligned}$$

If  $x_0$  is a solution, then the set of all solutions is the set of integers congruent to  $x_0$  modulo  $mn$ .

The most conceptual way to prove the formula for Euler's phi function, and, on the way, to prove the Chinese Remainder Theorem, is to obtain the result as an application of a theorem that says that two commutative rings are isomorphic. That is why we introduce in this chapter the concept of a homomorphism, which is a function from one set with certain mathematical properties to another with the same properties, where the function respects those properties. We'll be interested in ring homomorphisms, group homomorphisms, and linear transformations.

## 12.2 On Functions

Before being precise about the definition of a homomorphism, we need some ideas related to general functions from one set to another. Hopefully, these ideas are somewhat familiar from previous math courses, such as calculus.

If  $R, S$  are two sets, a function  $f$  from  $R$  to  $S$  will be denoted by

$$f : R \rightarrow S.$$

The function  $f$  assigns to each element  $r$  of  $R$  a unique element of  $S$ , called  $f(r)$ . Thus  $R$  is the *domain* of the function  $f$ , and  $S$  is the *codomain*.

The *range* or *image* of  $f : R \rightarrow S$  is the set

$$f(R) = \{s \text{ in } S | s = f(r) \text{ for some } r \text{ in } R\}$$

The range of  $f$  is a subset of the codomain  $S$  of  $f$ . If the range of  $f$  is all of  $S$ , we say that the function  $f$  is *onto*, or more formally, *surjective*.

Examples: the exponential function  $f : \mathbb{R} \rightarrow \mathbb{R}$ , defined by  $f(x) = e^x$  for all  $x$  in the field  $\mathbb{R}$  of real numbers, has codomain  $\mathbb{R}$  and range  $\{y \in \mathbb{R} : y > 0\}$ , so is not surjective. But  $g : \mathbb{R} \rightarrow \mathbb{R}$  by  $g(x) = x^3 - x$  and  $h : \mathbb{R} \rightarrow \mathbb{R}$  by  $h(x) = x^3 + x$  are both surjective.

A function  $f : R \rightarrow S$  is *one-to-one*, or more formally, *injective*, if for all  $r_1 \neq r_2$  in  $R$ , then  $f(r_1) \neq f(r_2)$  in  $S$ .

Examples: the function  $h(x) = x^3 + x$  is one-to-one because its derivative  $h'(x) = 3x^2 + 1 > 0$  for all real numbers  $x$ , so  $h(x)$  is a strictly increasing function of  $x$  for all real  $x$  (that is, if  $x_1 < x_2$ , then  $h(x_1) < h(x_2)$ ) by the Mean Value Theorem from calculus. The same is true for the function  $f(x) = e^x$ . But the function  $g(x) = x^3 - x$  is not one-to-one because  $g(0) = g(1)$ .

A function  $f : R \rightarrow S$  is *bijective* if  $f$  is injective and surjective, that is, one-to-one and onto  $S$ .

Examples: the function  $h : \mathbb{R} \rightarrow \mathbb{R}$  by  $h(x) = x^3 + x$  is bijective, but the function  $g$ ,  $g(x) = x^3 - x$  is not one-to-one, so is not bijective, and the function  $f(x) = e^x$  is not onto, so is not bijective.

We note the following special situation.

**Proposition 12.3** *Let  $f$  be a function from  $S$  to  $T$  where  $S$  and  $T$  are finite sets with the same cardinality. Then  $f$  is one-to-one if and only if  $f$  is onto.*

The proof is left as Exercise 12.1.

## 12.3 Ring Homomorphisms

**Definition** Let  $R, S$  be commutative rings. A function  $f$  from  $R$  to  $S$ , or symbolically,  $f : R \rightarrow S$ , is a *ring homomorphism* if  $f$  satisfies the following properties:

- (i)  $f(r + r') = f(r) + f(r')$  for all  $r, r'$  in  $R$ .
- (ii)  $f(r \cdot r') = f(r) \cdot f(r')$  for all  $r, r'$  in  $R$ .
- (iii)  $f(1) = 1$ .

Here the addition and multiplication of  $f(r)$  and  $f(r')$  are in  $S$ , and in (iii) the 1 inside  $f(1)$  is in  $R$  while the 1 on the right side of the equation is in  $S$ .

**Proposition 12.4** *If  $f$  satisfies the conditions (i)–(iii), then*

- (iv)  $f(0) = 0$ .
- (v)  $f(-r) = -f(r)$  for any  $r$  in  $R$ .

*Proof* In (iv) the left 0 is in  $R$ , and the right 0 is in  $S$ . Then (iv) follows from (i). For given any  $b$  in  $R$ ,

$$f(b) = f(0 + b) = f(0) + f(b);$$

adding  $-f(b)$  to both sides (in  $S$ ) gives

$$0 = f(0) + 0 = f(0).$$

To prove (v), notice that by definition of the negative in  $S$ , we have

$$0 = f(0) = f(r + (-r)) = f(r) + f(-r).$$

Since the negative of any element of  $S$  is unique,  $f(-r) = -f(r)$ .  $\square$

We also have

**Proposition 12.5** *If  $f : R \rightarrow S$  is a ring homomorphism, then  $f(U_R)$  is a subset of  $U_S$ .*

*In words, if  $a$  is a unit (invertible element) of  $R$ , then  $f(a)$  is a unit of  $S$ , and  $f(a)^{-1} = f(a^{-1})$ .*

*Proof* Let  $a$  be a unit of  $R$ . Then  $a \cdot a^{-1} = 1$ . Apply the ring homomorphism  $f$  to both sides of this equation:

$$f(a \cdot a^{-1}) = f(1).$$

By properties (ii) and (iii) above, we have

$$f(a) \cdot f(a^{-1}) = 1.$$

So  $f(a^{-1})$  acts like an inverse to  $f(a)$  in  $S$ . So  $f(a)$  is a unit of  $S$ . Moreover, by uniqueness of the inverse of an element in a commutative ring,  $f(a^{-1}) = f(a)^{-1}$ .  $\square$

**Definition** A homomorphism  $f : R \rightarrow S$  that is both one-to-one and onto is called an *isomorphism*. If there is an isomorphism between  $R$  and  $S$ , we say that  $R$  and  $S$  are isomorphic.

Here are some examples of ring homomorphisms that we have implicitly used throughout the book.

*Example 12.6* For  $m$  a positive integer, let  $f : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  be defined by  $f(a) = a + m\mathbb{Z}$ . Then  $f$  is a ring homomorphism. This is a consequence of the way we defined addition and multiplication in  $\mathbb{Z}/m\mathbb{Z}$ . To see this, recall from Section 5.5 that addition of elements of  $\mathbb{Z}/m\mathbb{Z}$  is by

$$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}.$$

In words, to sum two cosets, add their representatives and construct the coset of the sum of the representatives. Using that  $f(a) = a + m\mathbb{Z}$ , this formula for addition is precisely the formula

$$f(a) + f(b) = f(a + b).$$

Multiplication is shown the same way.

Since  $1 + m\mathbb{Z}$  is the multiplicative identity for  $\mathbb{Z}/m\mathbb{Z}$  and

$$f(1) = 1 + m\mathbb{Z},$$

we see that  $f$  takes the multiplicative identity of  $\mathbb{Z}$  to the multiplicative identity of  $\mathbb{Z}/m\mathbb{Z}$ .

Thus  $f : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  is a ring homomorphism.

Evidently  $f$  is a surjective ring homomorphism, because the coset  $a + m\mathbb{Z} = f(a)$  for every integer  $a$ . But  $f$  is not one-to-one, because  $f(a) = f(b)$  if and only if  $a + m\mathbb{Z} = b + m\mathbb{Z}$ , if and only if  $a \equiv b \pmod{m}$ .

Concerning units, it is true (by Proposition 12.5 that  $f : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  sends units of  $\mathbb{Z}$  to units of  $\mathbb{Z}/m\mathbb{Z}$ , but it is not true that  $f$  maps the units of  $\mathbb{Z}$  onto the units of  $\mathbb{Z}/m\mathbb{Z}$ . Examples are easy to find. The only units of  $\mathbb{Z}$  are 1 and  $-1$ , while if  $p$  is a prime  $> 3$ , then  $\mathbb{Z}/p\mathbb{Z}$  has  $p - 1 > 2$  units. Only two of them can come from  $\mathbb{Z}$ .

*Example 12.7* In Section 5.6 we defined a function  $\mathcal{C} : \mathbb{Z}_m \rightarrow \mathbb{Z}/m\mathbb{Z}$  by

$$\mathcal{C}(r) = r + m\mathbb{Z}$$

for  $r = 0, 1, \dots, m - 1$ . Since  $\mathbb{Z}/m\mathbb{Z}$  has a complete set of representatives consisting of  $0, 1, \dots, m - 1$ ,  $\mathcal{C}$  is one-to-one and onto, so is a bijection. In Section 5.6 we showed that  $\mathcal{C}$  is also a homomorphism. So  $\mathcal{C}$  is an isomorphism of rings.

It is because of the isomorphism  $\mathcal{C}$  that we have freely used  $\mathbb{Z}_m$ , integers modulo  $m$ , instead of  $\mathbb{Z}/m\mathbb{Z}$ , cosets of the ideal  $m\mathbb{Z}$ , throughout the book.

*Example 12.8* Let  $\alpha$  be a complex number, and let  $f_\alpha : \mathbb{Q}[x] \rightarrow \mathbb{C}$  by  $f_\alpha(p(x)) = p(\alpha)$  for any polynomial  $p(x)$  in  $\mathbb{Q}[x]$ . Then  $f_\alpha$  is a ring homomorphism, called the “evaluation at  $\alpha$  homomorphism”.

**The kernel.** A ring homomorphism  $f$  is one-to-one, or injective, if  $f$  is one-to-one as a function: that is, for all  $a, b$  in  $R$ , if  $f(a) = f(b)$ , then  $a = b$ .

Here is a convenient test for deciding if  $f$  is injective:

**Proposition 12.9** A ring homomorphism  $f$  is one-to-one if and only if 0 is the only element  $r$  of  $R$  with  $f(r) = 0$ .

*Proof* If  $r \neq 0$  and  $f(r) = 0$ , then since  $f(0) = 0$ ,  $f$  is not one-to-one. On the other hand, if  $f$  is not one-to-one, then there are two different elements  $a$  and  $b$  of  $R$  so that  $f(a) = f(b)$ . But then  $f(a - b) = f(a) - f(b) = 0$ , and  $a - b$  is not the zero element of  $R$ .  $\square$

**Definition** Let  $f : R \rightarrow S$  be a ring homomorphism. The *kernel* of  $f$ , written  $\ker(f)$ , is the set of elements  $r$  of  $R$  so that  $f(r) = 0$ . Concisely,

$$\ker(f) = \{r \text{ in } R \mid f(r) = 0 \text{ in } S\}.$$

Recall from Chapter 5 that an ideal  $J$  of a commutative ring is a subset of  $R$  that is closed under addition and scalar multiplication: that is,

- if  $a_1, a_2$  are in  $J$ , then  $a_1 + a_2$  is in  $J$ ;
- if  $a$  is in  $J$  and  $r$  is in  $R$ , then  $ra$  is in  $J$ .

**Proposition 12.10** If  $f : R \rightarrow S$  is a ring homomorphism, then  $\ker(f)$  is an ideal of  $R$ .

*Proof* Let  $a_1, a_2$  be in  $\ker(f)$ . Then  $f(a_1) = 0$  and  $f(a_2) = 0$ . Since  $f$  is a homomorphism,

$$f(a_1 + a_2) = f(a_1) + f(a_2) = 0 + 0 = 0;$$

also if  $a$  is in  $\ker(f)$  and  $r$  is any element of  $R$ , then

$$f(ra) = f(r)f(a) = f(r)0 = 0.$$

So the kernel  $\ker(f)$  of  $f$  is a subset of  $R$  that is closed under addition and scalar multiplication, hence is an ideal of  $R$ .  $\square$

The size of the kernel of a homomorphism  $f : R \rightarrow S$  describes how far  $f$  is from being one-to-one. If  $\ker(f) = \{0\}$ , then  $f$  is one-to-one. In general, we have:

**Proposition 12.11** Let  $f : R \rightarrow S$  be a ring homomorphism and let  $s$  be in the range of  $f$ , so that  $s = f(r_0)$  for some  $r_0$  in  $R$ . Then the set

$$\{r \text{ in } R \mid f(r) = s\}$$

of elements of  $R$  mapped by  $f$  to the element  $s$  of  $S$  is the coset  $r_0 + \ker(f)$ . So if  $\ker(f)$  has  $m$  elements, then  $f$  is an  $m$ -to-one function from  $R$  to  $S$ .

*Proof* It is easy to see that if  $f(r_0) = s$ , then

$$\{r \text{ in } R \mid f(r) = s\} \supseteq \{r_0 + t \mid t \text{ in } \ker(f)\} = r_0 + \ker(f).$$

For the other direction, suppose  $f(r) = s = f(r_0)$ . Then  $f(r - r_0) = s - s = 0$ , so  $r - r_0 = t$  with  $t \in \ker(f)$ . So  $r = r_0 + t$  with  $t \in \ker(f)$ . Hence

$$\{r \text{ in } R \mid f(r) = s\} = \{r_0 + t \mid t \text{ in } \ker(f)\}.$$

Thus given an element  $r_0$  of  $R$  so that  $f(r_0) = s$  in  $S$ , then the kernel of  $f$  is in one-to-one correspondence with the set of elements of  $R$  that  $f$  maps to  $s$  in  $S$ . The correspondence sends  $t$  in  $\ker f$  to  $r_0 + t$ .

Thus if  $\ker f$  has  $m$  elements, then  $f$  is an  $m$ -to-one function.  $\square$

The one-to-one correspondence between  $\ker(f)$  and the coset  $r_0 + \ker(f)$  in the proof of Proposition 12.11 is the same as the result in Chapter 10 associated with Lagrange's Theorem, that the number of elements in a subset  $H$  of a group  $G$  is equal to the number of elements in any coset of  $H$  in  $G$ .

## 12.4 Fundamental Homomorphism Theorem

In Proposition 12.11 we showed that if  $f : R \rightarrow S$  is a ring homomorphism and if  $s$  in  $S$  is in the range of  $f$ , so that  $s = f(r_0)$  for some  $r_0$  in  $R$ , then the set of elements  $r$  in  $R$  so that  $f(r) = s$  is the coset  $r_0 + K$  of the kernel  $K$  of  $f$ . We can express this fact formally as:

**Proposition 12.12** *Let  $R, S$  be commutative rings and  $f : R \rightarrow S$  a ring homomorphism with kernel  $K$ . Then  $f$  induces a one-to-one function  $\bar{f}$  from the set  $R/K$  of cosets of the kernel of  $f$  to  $S$ , defined by  $\bar{f}(r + K) = f(r)$ .*

Proposition 12.11 says that for each  $s = f(r_0)$  in the range of the function  $f$ , the set of elements of  $R$  that  $f$  sends to  $s$  is the coset  $r_0 + K$ . So there is a one-to-one correspondence between the cosets of  $K$  in  $R$  and the elements of the range of  $f$ . Proposition 12.12 just reminds us that the set of cosets of  $K$  in  $R$  was given a name,  $R/K$ , in Section 5.6. Proposition 12.12 also gives a name,  $\bar{f}$ , to the one-to-one correspondence from the set of cosets of  $K$  in  $R$  to the range of  $f$  in  $S$ .

Now recall from Section 5.6, Theorem 5.6, that if  $R$  is a commutative ring and  $J$  is an ideal of  $R$ , then the set  $R/J$  of cosets of  $J$  in  $R$  is not just a set, but can be made into a commutative ring with the operations

$$\begin{aligned} (r_1 + J) + (r_2 + J) &= (r_1 + r_2) + J \\ (r_1 + J) \cdot (r_2 + J) &= (r_1 \cdot r_2) + J. \end{aligned}$$

In words, to add (or multiply) cosets, add (or multiply) representatives of the cosets and then take the coset of the result.

We showed that addition and multiplication of cosets was “well-defined”, that is, did not depend on the choice of representatives of the cosets used to define the addition or multiplication. The argument needed that  $J$  is an ideal.

Since  $R/J$  is a commutative ring and  $f : R \rightarrow S$  is a ring homomorphism, Proposition 12.12 can be strengthened to yield a general result in commutative ring theory that we can apply to reprove the Chinese Remainder Theorem (!).

**Theorem 12.13** (Fundamental Homomorphism Theorem) *Let  $R, S$  be commutative rings and let  $f : R \rightarrow S$  be a ring homomorphism. Let  $J = \ker(f) = \{r \text{ in } R : f(r) = 0\}$ . Then the induced one-to-one function  $\bar{f}$  of Proposition 12.12 from  $R/J$  to  $S$ , defined by  $\bar{f}(a + J) = f(a)$ , is a ring homomorphism.*

*Proof* We already showed in Propositions 12.11 and 12.12 that  $\bar{f} : R/J \rightarrow S$ , given by  $\bar{f}(r+J) = f(r)$ , is well defined and a one-to-one function from  $R/J$  to  $S$ . All that remains is to show that  $\bar{f}$  is a homomorphism.

But this is true because  $f$  is a homomorphism. To check addition, for any  $b, c$  in  $R$ ,

$$\begin{aligned}\bar{f}((b+J)+(c+J)) &= \bar{f}((b+c)+J) \\ &= f(b+c) \\ &= f(b)+f(c) \\ &= \bar{f}(b+J)+\bar{f}(c+J).\end{aligned}$$

Multiplication is similar:

$$\begin{aligned}\bar{f}((b+J) \cdot (c+J)) &= \bar{f}((b \cdot c)+J) \\ &= f(b \cdot c) \\ &= f(b) \cdot f(c) \\ &= \bar{f}(b+J) \cdot \bar{f}(c+J).\end{aligned}$$

Finally, the multiplicative identity element of the ring  $R/J$  is the coset  $1+J$ , and  $\bar{f}(1+J) = f(1) = 1$ , the multiplicative identity of  $S$ , because  $f$  is a ring homomorphism.

So  $\bar{f}$  is a ring homomorphism from  $R/J$  to  $S$ , as claimed.  $\square$

We specialize the Fundamental Homomorphism Theorem to the case where  $R = \mathbb{Z}$ . It turns out that for any commutative ring  $S$ , there is exactly one ring homomorphism from  $\mathbb{Z}$  to  $S$ , because a ring homomorphism must send 1 to the multiplicative identity of  $S$ . (See Exercise 12.6).

Let  $S$  be a commutative ring and let  $0_S, 1_S$  be the zero element and the multiplicative identity in  $S$ , respectively. Then for an integer  $n$ , the element  $n \cdot 1_S$  means  $1_S + 1_S + \dots + 1_S$  ( $n$  copies) if  $n > 0$ , it means  $0_S$  if  $n = 0$ , and it means  $(-1_S) + (-1_S) + \dots + (-1_S)$  ( $-n$  copies) if  $n < 0$ .

**Corollary 12.14** *Let  $S$  be a commutative ring and let  $f : \mathbb{Z} \rightarrow S$  be the homomorphism defined by  $f(n) = n \cdot 1_S$  for all  $n$  in  $\mathbb{Z}$ . Then  $f$  is a homomorphism from  $\mathbb{Z}$  to  $S$ . Suppose  $f$  is not one-to-one and  $\ker(f) = m\mathbb{Z}$  for some  $m \neq 0$  in  $\mathbb{Z}$ . Then  $f$  induces a one-to-one homomorphism  $\bar{f}$  from  $\mathbb{Z}/m\mathbb{Z}$  to  $S$ , defined by  $\bar{f}(a+m\mathbb{Z}) = f(a) = a \cdot 1_S$ .*

It is routine to verify that  $f$  is the unique ring homomorphism from  $\mathbb{Z}$  to  $S$ . The rest of the corollary is an immediate application of the Fundamental Homomorphism Theorem.

We'll use Corollary 12.14 to give a proof of the Chinese Remainder Theorem and of the formula for Euler's phi function in Sections 12.6 and 12.7.

## 12.5 Group Homomorphisms

We also need the concept of group homomorphism.

Let  $(G, *)$  and  $(G', *)$  be groups. A group homomorphism  $f : G \rightarrow G'$  is a function that satisfies

$$\begin{aligned}f(g_1 * g_2) &= f(g_1) * f(g_2) \\ f(e_G) &= e_{G'}.\end{aligned}$$

Thus  $f$  respects the group operations and the identities  $e_G$  and  $e_{G'}$  of  $G$  and  $G'$ . We used  $*$  for the group operation on both  $G$  and  $G'$ , but the operation on  $G$  need not be the same as that on  $G'$ .

*Example 12.15* Define  $f : (\mathbb{Z}_6, +) \rightarrow (U_7, \cdot)$  by  $f(r) = (3^r \bmod 7)$ . Then  $f$  is a group homomorphism because, modulo 7,

$$f(r+s) = 3^{r+s} = 3^r \cdot 3^s = f(r) \cdot f(s),$$

and  $f(0) = 3^0 = 1$ .

See also Exercise 12.5.

A ring homomorphism  $f : R \rightarrow S$  is in particular a group homomorphism from the group  $(R, +)$  under addition to the group  $(S, +)$  under addition. That is,  $f$  is a group homomorphism from  $R$  to  $S$  when we just forget the multiplication on  $R$  and  $S$ .

If  $f : G \rightarrow G'$  is a group homomorphism, then  $f$  respects inverses: this means,  $f(g^{-1}) = f(g)^{-1}$ . To see this, we have, for all  $g$  in  $G$ ,

$$e_{G'} = f(e_G) = f(g * g^{-1}) = f(g) * f(g^{-1}).$$

Since the inverse of any element of a group is unique, this equation implies that  $f(g^{-1}) = f(g)^{-1}$ :  $f$  maps the inverse of  $g$  to the inverse of  $f(g)$ .

As with ring homomorphisms, we can define the kernel of a group homomorphism  $f : G \rightarrow G'$  by

$$\ker(f) = \{g \text{ in } G : f(g) = e_{G'}\},$$

and we have

**Proposition 12.16** *A group homomorphism  $f : G \rightarrow G'$  is one-to-one if and only if  $\ker(f)$  contains only  $e_G$ , the identity element of  $G$ .*

*Proof* If  $f$  is one-to-one, then  $\ker(f)$  cannot have any elements other than the identity element  $e_G$  of  $G$ . Assume  $\ker(f) = \{e_G\}$ , and suppose  $f(a) = f(b)$  for  $a, b$  in  $G$ . Then  $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_{G'}$ , so  $ab^{-1}$  is in  $\ker(f)$ . So  $ab^{-1} = e_G$ , so  $a = b$ . Thus  $f$  is one-to-one.  $\square$

We have:

**Proposition 12.17** *The kernel of a group homomorphism:  $f : G \rightarrow G'$  is a subgroup of  $G$ .*

*Proof* We need to show that the product of two elements in the kernel of  $f$  is in the kernel of  $f$ , and the inverse of an element in the kernel of  $f$  is in the kernel of  $f$ . But those facts are almost immediate from the properties of a homomorphism. (See the proof of Proposition 12.16 for an illustration of how to use those properties.)  $\square$

The size of the kernel of a group homomorphism with domain a finite group measures how far the homomorphism is from being one-to-one.

**Proposition 12.18** *Let  $f : G \rightarrow H$  be a group homomorphism with kernel  $K$ . Then for each  $h$  in  $H$ , if  $f(s) = h$  for some  $s$  in  $G$ , then  $\{g \in G : f(g) = h\}$  is the coset  $s * K$ . Hence if  $K$  has  $m$  elements, then the function  $f$  is an  $m$ -to-one function.*

*Proof* Since  $f$  is a group homomorphism, for every element  $k$  in  $K$ ,  $f(s * k) = f(s) * f(k) = f(s)$ , so  $\{g \in G : f(g) = h\}$  contains the coset  $s * K$ . Also, if  $f(s) = f(t) = h$ , then  $f(s^{-1}t) = f(s)^{-1} * f(t) = e'$ , the identity element of  $H$ , and so  $s^{-1} * t$  is in  $K$ , hence  $t = s * (s^{-1} * t)$  is in  $s * K$ . So the set of elements of  $G$  that  $f$  sends to  $f(s)$  in  $H$  is the coset  $s * K$ .

As part of the proof of Lagrange's Theorem, we showed that every coset of  $K$  has the same number of elements as  $K$ . So for each  $h$  in the range of  $f$ , the number of elements in  $G$  that  $f$  sends to  $h$  in  $H$  is the same as the number of elements in the kernel  $K$  of  $f$ .  $\square$

From Proposition 12.5 we know that any ring homomorphism takes units to units. In fact,

**Proposition 12.19** *Let  $f : R \rightarrow S$  be a ring homomorphism. Then  $f$  yields by restriction a group homomorphism from  $U(R)$  to  $U(S)$ .*

We usually call the restriction of  $f$  to  $U(R)$  by  $f$  also. To see that  $f : U(R) \rightarrow U(S)$  is a group homomorphism, we just observe that  $f$  preserves multiplication in  $R$  (property (ii) of ring homomorphisms) and maps the multiplicative identity 1 of  $R$  to the identity of  $S$  (property (iii)). The fact that  $f$  preserves inverses was shown in Proposition 12.5.

If the ring homomorphism  $f : R \rightarrow S$  is one-to-one, then so is the restriction of  $f$  on  $U(R)$ . But we observed earlier that while the ring homomorphism  $f : R \rightarrow S$  may be surjective, the restriction of  $f$  from  $U(R)$  to  $U(S)$  need not be surjective.

Here are three other sets of examples of group homomorphisms.

**The “multiplication by  $r$ ” homomorphism.** For any integer  $r$ , let

$$f_r : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$$

be the function that multiplies by  $r$ :

$$f_r(a) \equiv ra \pmod{m}.$$

Then  $f_r$  is a group homomorphism on the additive group of  $\mathbb{Z}_m$ :

$$\begin{aligned} f_r(a+b) &= r(a+b) = ra + rb = f_r(a) + f_r(b) \pmod{m} \\ f_r(0) &= r \cdot 0 = 0. \end{aligned}$$

The kernel of  $f_r$  is

$$\{a : ra \equiv 0 \pmod{m}\},$$

which as we've seen consists of the set of elements of the form

$$\frac{m}{(m, r)}t$$

for  $t = 1, \dots, (m, r)$ . So  $f$  is one-to-one on  $\mathbb{Z}_m$  if and only if  $r$  is coprime to  $m$ .

Note that  $f_r$  is not a ring homomorphism, because  $f_r$  does not respect multiplication in  $\mathbb{Z}_m$ : if  $r \neq 1$  or 0, then  $r(ab) \not\equiv (ra)(rb) \pmod{m}$ .

**The “raise to the  $r$ -th power” homomorphism.** Here is the analogue of  $f_r$  for multiplicative groups of units.

Let  $g_r : U_m \rightarrow U_m$  be the “take the  $r$ -th power” function:

$$g_r(b) \equiv b^r \pmod{m}$$

for  $b$  coprime to  $m$ . Then  $g_r(bc) = (bc)^r = b^r c^r$  and  $g_r(1) = 1$ , so  $g_r$  is a homomorphism from  $U_m$  to  $U_m$ .

The kernel of  $g_r$  is

$$\ker(g_r) = \{b \in U_m : b^r = 1\}.$$

The kernel of  $g_r$  is the subgroup  $U_m(r)$  of  $r$ -th roots of unity of  $U_m$ .

We illustrate Proposition 12.18.

*Example 12.20* Let  $g_3 : U_{19} \rightarrow U_{19}$ . Then the kernel  $K$  of  $g_3$  is the subgroup of cube roots of 1 in  $U_{19}$ :  $K = \{7, 11, 1\}$ . We find that  $g_3(13) = 12$  in  $U_{19}$ . So the set of solutions of  $x^3 = 12$  are elements in the coset  $13 \cdot K$ , namely,  $13, 13 \cdot 7 = 15$  and  $13 \cdot 11 = 10$ .

**Linear transformations on  $\mathbb{F}_p^n$ .** For  $p$  prime, let  $F = \mathbb{F}_p = \mathbb{Z}_p$ , the field of  $p$  elements. Let  $V$  be the vector space  $\mathbb{F}_p^n$  of column vectors with  $n$  components. Then  $V$  is an abelian group under vector addition. Let  $\mathbf{0}$  be the zero vector.

Let  $\mathbf{H}$  be an  $m \times n$  matrix with entries in  $\mathbb{F}_p$ . Then for  $\mathbf{v}$  in  $V$ ,  $\mathbf{H}\mathbf{v}$  is in  $\mathbb{F}_p^m$ . Multiplication by the matrix  $\mathbf{H}$  defines a linear transformation

$$T_{\mathbf{H}} : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^m$$

by

$$T_{\mathbf{H}}(\mathbf{v}) = \mathbf{H}\mathbf{v}$$

because  $\mathbf{H}\mathbf{0} = \mathbf{0}$  and  $\mathbf{H}(\mathbf{v} + \mathbf{w}) = \mathbf{H}\mathbf{v} + \mathbf{H}\mathbf{w}$  for all  $\mathbf{v}, \mathbf{w}$  in  $\mathbb{F}_p^n$ . Then  $T_{\mathbf{H}}$  is a group homomorphism from the additive group  $\mathbb{F}_p^n$  to the additive group  $\mathbb{F}_p^m$ .

The kernel of  $T_{\mathbf{H}}$  is the set

$$\ker(T_{\mathbf{H}}) = \{\mathbf{v} \text{ in } \mathbb{F}_p^n : T_{\mathbf{H}}(\mathbf{v}) = \mathbf{H}\mathbf{v} = \mathbf{0}\},$$

a subgroup of  $\mathbb{F}_p^n$ . In linear algebra,  $\ker(T_{\mathbf{H}})$  is called the null space of the matrix  $\mathbf{H}$ .

*Example 12.21* Let  $p = 2$ , so the field is  $\mathbb{F}_2 = \{0, 1\}$ , integers modulo 2. Let  $V = \mathbb{F}_2^8$  and let

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

then the null space of  $H$  is

$$\ker(T_{\mathbf{H}}) = \{\mathbf{v} \text{ in } \mathbb{F}_2^8 : \mathbf{H}\mathbf{v} = \bar{0}\} = \mathcal{C},$$

the group of code vectors of the Hamming (8, 4) code of Chapter 7.

We'll revisit all three sets of examples of group homomorphisms in Section 14.1.

## 12.6 The Product of Rings and the Chinese Remainder Theorem

To apply the Homomorphism Theorem to Euler's phi function, we need one more "abstract" idea.

**Products of rings.** Let  $R, S$  be two sets. The product of  $R$  and  $S$ , written  $R \times S$ , is the set of ordered pairs  $(r, s)$  where  $r$  is in  $R$ ,  $s$  in  $S$ .

The notion of ordered pairs should be familiar from analytic geometry: if we pick an origin in the plane and set up a pair of coordinate axes, we can then assign coordinates (ordered pairs of real numbers) to points in the plane. Assigning coordinates gives a one-to-one correspondence between points in the plane and the set  $\mathbb{R} \times \mathbb{R}$  of ordered pairs of real numbers.

Suppose  $R$  and  $S$  are commutative rings. Then the product  $R \times S$  can be made into a commutative ring as follows:

$$\begin{aligned}(r, s) + (r', s') &= (r + r', s + s'), \\ (r, s) \cdot (r', s') &= (rr', ss'), \\ -(r, s) &= (-r, -s).\end{aligned}$$

The operations on  $R \times S$  are defined by using the operations of  $R$  in the left coordinates and the operations of  $S$  in the right coordinates.

The zero element 0 is  $(0, 0)$ ; the multiplicative identity element 1 is  $(1, 1)$ .

If  $R$  and  $S$  are commutative rings, then  $R \times S$  is a commutative ring, as is easily seen. For example, to show commutativity of multiplication, we have, for all  $r, r'$  in  $R$  and  $s, s'$  in  $S$ ,

$$(r, s) \cdot (r', s') = (rr', ss')$$

and

$$(r', s') \cdot (r, s) = (r'r, s's).$$

Since  $R$  and  $S$  are commutative rings,  $rr' = r'r$  and  $s's = ss'$ . So  $(r'r, s's) = (rr', ss')$ .

The other properties of a commutative ring are shown for  $R \times S$  in a similar way.

If  $R$  has  $m$  elements and  $S$  has  $n$  elements, then  $R \times S$  has  $mn$  elements.

*Example 12.22*  $\mathbb{Z}_2 \times \mathbb{Z}_3$  has six elements. Here is the addition table for  $\mathbb{Z}_2 \times \mathbb{Z}_3$ :

+	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)
(0, 0)	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)
(1, 1)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)	(0, 0)
(0, 2)	(0, 2)	(1, 0)	(0, 1)	(1, 2)	(0, 0)	(1, 1)
(1, 0)	(1, 0)	(0, 1)	(1, 2)	(0, 0)	(1, 1)	(0, 2)
(0, 1)	(0, 1)	(1, 2)	(0, 0)	(1, 1)	(0, 2)	(1, 0)
(1, 2)	(1, 2)	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)

From the first row of the addition table you can see that  $(0, 0)$  is the additive identity.

Here is the multiplication table:

.	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(1, 1)	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)
(0, 2)	(0, 0)	(0, 2)	(0, 1)	(0, 0)	(0, 2)	(0, 1)
(1, 0)	(0, 0)	(1, 0)	(0, 0)	(1, 0)	(0, 0)	(1, 0)
(0, 1)	(0, 0)	(0, 1)	(0, 2)	(0, 0)	(0, 1)	(0, 2)
(1, 2)	(0, 0)	(1, 2)	(0, 1)	(1, 0)	(0, 2)	(1, 1)

The element  $(1, 1)$  is the identity element.

We can use the multiplication table to identify the units and the zero divisors of  $\mathbb{Z}_2 \times \mathbb{Z}_3$ . The units are pairs that head rows containing  $(1, 1)$ . The zero divisors are non-zero pairs that head rows that contain  $(0, 0)$  in a column other than the first column. Thus  $(1, 1)$  and  $(1, 2)$  are units, because from the table,  $(1, 1)(1, 1) = (1, 1)$  and  $(1, 2)(1, 2) = (1, 1)$ . The zero divisors are  $(0, 2)$ ,  $(1, 0)$  and  $(0, 1)$ , because  $(0, 2)(1, 0) = (0, 0)$  and  $(0, 1)(1, 0) = (0, 0)$ .

We can find the units and zero divisors of any product of rings:

**Proposition 12.23** (i)  $(a, b)$  is a unit of  $R \times S$  if and only if  $a$  is a unit of  $R$  and  $b$  is a unit of  $S$ .

(ii)  $(a, b)$  in  $R \times S$  is a zero divisor if and only if  $(a, b) \neq (0, 0)$  and  $a$  is zero or a zero divisor of  $R$ , or  $b$  is zero or a zero divisor of  $S$ .

*Proof* Part (i) is easy:  $(a, b)(a', b') = (1, 1)$  if and only if  $aa' = 1$  in  $R$  and  $bb' = 1$  in  $S$ .

For (ii),  $(a, b)$  is a zero divisor in  $R \times S$  if and only if  $(a, b) \neq (0, 0)$  and there is some  $(a', b')$  not zero so that

$$(a, b)(a', b') = (aa', bb') = (0, 0),$$

that is, so that  $aa' = 0$  in  $R$  and  $bb' = 0$  in  $S$ . Proving (ii) is a matter of looking at the various possibilities for  $a$  and  $b$ :  $a = 0$ ,  $a$  a zero divisor, or  $a$  a non-zero divisor, and similarly for  $b$ . The proof is left as Exercise 12.12.  $\square$

**Definition** A ring homomorphism  $f : R \rightarrow S$  is an *isomorphism* if  $f$  is one-to-one and onto. Two rings  $R$  and  $S$  are *isomorphic* if there is an isomorphism between them.

Notation: if the rings  $R$  and  $S$  are isomorphic by some isomorphism that is understood from the context, we write

$$R \cong S,$$

in words,  $R$  is isomorphic to  $S$ .

There is a similar definition of an isomorphism of groups.

**On the Chinese Remainder Theorem.** The Fundamental Homomorphism Theorem, Theorem 12.13, yields the following description of  $\mathbb{Z}_{mn}$  when  $mn$  is a product of two coprime numbers  $m, n$ . Recall that  $[m, n]$  denotes the least common multiple of  $m$  and  $n$ .

**Theorem 12.24** Suppose  $m$  and  $n$  are natural numbers  $\geq 2$ . Then there is a homomorphism of rings

$$\bar{f} : \mathbb{Z}_{[m,n]} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$

given by  $\bar{f}(a \bmod [m, n]) = (a \bmod m, a \bmod n)$ .

If  $m$  and  $n$  are coprime, then  $[m, n] = mn$  and the homomorphism

$$\bar{f} : \mathbb{Z}_{[m,n]} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$

is an isomorphism (a one-to-one and onto homomorphism).

*Example 12.25* Let  $m = 2, n = 3$ . Then the theorem says that the ring  $\mathbb{Z}_6$  is isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_3$ . Here is what  $\bar{f}$  does:

$$\begin{aligned}\bar{f}(0) &= (0, 0), \\ \bar{f}(1) &= (1, 1), \\ \bar{f}(2) &= (2, 2) \\ \bar{f}(3) &= (3, 3) \\ \bar{f}(4) &= (4, 4) \\ \bar{f}(5) &= (5, 5).\end{aligned}$$

Reducing the left components modulo 2 and the right components modulo 3 yields

$$\begin{aligned}\bar{f}(0) &= (0, 0), \\ \bar{f}(1) &= (1, 1), \\ \bar{f}(2) &= (0, 2) \\ \bar{f}(3) &= (1, 0) \\ \bar{f}(4) &= (0, 1) \\ \bar{f}(5) &= (1, 2).\end{aligned}$$

The unit 1 corresponds to the unit  $(1, 1)$  and the unit 5 corresponds to  $(1, 2)$  in  $\mathbb{Z}_2 \times \mathbb{Z}_3$ ; the zero divisors 2, 3, 4 of  $\mathbb{Z}_6$  correspond to the zero divisors  $(0, 2)$ ,  $(1, 0)$  and  $(0, 1)$ , respectively, of  $\mathbb{Z}_2 \times \mathbb{Z}_3$ .

Comparing the addition and multiplication tables for  $\mathbb{Z}_6$  with those for  $\mathbb{Z}_2 \times \mathbb{Z}_3$  in Example 12.22 above, you can see that they are identical except for how we labeled the elements.

The proof of Theorem 12.24 relates to the Chinese Remainder Theorem.

*Proof* Let

$$f : \mathbb{Z} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$

by  $f(a) = ((a \bmod m), (a \bmod n))$ . We show that the kernel of  $f$  is  $[m, n]\mathbb{Z}$ .

If  $a$  is a common multiple of  $m$  and  $n$ , say  $a = rm = sn$  for some integers  $r, s$ , then  $((a \bmod m), (a \bmod n)) = ((rm \bmod m), (sn \bmod n)) = (0, 0)$ , the zero element of  $\mathbb{Z}_m \times \mathbb{Z}_n$ . So  $a$  is in the kernel of  $f$ .

Conversely, let  $f(a) = 0$ . Then

$$((a \bmod m), (a \bmod n)) = (0, 0).$$

So  $m$  divides  $a$  and  $n$  divides  $a$ . So  $a$  is a common multiple of  $m$  and  $n$ . Thus the kernel of  $f$  consists of all common multiples of  $m$  and  $n$ . Since every common multiple of  $m$  and  $n$  is divisible by the least common multiple  $[m, n]$ , we see that  $\ker(f) = [m, n]\mathbb{Z}$ .

By the Fundamental Homomorphism Theorem we get an induced one-to one homomorphism  $\bar{f}$ :

$$\bar{f} : \mathbb{Z}_{[m,n]} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$

by  $\bar{f}(a) = ((a \bmod m), (a \bmod n))$  for  $a$  in  $\mathbb{Z}_{[m,n]}$ .

If  $m$  and  $n$  are not coprime, then  $\bar{f}$  is not onto, because the domain of  $\bar{f}$  has  $[m, n] = mn/(m, n) < mn$  elements, while the codomain of  $\bar{f}$  has  $mn$  elements.

If  $m$  and  $n$  are coprime, we can see that  $\bar{f}$  is onto, hence an isomorphism. For if  $m$  and  $n$  are coprime, then the least common multiple of  $m$  and  $n$  is  $mn$ , and  $mn\mathbb{Z}$  is the kernel of  $f$ . To show that  $\bar{f}$  is then an isomorphism, we only need to show that  $\bar{f}$  is onto. Showing that  $\bar{f}$  is onto relates to the Chinese Remainder Theorem.

First we show that  $\bar{f}$  is onto using the Chinese Remainder Theorem.

Let  $(b, c)$  be an arbitrary element of  $\mathbb{Z}_{[m,n]} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ . To show that  $(b, c) = ((a \bmod m), (a \bmod n)) = \bar{f}(a)$  for some integer  $a$ , we must find an integer  $a$  so that

$$\begin{aligned}a &\equiv b \pmod{m}, \\ a &\equiv c \pmod{n}.\end{aligned}$$

But  $m$  and  $n$  are coprime, so the Chinese Remainder Theorem shows that there is a unique number modulo  $mn$  that solves this pair of simultaneous congruences. Thus  $\bar{f}$  is onto.

But to show that  $\bar{f}$  is onto, without using the Chinese Remainder Theorem, we can just apply Proposition 12.3:  $\bar{f}$  is a one-to-one function from a set with  $mn$  elements, namely,  $\mathbb{Z}_{mn}$ , to another set with  $mn$  elements, namely,  $\mathbb{Z}_m \times \mathbb{Z}_n$ . So  $f$  must be onto.

Since  $e$  is onto when  $m, n$  are coprime, it follows that given any pair  $(b, c)$  in  $\mathbb{Z}_m \times \mathbb{Z}_n$ , there must be some integer  $a$  that solves the pair of congruences

$$\begin{aligned} x &\equiv b \pmod{m}, \\ x &\equiv c \pmod{n}. \end{aligned}$$

So the Chinese Remainder Theorem holds for sets of two congruences to coprime moduli.  $\square$

If  $f : S \rightarrow T$  is a one-to-one, onto function, then there is always an inverse function  $g : T \rightarrow S$  with the property that  $g \circ f : S \rightarrow T \rightarrow S$  is the identity (that is,  $(g \circ f)(s) = g(f(s)) = s$  for all  $s$  in  $S$ ), and  $f \circ g : T \rightarrow S \rightarrow T$  is the identity. Describing the inverse function is not always easy, as we'll see with the discrete logarithm function in Chapter 13. But for the function  $f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$  given by  $f(a) = ((a \bmod m), (a \bmod n))$  for  $a$  in  $\mathbb{Z}_{mn}$  with  $m$  and  $n$  coprime, we can describe the inverse homomorphism:

$$g : \mathbb{Z}_m \times \mathbb{Z}_n \rightarrow \mathbb{Z}_{mn}$$

using the method of solving a pair of congruences in Proposition 2 of Chapter 11. We solve Bezout's identity for  $m$  and  $n$ : find  $r$  and  $s$  with  $rm + sn = 1$ . Call  $sn = e_1$  and  $rm = e_2$ . Then the unique  $x$  modulo  $mn$  that solves

$$\begin{aligned} x &\equiv b \pmod{m} \\ x &\equiv c \pmod{n}, \end{aligned}$$

is  $be_1 + ce_2$ . So

**Proposition 12.26** *If  $f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$  is the homomorphism of Theorem 12.24 and  $m$  and  $n$  are coprime, then the inverse isomorphism  $g$  is defined by*

$$g(b, c) = ((be_1 + ce_2) \bmod mn).$$

where  $e_1, e_2$  come from Bezout's Identity for  $m$  and  $n$  as above.

In particular,  $g(1, 0) = e_1$ , and  $g(0, 1) = e_2$ .

## 12.7 Units and Euler's Formula

Now we proceed to a proof of Euler's formula: if  $(m, n) = 1$ , then  $\phi(mn) = \phi(m)\phi(n)$ .

As we observed with the example of  $\mathbb{Z}_6$  above, units of  $\mathbb{Z}_6$  correspond to the units of  $\mathbb{Z}_2 \times \mathbb{Z}_3$ . This is always the case for  $m$  and  $n$  coprime. We have

**Proposition 12.27** *If  $m$  and  $n$  are coprime, and*

$$\bar{f} : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$

is the isomorphism given by

$$\bar{f}(a) = ((a \bmod m), (a \bmod n)).$$

then  $\bar{f}$  restricts to an isomorphism of groups from  $U_{mn}$  to  $U_m \times U_n$ .

Thus  $U_{mn} \cong U_m \times U_n$  if  $m$  and  $n$  are coprime.

*Proof* Since  $\bar{f}$  is a ring homomorphism,  $\bar{f}$  restricts to a group homomorphism from the units of  $\mathbb{Z}_{mn}$  to the group of units of  $\mathbb{Z}_m \times \mathbb{Z}_n$ . Let  $\psi$  be  $\bar{f}$  restricted to  $U_{mn}$ , the group of units of  $\mathbb{Z}_{mn}$ . Then  $\psi : U_{mn} \rightarrow U_m \times U_n$  is one-to-one because  $\bar{f}$  is one-to-one.

To show that  $\psi$  is onto, let  $(b, c)$  be in  $U_m \times U_n$ . There is some  $a$  in  $\mathbb{Z}_{mn}$  so that

$$\bar{f}(a) = ((a \bmod m), (a \bmod n)) = (b, c).$$

Let  $(b', c')$  be the inverse of  $(b, c)$ : then

$$bb' \equiv 1 \pmod{m}; \quad cc' \equiv 1 \pmod{n}.$$

Since  $\bar{f}$  is one-to-one and onto, there is a unique  $a'$  in  $\mathbb{Z}_{mn}$  so that

$$\bar{f}(a') = (b', c').$$

Then

$$\begin{aligned} \bar{f}(aa') &= (b, c)(b', c') \\ &= ((bb' \bmod m), (cc' \bmod n)) \\ &= (1, 1). \end{aligned}$$

Since  $\bar{f}$  is one-to-one,

$$aa' \equiv 1 \pmod{mn}.$$

So  $a$  is a unit of  $\mathbb{Z}_{mn}$  with inverse  $a'$ . So  $a$  is in  $U_{mn}$ , and  $\bar{f}(a) = \psi(a)$ . So  $\psi : U_{mn} \rightarrow U_m \times U_n$  is surjective, and hence an isomorphism of groups.  $\square$

This theorem yields the formula for Euler's phi function:

**Corollary 12.28** *If  $m$  and  $n$  are coprime, then  $\phi(mn) = \phi(m)\phi(n)$ .*

*Proof*  $\phi(mn)$  is the number of elements of  $U_{mn}$ , and  $\phi(m)\phi(n)$  is the number of elements of  $U_m \times U_n$ . By Proposition 12.27, since  $\psi : U_{mn} \rightarrow U_m \times U_n$  is a bijection, the sizes of the domain and codomain of  $\psi$  are equal.  $\square$

Just as the Chinese Remainder Theorem is valid for  $g > 2$  congruences as long as the moduli are pairwise coprime, Proposition 12.27 extends from a factorization of  $m$  into two coprime factors to a factorization of  $m$  into  $g > 2$  pairwise coprime factors:

**Corollary 12.29** *Let  $m = p_1^{e_1} p_2^{e_2} \cdots p_g^{e_g}$  be a product of prime powers. Then*

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_g^{e_g}} = \prod_{i=1}^g \mathbb{Z}_{p_i^{e_i}},$$

$$U_m \cong U_{p_1^{e_1}} \times \cdots \times U_{p_g^{e_g}} = \prod_{i=1}^g U_{p_i^{e_i}}$$

and

$$\phi(m) = \phi(p_1^{e_1}) \cdot \dots \cdot \phi(p_g^{e_g}) = \prod_{i=1}^g \phi(p_i^{e_i}).$$

The proof of this is a routine induction from Proposition 12.27.

This last result shows that IF we can factor  $m$  into a product of primes, we can find  $\phi(m)$  easily. Fortunately for cryptography, that is a big "IF"!

We conclude this chapter with an observation on roots of unity. Recall that  $U_m(e)$  is the set of  $e$ -th roots of unity in  $U_m$ , that is, the set of units  $a$  so that  $a^e = 1$ :

**Proposition 12.30** *Let  $m = rs$  with  $r, s$  coprime. Then for all numbers  $e \geq 1$ ,*

$$U_m(e) \cong U_r(e) \times U_s(e).$$

*Proof* The isomorphism  $f : U_m \rightarrow U_r \times U_s$  given by

$$f(a) = ((a \bmod r), (a \bmod s))$$

is one-to one and onto, and preserves multiplication. So

$$\begin{aligned} f(a^e \bmod m) &= (f(a)^e \bmod m) \\ &= ((a \bmod r), (a \bmod s))^e \\ &= ((a^e \bmod r), (a^e \bmod s)). \end{aligned}$$

If  $a$  is in  $U_m(e)$ , then the left side = 1. Then, since  $f$  is a group homomorphism, the right side is  $(1, 1)$ . So  $(a \bmod r)$  is in  $U_r(e)$  and  $(a \bmod s)$  is in  $U_s(e)$ . Since  $f$  is one-to-one on  $U_m$ ,  $f$  maps  $U_m(e)$  one-to-one into  $U_r(e) \times U_s(e)$ .

To show that  $f$  restricted to  $U_m(e)$  maps onto  $U_r(e) \times U_s(e)$ , suppose given  $(b, c)$  in  $U_r(e) \times U_s(e)$ . Let  $f(a) = (b, c)$ . Then, since  $f$  is a homomorphism,

$$f(a^e) = f(a)^e = (b, c)^e = (b^e, c^e).$$

If  $(b^e, c^e) = (1, 1)$ , then, since  $f$  is one-to-one, it follows that  $a^e = 1$ . So  $a$  is in  $U_m(e)$  and maps by  $f$  to  $(b, c)$  in  $U_r(e) \times U_s(e)$ . Thus  $f$  is onto. Thus  $f$  restricts to an isomorphism from  $U_m(e)$  onto  $U_r(e) \times U_s(e)$ .  $\square$

Here is an immediate application of Proposition 12.30. Recall that a number  $m$  is a Carmichael number (see Section 9.7) if  $m$  is composite and for all  $a$  coprime to  $m$ ,  $a^{m-1} \equiv 1 \pmod{m}$ .

**Proposition 12.31** *An odd number  $m$  is a Carmichael number if and only if  $p - 1$  divides  $m - 1$  for each prime  $p$  dividing  $m$ .*

*Proof* It is known (see Proposition 14.13) that a Carmichael number  $m$  must be a product of distinct primes:  $m = p_1 p_2 \cdots p_g$ . By definition,  $m$  is a Carmichael number if and only if  $U_m = U_m(m-1)$ , that is, if and only if the  $m - 1$ -st power of every unit mod  $m$  is equal to 1.

Now by Proposition 12.29,

$$(*) \quad U_m \cong U_{p_1} \times U_{p_2} \times \cdots \times U_{p_g},$$

and by an obvious extension of Proposition 12.30,

$$(**) \quad U_m(m-1) = U_{p_1}(m-1) \times U_{p_2}(m-1) \times \cdots \times U_{p_g}(m-1).$$

Suppose  $p$  is a prime divisor of  $m$  and  $p - 1$  divides  $m - 1$ . By Fermat's Theorem, every element of  $U_p$  has order dividing  $p - 1$ . So every element of  $U_p$  has order dividing  $m - 1$ . So  $U_p(m - 1) = U_p$ .

So if  $p_i - 1$  divides  $m - 1$  for  $i = 1, \dots, g$ , then  $U_{p_i}(m - 1) = U_{p_i}$  for all  $i$ . Comparing  $(*)$  and  $(**)$ , we see that  $U_m(m - 1) = U_m$ . Hence  $m$  is Carmichael.

Conversely, suppose  $m$  is Carmichael. Then  $U_m(m - 1) = U_m$ , so comparing  $(*)$  and  $(**)$ , we must have that for all  $i$ ,  $U_{p_i}(m - 1) = U_{p_i}$ .

Let  $p$  be a prime dividing  $m$ . There is a primitive root modulo  $p$ , hence an element  $b$  of  $U_p$  whose order is  $p - 1$ . If  $U_p(m - 1) = U_p$ , then  $b^{m-1} = 1$  in  $U_p$ .

But then, since the order of  $b$  is  $p - 1$ , it follows that  $p - 1$  divides  $m - 1$ .

Since this is true for all primes  $p$  dividing  $m$ , the proof is complete.  $\square$

*Example 12.32* The Carmichael number 561 factors as  $561 = 3 \cdot 11 \cdot 17$ , and  $560 = 2 \cdot 280 = 10 \cdot 56 = 16 \cdot 35$ .

The Carmichael number 1729 factors as  $1729 = 7 \cdot 13 \cdot 19$ , and  $1728 = 6 \cdot 288 = 12 \cdot 144 = 18 \cdot 96$ . (See Exercise 9.14.)

## Exercises

- 12.1. Let  $f : S \rightarrow T$  be a function, where  $S, T$  are both sets with  $n$  elements ( $n$  a finite number). Show
  - (i) if  $f$  is one-to-one, then  $f$  is onto.
  - (ii) if  $f$  is onto, then  $f$  is one-to-one.
- 12.2. For  $\mathbb{Q}$  the field of rational numbers, define a function  $q : \mathbb{Q}[x] \rightarrow \mathbb{Q}[x]$  by  $q(p(x)) = p(x)^2$ . Decide whether or not  $q$  is a ring homomorphism. Explain your answer.
- 12.3. Let  $p$  be a prime and  $\mathbb{F}_p = \mathbb{Z}_p$  be the field of  $p$  elements. Define the function

$$\mathcal{F} : \mathbb{F}_p[x] \rightarrow \mathbb{F}_p[x]$$

by

$$\mathcal{F}(f(x)) = (f(x))^p$$

for  $f(x) = a_n x^n + \dots + a_1 x + a_0$  any polynomial with coefficients in  $\mathbb{F}_p$ . Show that  $\mathcal{F}$  is a ring homomorphism. (To show that  $\mathcal{F}$  gets along with addition, see Proposition 8.29.)

- 12.4. Let  $F$  be a field,  $a$  an element of  $F$ , and define  $\phi_a : F[x] \rightarrow F$  by  $\phi_a(f(x)) = f(a)$ . Show that  $\phi_a$  is a ring homomorphism (called the “evaluation at  $a$ ” map in Example 12.8). Find a criterion for a polynomial in  $F[x]$  to be in the kernel of  $\phi_a$ .
- 12.5. Show that  $x \mapsto e^x$  is a group homomorphism from the group  $(\mathbb{R}, +)$  of real numbers under addition to the group  $(\mathbb{R}_+, *)$  of positive real numbers under multiplication. Show that this exponential homomorphism is an isomorphism with inverse  $y \mapsto \ln(y)$  where  $\ln(y)$  is the natural logarithm of  $y$ .
- 12.6. Show that for every ring  $R$ , the only ring homomorphism from  $\mathbb{Z}$  to  $R$  is the homomorphism  $f$  defined by  $f(n) = n \cdot 1_R$  where  $n$  is in  $\mathbb{Z}$  and  $1_R$  is the multiplicative identity of  $R$ .
- 12.7. Let  $R$  be a commutative ring containing a finite number of elements, and let  $f : \mathbb{Z} \rightarrow R$  by  $f(n) = n \cdot 1_R$ , where  $1_R$  is the multiplicative identity of  $R$ .
  - (i) Show that  $f$  cannot be one-to-one, so  $\ker(f) = m\mathbb{Z}$  for some number  $m$ .

- (ii) Suppose the kernel of  $f$  is  $m\mathbb{Z}$  and  $m$  factors as  $m = rs$  for  $r, s < m$ . Show that  $f(r)$  and  $f(s)$  are complementary zero divisors in  $R$ .
- (iii) Suppose  $R$  is a field. Show that the kernel of  $f$  is the ideal  $p\mathbb{Z}$  for some prime  $p$ . (The prime number  $p$  is called the *characteristic* of the field  $R$ .)
- 12.8. Let  $(e, m) = 1$ . Show that  $g : U_m \rightarrow U_m$ , defined by  $g(a) = ea$ , is a one-to-one function, and hence a bijection. Show also that for  $2 \leq e < m$ ,  $g$  is not a homomorphism.
- 12.9. Let  $b \not\equiv 0 \pmod{m}$ . Let  $g : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$  be defined by  $g(a \pmod{m}) = (a + b) \pmod{m}$  for all integers  $a$ . Show that  $g$  is a one-to-one function, but is neither a ring homomorphism nor a group homomorphism from the additive group of  $\mathbb{Z}_m$  to itself.
- 12.10. Write down the elements of  $\mathbb{Z}_{10}$  and of  $\mathbb{Z}_2 \times \mathbb{Z}_5$ , and identify which elements correspond under the map  $\bar{f}$  from  $\mathbb{Z}_{10}$  to  $\mathbb{Z}_2 \times \mathbb{Z}_5$ . Identify the elements that are units, and those that are zero divisors.
- 12.11. Let  $\bar{f} : \mathbb{Z}_8 \rightarrow \mathbb{Z}_4 \times \mathbb{Z}_2$  by  $\bar{f}(a \pmod{8}) = (a \pmod{4}, a \pmod{2})$ . List what  $f(a \pmod{8})$  is for  $a = 0, 1, \dots, 7$ . Which elements of  $\mathbb{Z}_8$  are in the kernel of  $f$ ? Which elements of  $\mathbb{Z}_4 \times \mathbb{Z}_2$  are in the image of  $f$ ?
- 12.12. Prove part (ii) of Proposition 12.23.
- 12.13. Let  $p, q$  be distinct odd primes and  $m = pq$ . Using that  $U_m \cong U_p \times U_q$  (from Proposition 12.27), show that if  $\lambda = [p - 1, q - 1]$ , then for every element  $a$  of  $U_m$ ,  $a^\lambda = 1$ .
- 12.14. Suppose  $m = rs$  with  $(r, s) = 1$ . Then  $U_m \cong U_r \times U_s$  by Proposition 12.27. Show that if there is an element  $a$  of  $U_r$  of order  $f$ , and an element  $b$  of  $U_s$  of order  $g$ , then there is an element of  $U_m$  of order  $[f, g]$ .
- 12.15. Show that  $U_m(e) = U_m(d)$  where  $d = (e, \phi(m))$ . (Hint: recall Bezout's Identity.)
- 12.16. Show that  $g_r : U_m \rightarrow U_m$  given by  $g_r(a) = a^r$  is a one-to-one function if and only if  $r$  and  $\phi(m)$  are coprime.
- 12.17. For every  $m > 1$ , list the elements of  $U_m(1)$ .
- 12.18. Show that if  $p$  is an odd prime, then the polynomial  $x^2 - 1$  has exactly two roots in  $\mathbb{F}_p$ . Hence, for  $p$  an odd prime,  $U_p(2)$  has exactly two elements. (Hint: recall D'Alembert's Theorem from Chapter 6).
- 12.19. Let  $m = pq$  with  $p, q$  distinct odd primes. Using Proposition 12.30 show that if  $p, q$  are prime and  $m = pq$ , then  $U_m(2)$  has exactly four elements.
- 12.20. Let  $p_1, p_2, \dots, p_g$  be distinct odd primes, and let  $m = p_1 \cdot p_2 \cdots p_g$ .
- (i) Using Proposition 12.30, show that

$$U_m(2) \cong U_{p_1}(2) \times \cdots \times U_{p_g}(2).$$

- (ii) Using Exercise 12.18 above, show that  $U_m(2)$  has order  $2^g$ . Hence  $x^2 - 1$  has  $2^g$  roots in  $\mathbb{Z}/m\mathbb{Z}$ .

A pair of twin primes is a pair  $(q, p)$  of prime numbers where  $p = q + 2$ . Examples:  $(3, 5)$ ,  $(71, 73)$ ,  $(659, 661)$ ,  $(4517, 4519)$ ,  $(10037, 10039)$ ,  $(3756801695685 \cdot 2^{666669} - 1, 3756801695685 \cdot 2^{666669} + 1)$  [Search on “twin primes”]. (The problem of showing that there are infinitely many pairs of twin primes has been worked on for centuries but is still unsolved. There was a famous breakthrough on the problem by Yitang Zhang, who proved in 2013 that there is a fixed finite number  $d$  so that there are infinitely many prime pairs  $(p, q)$  where  $|p - q| \leq d$ . The twin prime conjecture is that one can choose  $d = 2$ . Zhang's result had  $d = 70,000,000$ . The best  $d$  as of 2015 is  $d = 246$ . Zhang was awarded a MacArthur Fellowship in 2014.)

- 12.21. Let  $m = pq$  where  $p$  and  $q$  are twin primes. Show that  $U_m(m - 1) = U_m(2)$ , so by Exercise 12.19 has order 4. Find the four elements of  $U_m(m - 1)$ .

If  $m$  is prime, then  $U_m(m - 1) = U_m$  by Fermat's Theorem. If  $m$  is composite then the elements of  $U_m(m - 1)$  are represented by the numbers  $a$  so that  $m$  is an  $a$ -pseudoprime.

- 12.22. Suppose you are searching for a large prime by using  $a$ -pseudoprime tests, and you test a number  $m$  which happens to be a product of a pair of twin primes. How likely is it that an  $a$ -pseudoprime test of  $m$  for a randomly chosen test number  $a$  will show that  $m$  is composite?
- 12.23. (i) Suppose  $p$  is a safeprime (which means  $p$  is prime and  $p = 2q + 1$  where  $q$  is also prime). Find  $(\phi(pq), pq - 1)$ .  
(ii) Suppose you are searching for a large prime by using  $a$ -pseudoprime tests, and you test a number  $m$  which happens to be a product  $pq$  where  $p = 2q + 1$  is a safeprime. How likely is it that an  $a$ -pseudoprime test of  $m$  for a randomly chosen test number  $a$  will show that  $m$  is composite? (Determine the size of  $U_m(m - 1)$  using Exercise 12.15.)
- 12.24. Show that  $U_{77}(2)$  is not a cyclic group, but that  $U_{77}(15)$  is cyclic: find a generator of  $U_{77}(15)$ .

# Chapter 13

## Cyclic Groups and Cryptography



In this chapter we review cyclic groups and then use them for discrete logarithm cryptography. In particular, we discuss the Diffie–Hellman key exchange cryptosystem, a system used widely on the internet. As with RSA, the security of Diffie–Hellman key exchange depends on the difficulty of reversing an easy computation.

For RSA, the easy computation is that of taking two prime numbers  $p$  and  $q$  and multiplying them together to get a modulus  $m$ , while the hard problem is: given  $m$  which is known to be a product of two prime numbers, find the prime factors  $p$  and  $q$  of  $m$ . Multiplying is easy, factoring is not.

For Diffie–Hellman, the easy computation is to take a number  $g$  in  $U_p$ , the group of units modulo  $p$ , and find  $b = g^e \bmod p$ . The hard computation is: given  $g$  and  $b$ , find the number  $e$  so that  $b = g^e$ . This is called the discrete logarithm problem. Finding powers of a number modulo  $p$  is easy, by the XS-binary algorithm. Finding the discrete logarithm  $e = \log_g(b)$  is not easy.

Diffie–Hellman cryptography can be done using any cyclic group, but the original implementation, and one that is still used on the internet, uses the group  $U_p$  of units modulo a large prime  $p$ . It is a fact that for every prime  $p$ , the group  $U_p$  is a cyclic group. In this chapter we will prove that result, called the Primitive Root Theorem. Thus by choosing a large prime number  $p$ , we can find a cyclic group  $U_p$  of large order for use in cryptography.

To prove the Primitive Root Theorem, we introduce the exponent of a finite abelian group  $G$ , which is the largest number that is the order of some element of  $G$ . Using the decomposition of the group  $U_m$  of units obtained at the end of Chapter 11, we can determine the exponent of  $U_m$  for every odd number.

One way to crack a Diffie–Hellman cryptosystem using a cyclic group  $G = \langle g \rangle$  is to find a way to find the discrete logarithm  $\log_g(b)$  of  $b$  in  $G$ , where  $\log_g(b) = e$  if  $g^e = b$ . The naive method would be to find discrete logarithms by writing down a log table, a list of all of the powers of  $g$  modulo  $p$ : “trial exponentiation”. In the last sections of this chapter we describe two algorithms that are faster than trial exponentiation. One is the Pohlig–Hellman algorithm, which uses the Chinese Remainder Theorem to replace the discrete logarithm problem in  $U_p$  by a collection of discrete logarithm problems in subgroups of  $U_p$  of prime power order when  $p - 1$  is divisible only by small primes. The other is the Baby Step–Giant Step algorithm. But neither algorithm is very fast. That’s why Diffie–Hellman key exchange is so widely used.

### 13.1 Cyclic Groups

Let  $(G, *)$  (with identity  $e$ ) be a finite group. Recall that a subgroup of a finite group  $G$  is a subset  $H$  that is closed under the operation  $*$ . (We showed in Section 10.2 that if  $G$  is finite, a subset closed under  $*$  will also be closed under inverses and will contain the identity of  $G$ .) For  $a$  in  $G$ , we’ll use

exponential notation,

$$a^n = a * a * \dots * a \text{ (n factors).}$$

Thus  $a^0 = e$  = the identity of  $G$ , and  $a^1 = a$ ,  $a^2 = a * a$ ,  $a^3 = a * a * a$ , etc.

A subgroup  $H$  of a finite group  $G$  is cyclic if there is an element  $a$  of  $H$  so that every element  $b$  of  $H$  can be written as  $b = a^r$  for some  $r > 0$ . If so, then  $a$  is a generator of  $H$ , and we write  $H = \langle a \rangle$ .

For  $G$  a finite group, each element  $b$  of  $G$  generates a cyclic subgroup of  $G$ :  $\langle b \rangle = \{b, b^2, b^3, \dots\}$ .

If  $G = \langle a \rangle$  for some  $a$  in  $G$ , then  $G$  is a cyclic group: we call  $G$  the cyclic group generated by  $a$ .

*Example 13.1* In  $U_{14}$ , the group of units of  $\mathbb{Z}_{14}$ , we list the cyclic subgroups generated by each of the elements of  $U_{14}$  (mod 14):

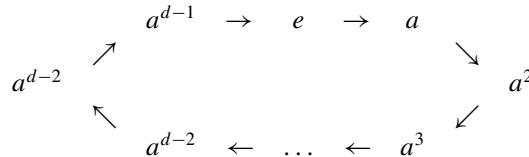
$$\begin{aligned}\langle 1 \rangle &= \{1\} \\ \langle 3 \rangle &= \{3, 9, 13, 11, 5, 1\} \\ \langle 5 \rangle &= \{5, 11, 13, 9, 3, 1\} \\ \langle 9 \rangle &= \{9, 11, 1\} \\ \langle 11 \rangle &= \{11, 9, 1\} \\ \langle 13 \rangle &= \{13, 1\}.\end{aligned}$$

Thus  $U_{14}$  has four cyclic subgroups,  $\langle 1 \rangle$ ,  $\langle 13 \rangle$ ,  $\langle 9 \rangle = \langle 11 \rangle$ , and  $\langle 3 \rangle = \langle 5 \rangle = U_{14}$ . In particular,  $U_{14}$  itself is a cyclic group, generated by 3 or 5.

The word “cyclic” comes from the idea that if  $a$  has order  $d$ , then  $a^d = e$ , so

$$\langle a \rangle = \{e, a, a^2, a^3, \dots, a^{d-1}\},$$

and the powers of  $a$  repeatedly cycle through the elements of  $\langle a \rangle$  as follows:



where each arrow denotes “multiply by  $a$ ”.

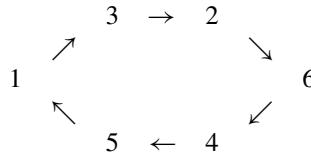
Some more examples of cyclic groups:

*Example 13.2* Let  $G = \mathbb{Z}_m$  for  $m \geq 2$ , a group under addition modulo  $m$ . Then  $G$  has identity element 0, and the elements of  $G$  are  $0, 1, 2, \dots, m-1$  modulo  $m$ . Then  $G$  is a cyclic group: in fact,  $G = \langle 1 \rangle$ , because for every  $k > 1$ ,  $k = 1 + 1 + \dots + 1$  ( $k$  summands). In particular,  $0 = 1 + 1 + \dots + 1$  ( $m$  summands).

*Example 13.3* Let  $G = U_7$ , a group under multiplication. Then

$$U_7 = \{1, 2, 3, 4, 5, 6\} = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} = \langle 3 \rangle$$

since  $3, 3^2, 3^3, 3^4, 3^5, 3^6 \equiv 3, 2, 6, 4, 5, 1 \pmod{7}$ , respectively. So  $U_7$  is a cyclic group. Letting  $\rightarrow$  denote “multiplication by 3 modulo 7”, the cycle picture looks like



*Example 13.4* Let  $q$  be a large prime number, and suppose that  $2q + 1$  is also a prime number. Then  $q$  is called a Sophie Germain prime (after the pioneering early 19th century French mathematician) and  $p$  is called a safeprime (for reasons related to factoring). It is not known, but is conjectured, that there are infinitely many safeprimes. Some examples:  $(q, p) = (2, 5), (11, 23), (23, 47), (41, 83), (5003, 10007)$ . The largest known Sophie Germain prime contains over 200,000 digits. (For the latest records on large primes, see [Ca16].)

Let  $g$  be a unit modulo  $p$ . Then  $g^{p-1} \equiv 1 \pmod{p}$  (Fermat's Theorem), so the order of  $g$  modulo  $p$  divides  $p - 1 = 2q$ . If  $g \not\equiv 1$  or  $-1 \pmod{p}$ , then the order of  $g$ , and hence the order (= the number of elements) of the subgroup  $\langle g \rangle$  is either  $q$  or  $2q = p - 1$ . For cryptographic applications, such large-order cyclic groups are particularly desirable.

For example, inside  $U_{10007}$ , the cyclic group generated by 2 has order either 5003 or 10006.

Later in this chapter we'll prove that for every prime  $p$ ,  $U_p$  is a cyclic group. But first, we look at a discrete analogue of the logarithm function for a cyclic group that is important for cryptography.

## 13.2 The Discrete Logarithm

**Definition** Let  $(G, *)$  be a cyclic group of order  $n$  with generator  $g$ . Every element  $b$  of  $G$  may be written as

$$b = g^r = g * g * \dots * g \quad (r \text{ factors})$$

for some integer  $r$  with  $0 \leq r < n$ . If  $b = g^r$ , then the number  $r$  is called the *logarithm of  $b$  to the base  $g$* , written

$$r = \log_g(b).$$

We'll write  $r = \log(b)$ , omitting the generator  $g$ , if the generator  $g$  is understood from the context.

When  $g$  is a generator of a finite cyclic group, the logarithm to the base  $g$  is called a *discrete logarithm*, to contrast it with the continuous real-valued functions  $\ln(x)$  or  $\log_{10}(x)$ , defined for all real  $x > 0$  in calculus.

Instead of thinking of  $\log_g$  as a function from  $G$  to  $\{1, \dots, n\}$ , we may think of it as a function from  $G$  to  $\mathbb{Z}_n$  where  $n$  is the order of  $G$ . This is because if  $b$  in  $G$  and  $b = g^r$ , then also  $b = g^{r+kn}$  for every  $k$  in  $\mathbb{Z}$ . In the same way, if we let  $\exp_g : \mathbb{Z} \rightarrow G$  by  $\exp_g(r) = g^r$ , then  $\exp_g$  can be thought of as a function from  $\mathbb{Z}_n$  to  $G$  since two integers that are congruent modulo  $n$  are sent by  $\exp_g$  to the same element of  $G$ . Then  $\exp_g$  is a bijection from  $\mathbb{Z}_n$  to  $G$ , and  $\log_g$  is the inverse function of  $\exp_g$ .

In fact, both  $\exp_g$  and  $\log_g$  are group homomorphisms (Section 12.5): both functions respect the group operations on  $(\mathbb{Z}_n, +)$  and  $(G, *)$ . For  $\exp_g$ :

$$\exp_g(r+s) = g^{r+s} = g^r * g^s = \exp_g(r) * \exp_g(s);$$

For  $\log_g$ : if  $a = g^r, b = g^s$ , then

$$\log_g(a * b) = \log_g(g^r * g^s) = \log_g(g^{r+s}) = r + s = \log_g(a) + \log_g(b).$$

So they are inverse isomorphisms of groups.

This last formula for  $\log_g$  is the analogue of the formula for the classical logarithm, invented by Napier and Briggs for computational purposes. The useful property of the base 10 logarithm of Briggs (1624) was that  $\log(ab) = \log(a) + \log(b)$ . This property enables users to transform multiplications of many-digit numbers into addition by using logarithm tables. To multiply  $a$  and  $b$ , they would look up  $\log(a)$  and  $\log(b)$ , add the logarithms, and then look up the number  $c$  with

$$\log(c) = \log(a) + \log(b).$$

Addition is much faster to perform than multiplication, especially by humans. So logarithms were widely used for computations until electronic calculating machines became available in the 1940s.

Just as with real numbers, we can use the formula

$$\log_g(ab) \equiv \log_g(a) + \log_g(b) \pmod{n},$$

and a table of discrete logarithms to aid in computing in a cyclic subgroup  $\langle g \rangle$  of the group  $U_m$  of units modulo  $m$ .

*Example 13.5* Let  $G = U_{11}$ . Then  $U_{11}$  is a cyclic group generated by 2 (modulo 11). Since  $U_{11}$  has ten elements,  $\log_2$  is a homomorphism from  $U_{11}$  to  $\mathbb{Z}_{10}$ , with inverse that takes  $a$  modulo 10 to  $2^a \pmod{11}$ . Here is a logarithm table for  $U_{11}$ :

$a = 2^b = \exp_2(b)$	$b = \log_2(a)$
1	10
2	1
3	8
4	2
5	4
6	9
7	7
8	3
9	6
10	5

For an illustration of how the table could be used, let

$$p(x) = x^8 + 5x^6 + 8x^4 + x^3 + 10x^2 + 2,$$

and suppose we want to find  $p(6)$  modulo 11. We may use the discrete logarithm table for  $U_{11}$  to write everything as powers of 2 and then use Fermat's Theorem to reduce exponents. In this way we avoid dealing directly with  $6^8$  and similar powers. Thus, modulo 11, working from left to right, and noting that  $2^{10} \equiv 1 \pmod{11}$ , we get

$$\begin{aligned}
p(6) &\equiv 6^8 &= (2^9)^8 = 2^{72} &\equiv 2^2 = 4 \\
&+ 5 \cdot 6^6 &\equiv 2^4 \cdot (2^9)^6 = 2^{58} &\equiv 2^8 = 3 \\
&+ 8 \cdot 6^4 &\equiv 2^3 \cdot (2^9)^4 = 2^{39} &\equiv 2^9 = 6 \\
&+ 6^3 &\equiv (2^9)^3 = 2^{27} &\equiv 2^7 = 7 \\
&+ 10 \cdot 6^2 &\equiv (2^5)(2^9)^2 = 2^{23} &\equiv 2^3 = 8 \\
&+ 2 &&= 2.
\end{aligned}$$

Adding the first and last columns, we find:

$$p(6) \equiv 4 + 3 + 6 + 7 + 8 + 2 = 30 \equiv 8 \pmod{11}.$$

But while discrete logarithms can be helpful for computing in cyclic groups of units modulo  $p$  for small primes  $p$ , they are difficult to compute in large cyclic groups, where log tables are impractical. And that is why they are interesting in cryptography.

Suppose  $G = \langle g \rangle$ , a subgroup of  $U_m$  for some  $m$ . If we want to find  $a = g^m$  for some  $m$ , we can use the XS binary algorithm from Section 8.5.

But suppose we are given the generator  $g$  and the element  $a$  of  $G$ . How do we find  $m = \log_g(a)$ ? That is, how do we find the exponent  $m$  so that  $g^m = a$ ? That turns out to be much harder. The algorithms available are slow.

The problem is analogous to the problem of taking two prime numbers  $p$  and  $q$  and multiplying them to obtain their product  $m$  (a task we can do by the usual multiplication algorithm), compared to the problem: take a number  $m$  known to be the product of two primes, and find the two primes—that is, factor  $m$  when we don't know  $p$  and  $q$ . For multiplying, we have a fast algorithm. For factoring, we don't.

*Example 13.6* Let  $G = U_{10007}$ . As noted earlier in this section, 10007 is a safeprime. It turns out that 5 has order 10006 modulo 10007. Let us compare the problem of finding  $5^{6583} \pmod{10007}$  with that of finding a number  $b$  so that  $5^b \equiv 3876 \pmod{10007}$ .

Here is the X-S algorithm to find  $5^{6583} \pmod{10007}$ . (In each row, the element in the third column is the element in the second column modulo 10007; the element in the second column is either the square of the third element in the previous row or the third element in the previous row multiplied by 5, depending on whether the first element in the row is even or odd.) The algorithm shows that  $5^{6583} \equiv 6250 \pmod{10007}$ :

1	5	5
2	25	25
3	125	125
6	15625	5618
12	31561924	9853
24	97081609	3702
25	18510	8503
50	72301009	434
51	2170	2170
102	4708900	5610
204	31472100	85
205	425	425
410	180625	499
411	2495	2495
822	6225025	671
1644	450241	9933
1645	49665	9637
3290	92871769	6809
3291	34045	4024
6582	16192576	1250
6583	6250	6250

This was done by 66 computations, working from the bottom of the first column upward to break down the exponent 6583, then working down from the top of the second and third columns.

By contrast, suppose you wish to find  $b$  so that

$$5^b \equiv 3876 \pmod{10007}.$$

It turns out that  $b = 8849$ . If you do it by trial and error, starting with  $b = 1$  and computing  $5, 5^2, 5^3, \dots$ , you would do about 8848 computations. We'll look at a faster algorithm in the last section of this chapter, but for a modulus of 100 digits or more, no method is anywhere nearly as fast as the XS algorithm, just as no general method for factoring is anywhere nearly as fast as multiplying.

Trying to find  $b$  so that  $5^b \equiv 3876 \pmod{10007}$  is an example of the following:

*The Discrete Logarithm Problem.* Let  $G$  be a finite cyclic group with generator  $g$ . Given an element  $a$  in  $G$ , then  $a = g^x$  for some number  $x$ . Find  $x = \log_g(a)$ .

Seeking efficient ways to determine  $\log_g(a)$  has been an intense area of research ever since Diffie and Hellman (1976) introduced public key cryptography with a cryptosystem whose security depended on the difficulty of the discrete logarithm problem. We present their scheme now.

### 13.3 Diffie–Hellman Key Exchange

Alice and Bob are far apart. They want to communicate with each other privately. But Eve can intercept everything sent between Alice and Bob. So Alice and Bob need to encrypt messages so that Eve cannot read them.

Alice and Bob have set up a private key cryptosystem to communicate with each other. But they need to share a new private key that Eve cannot determine.

Diffie and Hellman introduced a method by which Alice and Bob can agree on a common private key. In order for Eve to learn the key, Eve would apparently have to solve a discrete logarithm problem.

The method works as follows.

Alice and Bob agree on a finite cyclic group  $G$  of large order  $n$ , and a generator  $g$  of  $G$ . Their shared key will be an element of  $G$ . They assume Eve will know  $G, n$  and  $g$ .

Alice chooses a secret random number  $a$  between 0 and  $n$ , computes  $g^a = A$  in  $G$  and sends the resulting group element  $A$  to Bob.

Bob chooses a secret random number  $b$  between 0 and  $n$ , computes  $g^b = B$  in  $G$  and sends the resulting group element  $B$  to Alice.

Alice and Bob's shared private key is then the element  $K = g^{ab}$  in  $G$ .

Alice can compute  $K$  by computing  $B^a = (g^b)^a = g^{ab}$ , which she can do because she chose  $a$  and she received  $B$  from Bob. Bob can compute  $K$  by computing  $A^b = (g^a)^b = g^{ab}$ , which he can do because he chose  $b$  and he received  $A$  from Alice.

*Example 13.7* Let  $G = \langle 2 \rangle = U_{29}$ .

Alice chooses  $a = 8$  and sends  $A = 2^8 = 24$  to Bob.

Bob chooses  $b = 19$  and sends  $B = 2^{19} = 26$  to Alice.

Bob computes (in  $U_{29}$ )

$$\begin{aligned} 24^{19} &= (-5)^{19} = (-5) \cdot 25^9 = (-5)(-4)^9 \\ &= 5 \cdot 2^{18} = 5(-1)16 = -80 = 7. \end{aligned}$$

Alice computes

$$26^8 = (-3)^8 = 81^2 = (-6)^2 = 36 = 7.$$

So Alice and Bob's common private key is  $K = 7$ .

*Example 13.8* Let  $G = U_{10007} = \langle 5 \rangle$ . Alice and Bob know  $p = 10007$  and the generator  $5$  (modulo  $10007$ ). Alice chooses, at random,  $a = 3876$ , computes  $A = 5^{3876} = 8849$  and sends  $A$  to Bob. Bob chooses, at random,  $b = 1651$ , computes  $B = 5^{1651} = 2796$  and sends  $B$  to Alice. Alice computes

$$B^a = 2796^{3876} \equiv 1889 \pmod{10007};$$

Bob computes

$$A^b = 8849^{1651} \equiv 1889 \pmod{10007}.$$

The common secret key is  $K = 1889$ . Alice and Bob both obtain the key because

$$K = A^b = (5^a)^b = (5^b)^a = B^a.$$

Suppose that Eve can see the communications between Alice and Bob. Then Eve knows  $G$ ,  $g$ ,  $A$  and  $B$ . She wants to learn the key  $K$  so she can decrypt the encrypted messages between Alice and Bob. Since  $K = A^b = B^a = g^{ab}$ , she can determine  $K$  if she can learn  $a$ , or  $b$ , or  $ab$ .

To continue with Example 13.8 above:

Eve knows  $G = U_{10007}$ ,  $g = 5$ ,  $A = 8849$ ,  $B = 2796$ . If she can determine that

$$a = \log_5(8849) = 3876,$$

then she can compute  $B^a = 2796^{3876} = 1889 = K$ . Or, if she can determine that

$$b = \log_5(2796) = 1651,$$

then she can compute  $A^b = 8849^{1651} = 1889 = K$ .

Finding the discrete logarithms  $a$  or  $b$  for the group  $U_{10007}$  would be feasible for Eve if she knows the Baby Step-Giant Step algorithm to be presented in the last section of this chapter. But it would be different if the modulus were much larger.

Eve's problem is known as the *Diffie–Hellman problem*: Given a group  $G$ , an element  $g$  in  $G$ , and elements  $A$  and  $B$  in  $\langle g \rangle$  where  $A = g^a$  for some unknown number  $a$  and  $B = g^b$  for some unknown number  $b$ , determine  $K = g^{ab}$  in  $G$ .

Evidently, one way to find  $K$  is to solve the discrete logarithm problem: find  $a = \log_g(A)$  or  $b = \log_g(B)$ .

It is apparently unknown whether it is possible to compute  $K$  by some method that does not require solving the discrete logarithm problem. It is generally believed that the problem, given  $G$ ,  $g$ ,  $A$  and  $B$ , find  $K$ , is of the same order of difficulty as the discrete logarithm problem.

For a video description of the Diffie–Hellman key exchange by Dan Boneh, a leading expert in the field, see [Bo12].

## 13.4 ElGamal Cryptography

The Diffie–Hellman key exchange is effective for creating a shared secret key between Alice and Bob when they are using a symmetric cryptosystem, such as a Vigenère cipher or a modern system such as AES. But suitably modified, it can also be used to send messages. In that form it is called the ElGamal cryptosystem.

Alice wants to send Bob a message, consisting of a particular element of a cyclic group  $G = \langle g \rangle$  of large order  $n$ . (Alice and Bob agreed in advance on how to convert text messages into elements of the group  $G$ .)

To initiate the message process, Bob picks a random number  $b$  with  $1 < b < n$ . He computes  $g^b = B$  and sends Alice  $(g, B)$ .

Alice wants to send Bob the message  $M$ , an element of  $G$ . So Alice picks a random number  $a$  with  $1 < a < n$ , computes  $g^a = A$ , and also computes  $B^a = K$ , the secret key that she is sharing with Bob. She computes  $MK = C$  in  $G$  and sends Bob the pair  $(C, A)$ .

Bob first uses his secret random number  $b$  to compute  $A^b = (g^a)^b = g^{ab} = (g^b)^a = B^a = K$ , the shared secret key. Then he computes  $A^{n-b} = K^{-1}$ , the inverse of the key  $K$ . (Note that  $A^{n-b}K = A^{n-b}A^b = A^n = 1$ , hence  $A^{n-b}$  is the inverse of  $K$  in  $G$ .) Finally he finds  $M$  by computing  $CK^{-1} = MKK^{-1} = M$ .

Eve would need the secret key  $K$  to decrypt the encrypted message  $C = MK$ .

*Example 13.9* Let  $G = \langle 2 \rangle = U_{83}$ , the group of units of  $\mathbb{Z}_{83}$ . (It is not hard to check that 2 has order  $n = 82$  modulo 83.) Suppose Bob's secret random number is  $b = 22$ . Bob sends Alice  $B = 2^{22} \pmod{83} = 65$ . Suppose Alice picks her secret random number to be  $a = 13$ . Alice computes  $A = g^a = 2^{13} \pmod{83} = 58$ , and computes  $K = B^a = 65^{13} \pmod{83} = 41$ . Suppose Alice wants to send Bob the message  $M = 10$ . She computes  $C = KM = 41 \cdot 10 = 78 \pmod{83}$  and sends Bob the pair  $(A, C) = (58, 78)$ . Bob computes  $A^b = 58^{22} \pmod{83} = 41 = K$ , finds that  $K^{-1} = 81$ , then multiplies the encrypted message  $C$  by 81 to get  $(78 \cdot 81 \pmod{83}) = 10$ .

When the group  $G$  is the group of units  $U_p$  for a prime number  $p$ , Bob can use Euclid's algorithm to solve  $Kx \equiv 1 \pmod{p}$  and find the inverse of  $K$  modulo  $p$  instead of finding  $A^{n-b} \pmod{p}$ . (In fact, in the example, if  $K = 41$ , then  $2K \equiv 82 \equiv -1 \pmod{83}$ , so  $-2 \equiv 81$  is the inverse of  $K$ .)

*Remark 13.10* Just as with RSA (Section 9.3), there is a way to sign documents using ElGamal encryption. It is a bit less straightforward than with RSA. For information on the method, see [HPS10], Section 7.3, or try reading [US13], the U.S. National Institute of Standards and Technology publication 186-4, "Digital Signature Standard (DSS)".

## 13.5 Diffie–Hellman in Practice

The Diffie–Hellman key exchange cryptosystem was explicitly invented for sending private keys for use in a high-speed symmetric cryptosystem, and it is widely used for that purpose. The standard symmetric cryptosystem as of 2015 is AES (the Advanced Encryption Standard). The recommended size for a key for AES is 256 bits. Clearly if the Diffie–Hellman system for sending an AES key is insecure, then so is the AES cryptosystem.

Many Diffie–Hellman systems in wide use involve the group  $G = U_p$ , for  $p$  a large prime number. The Primitive Root Theorem, which we will prove in the next two sections, says that  $U_p$  is a cyclic group of order  $p - 1$ , generated by some primitive root  $g$ .

To read intercepted messages from a Diffie–Hellman exchange, Eve presumably must be able to solve the discrete logarithm problem for  $G = \langle g \rangle$ .

If the order  $p - 1$  of  $G$  factors into a product of only small primes, then the Pohlig–Hellman algorithm can solve the discrete logarithm problem in  $G$  fairly rapidly (See Section 13.9). So for a maximally secure Diffie–Hellman system,  $p$  should be a safeprime, so that  $p - 1 = 2q$  where  $q$  is a prime of almost the same size as  $p$ .

The best known attack on the discrete logarithm problem uses a method known as the index calculus. We describe it briefly in Section 17.5.

To apply the index calculus to a discrete logarithm problem involves four computational steps. The first three steps involve the group  $G$ . Only the final step involves finding the discrete logarithm  $a = \log_q(A)$  of a particular element  $A$  of  $G$ , needed to compute the key  $B^a = K$ . The first three steps of the index calculus, called the precomputation phase, are far more computationally demanding than the final step of actually computing a particular discrete logarithm of an element of  $G$ . For example, in [AB15] the authors solved the discrete logarithm problem for a group  $G = U_p$  where  $p$  is a prime number of 512 binary bits (= 154 decimal digits). The precomputation took about a week, with parallel computations on over two thousand computers. With the precomputation completed, the actual computation of any given discrete logarithm in the group, run in parallel on two computers, took on average about 70 seconds.

If each Diffie–Hellman implementation on the internet used a cyclic subgroup  $G$  of  $U_p$  for a different prime  $p$ , then there would be little concern about routine security, because the effort required for precomputation in each group would be cost-prohibitive. But companies that provide security on the internet found it convenient (cost-effective) to implement Diffie–Hellman using groups  $U_p$  where  $p$  is one of a very small set of publicly known safeprimes. Thus a dedicated Eve would find investing the resources to do the necessary precomputation on one of those groups worthwhile, because she could then determine any desired key based on that group in seconds, and so would have access to the encrypted communications of every internet user whose security is based on using Diffie–Hellman with that group.

For these reasons, broad use of the group  $U_p$  for a single widely used prime  $p$  is unsafe. The authors of [AB15] posted on the internet in the fall of 2015 [<https://weakhd.org/>] their estimate that an academic team could amass enough computing resources to break a Diffie–Hellman cryptosystem based on a 768-bit (231 decimal digit) prime and that a nation-state could break one based on a 1024-bit (308 decimal digit) prime. The authors suggested that breaking Diffie–Hellman cryptosystems based on just two widely used 1024-bit primes would compromise 18 percent of the top one million https domains, two-thirds of existing VPN servers and one-fourth of existing SSH servers. (See [Go15] for a news story on this development.)

For the highest level of long-term security (years), publicly available recommendations (e.g., from Cisco Systems [Cs15]) as of December 2015 call for the use of Diffie–Hellman in the group of units  $U_p$  where  $p$  is a safeprime of 3072 binary bits, or 924 decimal digits. Alternatively, the long-term recommendation is to use Diffie–Hellman with a cyclic subgroup of the group of an elliptic curve defined over  $\mathbb{F}_p$ , where  $p$  is a prime of 256 binary bits, or 77 decimal digits, or preferably where  $p$  has 384 bits or 115 decimal digits. (Elliptic curve cryptography is beyond the scope of this book. See [Kob94] or the more current [HPS10] for descriptions of elliptic curve cryptography.)

Further evidence for what is viewed as insecure can be found in the Strategic Goods List in force on April 8, 2015 for the Australian Defence Controls Act of 2011 [AD15]. That law requires a license to export any systems, equipment, application specific electronic assemblies, modules and integrated circuits for information security “... designed or modified to use ‘cryptography’ employing digital techniques performing any cryptographic function other than authentication, digital signature or the execution of copy-protected software, and having ... an asymmetric algorithm where the security of the algorithm is based on any of the following:

- “1. Factorisation of integers in excess of 512 bits (e.g., RSA);
- “2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie–Hellman over  $\mathbb{Z}_p$ ); or
- “3. Discrete logarithms in any group other than mentioned in 2. in excess of 112 bits (e.g., Diffie–Hellman over an elliptic curve).”

One could conclude from this list that any RSA cryptosystem with a modulus of 512 or fewer bits, or any DH cryptosystem in the group of units of a field  $\mathbb{F}_p$  where  $p$  has 512 bits or fewer, is considered so insecure as to not be a potential defense issue.

As with RSA, discrete logarithm cryptography is expected to be vulnerable to quantum computers in 15 to 30 years. Thus in 2015 the U.S. National Security Agency posted an announcement that the agency is actively working on developing cryptographic algorithms that would be quantum-resistant. See [Go15b] for a report on that development (which also references published work on quantum-resistant cryptographic algorithms by workers at the Government Communications Headquarters, the British counterpart to the NSA). See also [Cla19]. But not all researchers are convinced that large-scale quantum computing is feasible. See [Kal16].

## 13.6 The Exponent of an Abelian Group

In the next section is a proof of the Primitive Root Theorem, which says that the group of units  $U_p$  of the field  $\mathbb{Z}_p$  is a cyclic group for every prime  $p$ . Since the group of units of  $\mathbb{Z}_p$  has order  $p - 1$ , this result gives us a limitless supply of cyclic groups of arbitrarily large size.

In this section we prepare for the proof by introducing and studying properties of the exponent of a finite abelian group.

We recall the use of the word “order”.

For  $G$  a finite group, the *order* of  $G$  is defined to be the number of elements of  $G$ .

Let  $G$  be a finite abelian group of order  $n$ , with operation multiplication and with identity element  $e$ . Then for every  $a$  in  $G$ ,  $a^n = e$ , by Lagrange’s theorem. The *order* of the element  $a$  is the smallest number  $d > 0$  so that  $a^d = e$ .

Just as with the group of units modulo  $m$ , we have:

**Proposition 13.11** *In a finite abelian group  $G$  of order  $n$ ,*

- (i) *If  $d$  is the order of  $a$ , and  $m$  is any number with  $a^m = e$ , then  $d$  divides  $m$ .*
- (ii) *The order of  $a$  divides  $n$ , the order of  $G$ ;*
- (iii) *If  $d$  is the order of  $a$ , then  $a^r$  has order  $d/(r, d)$ , where  $(r, d)$  is the greatest common divisor of  $r$  and  $d$ .*

The proofs are more or less immediate consequences of the definition of the order of  $a$  in  $G$  as the least positive integer  $d$  so that  $a^d = e$ , the identity of  $G$ . See Section 8.1 of Chapter 8.

The new idea we introduce in this section is the concept of the exponent of a finite abelian group.

Let  $G$  have order  $n$ . The order of every element of  $G$  divides  $n$ . So the set of numbers that are orders of elements of  $G$  is a set of numbers  $\leq n$ .

**Definition** The *exponent*  $\lambda = \lambda(G)$  of a finite abelian group  $G$  is the number that is maximal among all orders of elements of  $G$ .

Thus the exponent  $\lambda$  is the order of some element of  $G$ ; and for every element  $b$  of  $G$ , if  $h$  is the order of  $b$ , then  $h \leq \lambda$ .

By Property (ii) of Proposition 13.11, the exponent  $\lambda$  divides the order  $n$  of  $G$ .

If  $G$  has order  $n$ , then the exponent of  $G$  is  $n$  if and only if  $G$  is cyclic.

*Example 13.12* Let  $G = U_{20}$ , the group of units of  $\mathbb{Z}_{20}$ . Then

$$G = \{1, 3, 7, 9, 11, 13, 17, 19\} \pmod{20}$$

has order 8 (that is, there are eight units). Then by Euler’s Theorem, for every  $a$  in  $U_{20}$ ,  $a^8 = 1$ . The orders of the elements of  $G$  are as follows:

element	order
1	1
3	4
7	4
9	2
11 = -9	2
13 = -7	4
17 = -3	4
19 = -1	2

Therefore, the exponent  $\lambda$  of  $G = U_{20}$  is  $= 4$ . Since  $\lambda = 4$  there is no element of order 8, so  $U_{20}$  is not a cyclic group.

We wish to prove:

**Theorem 13.13** *Let  $\lambda$  be the exponent of a finite abelian group  $G$ . Then the order of every element  $b$  of  $G$  divides  $\lambda$ .*

To prove this theorem we need one more fact about orders, beyond facts (i)–(iii) above:

**Proposition 13.14** *Let  $a, b$  be elements of a finite abelian group  $G$ . If  $a$  has order  $r$ , and  $b$  has order  $s$ , and  $(r, s) = 1$ , then  $ab$  has order  $rs$ .*

The hypothesis that  $r$  and  $s$  are coprime is necessary. For an extreme example, suppose  $b$  is an element of order  $r > 1$  in  $G$ . Then  $b^{-1}$  also has order  $r$ , but  $bb^{-1}$  has order 1, not  $r^2$  or  $[r, r] = r$ .

*Proof of Proposition 13.14* Let  $e$  be the identity of  $G$ . First observe that since  $a^r = e$  and  $b^s = e$ , we have  $(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = e$ , so the order of  $ab$  is  $\leq rs$ .

Now, let  $d > 0$  so that  $(ab)^d = e$ . To show that  $ab$  has order  $rs$ , we show that  $rs$  divides  $d$ . To do so, we show that  $s$  divides  $d$  and  $r$  divides  $d$ .

To show  $s$  divides  $d$ , we observe that since  $(ab)^d = e$ , then

$$e = (ab)^{dr} = a^{dr}b^{dr} = e^d b^{dr} = b^{dr}$$

since  $a^r = e$ . Since the order of  $b$  is  $s$ , therefore, by (ii) of Proposition 13.11,  $s$  divides  $dr$ . Recalling that  $(r, s) = 1$ , it follows by the Coprime Divisibility Lemma that  $s$  divides  $d$ .

Similarly,

$$e = (ab)^{ds} = a^{ds}b^{ds} = a^{ds}e^d = a^{ds}$$

since  $b^s = e$ . Now  $r$  is the order of  $a$ , so  $r$  divides  $ds$ . Since  $(r, s) = 1$ , it follows that  $r$  divides  $d$ .

Hence  $d$  is a common multiple of  $r$  and  $s$ . The least common multiple  $[r, s]$  of  $r$  and  $s$  divides every common multiple of  $r$  and  $s$ , and since  $r$  and  $s$  are coprime,  $[r, s] = rs$ . So  $rs$  divides  $d$ .

Since  $(ab)^{rs} = e$ , and every  $d > 0$  with  $(ab)^d = e$  is a multiple of  $rs$ , therefore the order of  $ab$  is  $rs$ .  $\square$

Now for the proof of Theorem 13.13:

*Proof* Let  $b$  be an element of  $G$ , and let  $m$  be the order of  $b$ . Let  $\lambda$  be the exponent of  $G$ . Then  $m \leq \lambda$ . We must show that  $m$  divides  $\lambda$ . By definition,  $\lambda$  is the order of some element  $a$  of  $G$ .

We use Proposition 4.3, which says that a number  $m$  divides  $\lambda$  if and only if for every prime number  $p$ , if  $p^e \parallel m$  and  $p^f \parallel \lambda$ , then  $e \leq f$ . (Recall that  $p^e \parallel m$  means that  $m = p^e q$  with  $(q, p) = 1$ .)

Let  $a$  have order  $\lambda$ . Let  $b$  be any element of  $G$ , and let  $m$  be the order of  $b$ . We show that  $m$  divides  $\lambda$ . If not, then there is some prime  $p$  so that  $p^r \parallel m$ ,  $p^s \parallel \lambda$ , and  $r > s$ . Let  $m = p^r q$  with  $(q, p) = 1$  and  $\lambda = p^s t$  with  $(t, p) = 1$ .

Using that  $r > s$ , we find an element of  $G$  whose order is  $> \lambda$ :

Since  $b$  in  $G$  has order  $m = p^r q$ , then

$$d = b^q$$

has order  $p^r$  by property (iii) of Proposition 13.11.

Since  $a$  in  $G$  has order  $\lambda = p^{st}$ , then

$$c = a^{p^s}$$

has order  $t$ , again by property (iii).

But the orders  $p^r$  and  $t$  of  $d$  and  $c$  are coprime. So by Proposition 13.14, the element  $cd$  of  $G$  has order  $tp^r = \lambda p^{r-s}$ , which is larger than  $\lambda$  since  $r > s$ .

This violates the assumption that  $\lambda$  is the exponent of  $G$ .

Hence for every prime  $p$ , the highest power of  $p$  that divides  $m$ , the order of  $b$ , is  $\leq$  the highest power of  $p$  that divides  $\lambda$ . So  $m$  divides  $\lambda$ . (See Proposition 4.3.)

We have therefore shown that the order of every element of  $G$  divides the exponent  $\lambda$ , and the proof is complete.  $\square$

**Corollary 13.15** *If  $\lambda$  is the exponent of a finite abelian group  $G$ , then  $a^\lambda = e$  for every  $a$  in  $G$ .*

This follows immediately from Theorem 13.13 and property (i) of Proposition 13.11.

We apply this to the group  $G = U_m$  of units modulo  $m$ :

**Corollary 13.16** *Let  $\lambda(m)$  be the exponent of  $U_m$ . Then for all integers  $a$  coprime to  $m$ ,*

$$a^{\lambda(m)} \equiv 1 \pmod{m}.$$

**Decrypting exponents for RSA.** Before proving the Primitive Root Theorem, we pause for an observation about RSA cryptography.

Recall that to implement an RSA cryptosystem, Bob picks a modulus  $m = pq$ , where  $p$  and  $q$  are distinct odd primes, and picks some encrypting exponent  $e < \phi(m)$  coprime to  $\phi(m) = (p-1)(q-1)$ . He sends the pair  $(m, e)$  to Alice. Alice has a message  $w$ , a number  $< m$ , and encrypts  $w$  by computing  $c = (w^e \pmod{m})$ . She sends  $c$  to Bob. Bob finds a decrypting exponent  $d < \phi(m)$  satisfying  $ed \equiv 1 \pmod{\phi(m)}$ . Then

$$c^d = w^{ed} = w^{\phi(m)k+1} \equiv w \pmod{m}.$$

So  $d$  is a decrypting exponent for this RSA system.

What makes the system work is that  $w^{\phi(m)} \equiv 1 \pmod{m}$ .

But because of Corollary 13.16, we can replace  $\phi(m) = (p-1)(q-1)$  by  $\lambda(m) = [(p-1), (q-1)]$ , the least common multiple of  $p-1$  and  $q-1$ .

To see why, we first notice that if the encrypting exponent  $e$  is coprime to  $(p-1)(q-1)$  then it is coprime to  $\lambda(m) = [(p-1), (q-1)]$ , because  $[(p-1), (q-1)]$  divides  $(p-1)(q-1)$ . If we find some number  $d' < \lambda(m)$  so that  $ed' \equiv 1 \pmod{\lambda(m)}$ , then the encrypted message  $c = (w^e \pmod{m})$  satisfies

$$c^{d'} = (w^e)^{d'} = w^{ed'} = w^{k\lambda(m)+1} \equiv w \pmod{m}$$

by Corollary 13.16. So  $d'$  is also a decrypting exponent for the RSA cryptosystem using the pair  $(m, e)$ .

In fact,  $d'$  is the smallest decrypting exponent for  $e$  (See Exercise 13.37.)

Here are some illustrations of  $d$  and  $d'$ .

**Example 13.17** Suppose  $m = 3131 = 31 \cdot 101$ . Then  $\phi(m) = 30 \cdot 100 = 3000$ , while  $\lambda(m) = [30, 100] = 300 = \frac{1}{10}\phi(m)$ . Then for  $e = 7$ ,  $d = 2143$ , while  $d' = 43$ .

*Example 13.18* Suppose  $m = 15361 \cdot 25601 = 393256961$ . Then  $\phi(m) = 15360 \cdot 25600 = 393216000$  while

$$\lambda(m) = [15360, 25600] = [2^{10} \cdot 3 \cdot 5, 2^{10} \cdot 5^2] = 2^{10} \cdot 75 = 76800.$$

So

$$\lambda(m) = \frac{\phi(m)}{5120}$$

If  $e = 11$ , then  $d = 357469091$ , while  $d' = 44591$ .

*Example 13.19* Let  $p = 5051$ ,  $q = 8081$ ,  $m = 40817131$ . Then

$$\phi(m) = (p - 1)(q - 1) = 5050 \cdot 8080 = 40804000,$$

while

$$\lambda(m) = [p - 1, q - 1] = [5050, 8080] = 40804000/1010 = 40400.$$

Let  $e = 107$ . Then  $d' = 2643$ , while  $d = 27838243$ .

While using  $d'$  instead of  $d$  reduces Bob's computational burden, there is a security risk to  $d'$  being too small— $d'$  might be found by trial and error.

In general, suppose the encrypting exponent is a number  $e < 100$ . Then the decrypting exponent  $d < \phi(m)$  is the inverse of  $e$  modulo  $\phi(m)$ , so  $de \geq \phi(m)$ , hence  $d$  will lie between  $\phi(m)/100$  and  $\phi(m)$ , while the decrypting exponent  $d'$  is the inverse of  $e$  modulo  $\lambda(m)$ , so will lie between  $\lambda(m)/100$  and  $\lambda(m)$ , as the examples above illustrate.

Since the cryptosystem depends on its security on Eve not finding a decrypting exponent, it is desirable to ensure that the smallest decrypting exponent  $d'$  is close to  $m = pq$  in size. So  $\lambda(m)$  should not be much smaller than  $\phi(m)$ . Since

$$\lambda(m) = \frac{\phi(m)}{(p - 1, q - 1)},$$

an optimal choice is to choose  $m = pq$  where  $p$  and  $q$  are safeprimes. In that case,  $\phi(m) = 2\lambda(m)$ .

*Example 13.20* Suppose  $m = 83 \cdot 107 = 8881$ , a product of safeprimes. Then  $\phi(m) = 82 \cdot 106 = 8692$ , while  $\lambda(m) = [82, 106] = 41 \cdot 106 = 4346 = \frac{1}{2}\phi(m)$ .

Let  $e = 11$ . Then  $ed \equiv 1 \pmod{8692}$  for  $d = 3951$ . Since  $d = 3951 < \lambda(m)$ , and  $\lambda(m)$  divides  $\phi(m)$ ,  $d' = 3951$  because the inverse of 11 modulo 4346 is unique.

Given an RSA cryptosystem with modulus  $m$  and encrypting exponent  $e$ , we showed in Chapter 9 that if Eve were to learn  $\phi(m)$ , then she could factor  $m$ . In Section 14.6, we'll show that if Eve can find any decrypting exponent  $d'$  for  $e$ , she can with high probability factor  $m$ .

**Finding primitive roots.** Recall Proposition 13.14: in  $U_m$  if  $a$  has order  $r$  and  $b$  has order  $s$  where  $r$  and  $s$  are coprime, then  $ab$  has order  $rs$ . Proposition 13.14 is useful for finding elements in an abelian group with large orders.

*Example 13.21* Let  $G = U_{31}$ , a group under multiplication. To see if  $U_{31}$  is cyclic, we try to find an element of order 30. The elements of  $U_{31}$  have orders that divide 30. We find some orders:

- 2 has order 5: for  $2^5 = 32 \equiv 1 \pmod{31}$ .
- $-2 = 29$  has order 10: for  $(-2)^5 = -1$ , so  $(-2)^{10} \equiv 1 \pmod{31}$ , and  $(-2)^1, (-2)^2$  and  $(-2)^5$  are all  $\not\equiv 1 \pmod{31}$ .
- 5 has order 3: for  $5^3 = 125 \equiv 1 \pmod{31}$  ( $31 \cdot 4 = 124$ ).

By Proposition 13.14, since  $-2$  and  $5$  have orders  $10$  and  $3$  that are coprime, therefore  $(-2) \cdot 5 = -10 \equiv 21$  has order  $30$ . Thus the cyclic group  $\langle 21 \rangle$  contains  $30$  elements (Proposition 10.20). So  $U_{31} = \langle 21 \rangle$ .

## 13.7 The Primitive Root Theorem

In this section we prove:

**Theorem 13.22** (The Primitive Root Theorem) *For every prime  $p$ ,  $U_p$  is a cyclic group.*

This means that for every prime  $p$  there is a unit  $b$  whose order modulo  $p$  is  $p - 1$ . Any such unit is called a *primitive root*.

We've seen some examples: we observed above that  $U_7$  and  $U_{31}$  are cyclic groups. In Chapter 5, we found that  $U_{11}$  is cyclic, and in Chapter 10, we found that  $U_{13}$  is cyclic.

*Proof* We know that  $\mathbb{Z}_p$  is a field, and the group of units  $U_p$  of  $\mathbb{Z}_p$  has order  $p - 1$ . In Chapter 6, we proved D'Alembert's Theorem: a polynomial of degree  $d$  with coefficients in a field cannot have more than  $d$  roots in the field. We'll apply D'Alembert's Theorem in the proof.

Suppose the exponent of  $U_p$  is  $\lambda$ . From Corollary 13.15, all of the  $p - 1$  elements of  $U_p$  are roots of the polynomial  $x^\lambda - 1$ . Since  $\mathbb{Z}_p$  is a field, by D'Alembert's Theorem,  $p - 1$  must be  $\leq \lambda$ .

Let  $b$  be some element of  $U_p$  whose order is  $\lambda$ . By Fermat's Theorem and Proposition 13.11 (ii),  $b^{p-1} = 1$ , so  $\lambda$  divides  $p - 1$ .

Since  $\lambda$  divides  $p - 1$  and  $p - 1 \leq \lambda$ , we conclude that  $\lambda = p - 1$ . Hence  $b$  has order  $p - 1$ .

So  $U_p = \langle b \rangle$  is a cyclic group.  $\square$

The proof of Theorem 13.22 generalizes easily to yield:

**Theorem 13.23** *Every finite subgroup of the multiplicative group of non-zero elements of a field is cyclic.*

In particular,

**Corollary 13.24** *The multiplicative group of units of a finite field is cyclic.*

There are many examples of finite fields other than the fields  $\mathbb{Z}_p$  for  $p$  a prime number, as we'll see in Section 18.5.

For Diffie–Hellman, we want a cyclic group of large order. Since there are infinitely many primes, we can find a cyclic group of order as large as we want by using  $U_p$  for  $p$  a large prime.

But we also need a generator of the cyclic group. So given a prime  $p$  of appropriately large size, we need to find a primitive root modulo  $p$ . So we ask, how difficult is it to find a primitive root of  $\mathbb{Z}_p$  for  $p$  prime?

It turns out, not at all difficult.

**Proposition 13.25** *In  $\mathbb{Z}_p$  there are  $\phi(p - 1)$  primitive roots.*

*Proof* Recall Proposition 13.11, (iii): in a finite abelian group  $G$ , if  $d$  is the order of  $a$ , then  $a^r$  has order  $d/(r, d)$ , where  $(r, d)$  is the greatest common divisor of  $r$  and  $d$ .

This result says, in particular, that if  $b$  is a primitive root of  $U_p$ , so that  $b$  has order  $p - 1$ , then for every  $r$  coprime to  $p - 1$ ,  $b^r$  also has order  $p - 1$ , so is a primitive root. So there are as many primitive roots modulo  $p$  as there are numbers coprime to  $p - 1$ .  $\square$

*Example 13.26* We found that 21 is a primitive root modulo 31. So 21 has order 30 in  $U_{31}$ . For every number  $r$  coprime to 30,  $21^r$  also has order 30 and is therefore a primitive root. So there are  $\phi(30) = \phi(2)\phi(3)\phi(5) = 1 \cdot 2 \cdot 4 = 8$  primitive roots in  $U_{31}$ .

The numbers coprime to 30 are 1, 7, 11, 13, 17, 19, 23, 29. So the eight primitive roots in  $U_{31}$  are:

$$\begin{aligned} 21^1 &\equiv 21 \pmod{31} \\ 21^7 &\equiv 11 \pmod{31} \\ 21^{11} &\equiv 12 \pmod{31} \\ 21^{13} &\equiv 22 \pmod{31} \\ 21^{17} &\equiv 24 \pmod{31} \\ 21^{19} &\equiv 13 \pmod{31} \\ 21^{23} &\equiv 17 \pmod{31} \\ 21^{29} &\equiv 3 \pmod{31}. \end{aligned}$$

In general, it is known that for all  $n > 2$ ,

$$\phi(n) \geq \frac{n}{1.781 \ln \ln n + \frac{3}{\ln \ln n}}$$

([Rib89], p. 172), so for large primes  $p$ , there are many primitive roots. For example, if  $p$  has 200 digits, then  $\ln \ln(p - 1) = \ln(460.5) = 6.13$ , so

$$\frac{\phi(p - 1)}{p - 1} \geq \frac{1}{1.781 \cdot 6.13 + \frac{3}{6.13}} = \frac{1}{11.41} = .088 :$$

Since the probability is  $\geq .088$  that a random number  $< p$  is a primitive root, if we pick 50 random numbers  $< p - 1$ , the probability of finding no primitive root among them is less than

$$(1 - .088)^{50} < .01.$$

*Example 13.27* To test the lower bound for  $\phi(p - 1)$ , let  $p = 10111$ , a prime number. We have  $n = p - 1 = 10110$ , and the lower bound implies that there are at least

$$\phi(10110) \geq \frac{10110}{1.781 \ln \ln 10110 + \frac{3}{\ln \ln 10110}} = 1905$$

primitive roots, since  $\ln \ln 10110 = 2.215$ .

In fact, 10110 factors as  $10110 = 2 \cdot 3 \cdot 5 \cdot 337$ , so

$$\phi(10110) = 2 \cdot 4 \cdot 336 = 2688$$

is the number of primitive roots modulo 10111.

For discrete logarithm cryptography, it is particularly desirable to work with a cyclic group whose order is either a large prime or is divisible by a large prime. If  $p$  is a safeprime, that is,  $p = 2q + 1$  where  $q$  is prime (a Sophie Germain prime), then  $U_p$  has order  $2q$ . For  $p$  a safeprime, the cyclic group  $G = U_p$  is particularly resistant against known strategies for solving the discrete logarithm problem.

For  $p$  a safeprime, finding a primitive root modulo  $p$ , that is, a generator of  $G$ , is especially easy. (See Exercise 13.9.)

Information is readily available on the internet regarding primitive roots for small primes. For example, the smallest primitive root modulo  $p = 191$  is 19, and the smallest primitive root modulo  $p = 71$  is 7. For every other prime  $p < 200$ ,  $U_p$  has a smallest primitive root equal to 6, 5, 3 or 2. Among those primes, 2 is a primitive root for  $p = 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181$  and 197.

## 13.8 The Exponent of $U_m$

It is a fact that if  $p$  is an odd prime, then the group of units of  $\mathbb{Z}_{p^n}$  is a cyclic group for all  $n \geq 1$ . In other words, there exist primitive roots modulo  $p^n$  for  $p$  an odd prime. [See Exercise 13.17].

For  $p = 2$ , the group of units  $U_{2^n}$  is not cyclic, but has exponent  $\lambda(2^n) = 2^{n-2}$ . As for numbers  $m$  divisible by two or more distinct primes, we can determine the exponent  $\lambda(m)$  of  $U_m$  by factoring  $m$  into a product of prime powers. The idea is:

**Proposition 13.28** *Let  $m = rs$  where  $r$  and  $s$  are coprime. Then*

$$\lambda(m) = [\lambda(r), \lambda(s)],$$

*the least common multiple of  $\lambda(r)$  and  $\lambda(s)$ .*

*Proof* We know that

$$U_m \cong U_r \times U_s$$

by Proposition 12.17. To show that there is an element of  $U_m$  with order  $[\lambda(r), \lambda(s)]$ , let  $b$  in  $U_r$  have order  $\lambda(r)$  and let  $c$  in  $U_s$  have order  $\lambda(s)$ . Let  $a$  in  $U_m$  satisfy

$$\begin{aligned} a &\equiv b \pmod{r} \\ a &\equiv c \pmod{s} \end{aligned}$$

( $a$  exists by the Chinese Remainder Theorem). Then  $a$  has order  $[\lambda(r), \lambda(s)]$ . So

$$[\lambda(r), \lambda(s)] \leq \lambda(m).$$

On the other hand, if  $b$  in  $U_m$  has order  $\lambda(m)$ , let  $b$  have order  $f$  modulo  $r$  and have order  $g$  modulo  $s$ . Since  $r$  and  $s$  are coprime,  $b$  has order  $[f, g]$  modulo  $m$ . So  $\lambda(m) = [f, g]$ . But  $f$  divides  $\lambda(r)$  and  $g$  divides  $\lambda(s)$ , so  $[f, g]$  divides  $[\lambda(r), \lambda(s)]$  (show this for each prime power factor of  $[f, g]$ ), and so  $\lambda(m)$  divides  $[\lambda(r), \lambda(s)]$ .

So  $[\lambda(r), \lambda(s)] = \lambda(m)$  when  $m = rs$  and  $(r, s) = 1$ . □

This result enables us to find  $\lambda(m)$  for every number  $m$ , as long as we can factor  $m$ .

*Example 13.29*  $U_{35} \cong U_5 \times U_7$ . The exponent of  $U_5$  is 4 (by Fermat's Theorem and the Primitive Root Theorem) and the exponent of  $U_7$  is 6 (for the same reasons). So the exponent of  $U_{35}$  is the least common multiple of 4 and 6, that is,  $\lambda(35) = [4, 6] = 12$ .

Recall that  $U_m(k)$  denotes the subgroup of  $U_m$  consisting of the  $k$ -th roots of unity in  $U_m$ :

$$U_m(k) = \{u \in U_m : u^k = 1\}.$$

We proved that if  $\lambda$  is the exponent of  $U_m$ , then not only is  $\lambda$  the order of some element of  $U_m$ , but also, for all  $b$  in  $U_m$ ,  $b^\lambda = 1$ : the order of every element of  $U_m$  divides  $\lambda$ . Thus

$$U_m(\lambda) = U_m,$$

but

$$U_m(\omega) \neq U_m \text{ for all } \omega < \lambda.$$

For example,  $\lambda(35) = [\lambda(7), \lambda(5)] = [6, 4] = 12$ , so

$$U_{35}(12) = U_{35},$$

but  $U_{35}(\omega) \neq U_{35}$  for  $\omega < 12$  because  $U_{35}$  has an element of order 12 (by definition of the exponent of  $U_{35}$ ).

*Remark 13.30* The Diffie–Hellman key exchange requires a cyclic group of large order. One source of cyclic groups of arbitrarily large order are the groups  $U_{p^e}$  of units of  $\mathbb{Z}_{p^e}$  for a small prime  $p$  and a large exponent  $e$ . The group  $U_{p^e}$  has order  $(p - 1)p^{e-1}$ .

But it turns out that  $U_{p^e}$  has a cyclic subgroup of order  $p^{e-1}$  for which the discrete logarithm problem is easy to solve, because there is an explicitly computable formula for the discrete logarithm function (involving  $e$  terms) for that cyclic subgroup. So for small primes  $p$  the cyclic group  $U_{p^e}$  is not an appropriate cyclic group for cryptography. To see how to solve the discrete logarithm problem in  $U_{p^e}$ , see Exercise 13.35.

## 13.9 The Pohlig–Hellman Algorithm

We describe the Pohlig–Hellman algorithm, dating from 1978, for finding the discrete logarithm of an element of  $U_p = \langle g \rangle$ . It is useful when  $p - 1$  is a product of powers of small primes. The algorithm uses the Chinese Remainder Theorem to transform the problem to one of finding the discrete logarithm of numbers in  $U_q$  where  $q$  runs through the prime power divisors of  $p - 1$ .

The existence of this algorithm implies that for a cryptosystem that relies on the difficulty of the discrete logarithm problem, the order of the group should be divisible by a large prime. In particular, for maximum security using a group of units  $U_p$ , it is desirable that  $p$  be a safeprime, so that the order of  $U_p$  is  $p - 1 = 2q$  where  $q$  is prime.

Suppose  $p$  is prime,  $U_p = \langle g \rangle$  where  $g$  is a primitive root modulo  $p$ , and  $p - 1 = q_1 q_2 \cdots q_k$  where  $q_1, \dots, q_k$  are the prime power factors of  $p - 1$ . The idea is that inside  $U_p$  are cyclic subgroups  $H_1, H_2, \dots, H_k$  of orders  $q_1, q_2, \dots, q_k$ . If we can solve the discrete logarithm problem in each of those subgroups  $H_i$ , then we can use the Chinese Remainder Theorem to solve the discrete logarithm problem in  $G$ .

*Example 13.31* We illustrate the Pohlig–Hellman algorithm.

We want to solve the discrete logarithm problem in  $U_{241}$ . We have  $\phi(241) = 240 = 3 \cdot 5 \cdot 16$ , a product of distinct prime powers, and 7 is a primitive root of  $U_{241}$ , so that  $U_{241} = \langle 7 \rangle$ .

We'll work in  $\mathbb{Z}_{241}$ , but will omit writing “mod 241” in all of the calculations in this example.

Suppose we wish to find  $x$  so that  $7^x = 6$ .

We observe that  $240 = 16 \cdot 15 = 5 \cdot 48 = 3 \cdot 80$ . So the unique subgroup of  $U_{241}$  of order 16 is  $\langle 7^{15} \rangle$ , the unique subgroup of order 5 is  $\langle 7^{48} \rangle$  and the unique subgroup of order 3 is  $\langle 7^{80} \rangle$ . We compute in  $U_{241}$ :

$$\begin{aligned} 7^{15} &= 111 \\ 7^{48} &= 91 \\ 7^{80} &= 15. \end{aligned}$$

Then  $\langle 111 \rangle$  is the subgroup of  $U_{241}$  of order 16,  $\langle 91 \rangle$  is the subgroup of  $U_{241}$  of order 5, and  $\langle 15 \rangle$  is the subgroup of  $U_{241}$  of order 3.

We find conditions on the  $x$  satisfying  $7^x = 6$  in  $\langle 7 \rangle$  by looking at related discrete logarithm problems in the subgroups  $\langle 111 \rangle$ ,  $\langle 91 \rangle$  and  $\langle 15 \rangle$ . Here is how it is done.

The  $x$  satisfying  $7^x = 6$  (always modulo 241) must satisfy:

$$\begin{aligned} 111^x &= 7^{15x} = 6^{15} \\ 91^x &= 7^{48x} = 6^{48} \\ 15^x &= 7^{80x} = 6^{80}. \end{aligned}$$

After some calculations we find that  $6^{15} = 177$ ,  $6^{48} = 87$  and  $6^{80} = 1$  in  $U_{241}$ . So we have transformed the original discrete logarithm problem: find  $x$  so that  $7^x = 6$ , into the simultaneous discrete logarithm problems: find  $x$  so that

$$\begin{aligned} 111^x &= 177 \\ 91^x &= 87 \\ 15^x &= 1. \end{aligned}$$

These are discrete logarithm problems in the subgroups generated by 111, 91 and 15, respectively.

Since these groups have small orders 16, 5 and 3, respectively, it is feasible to solve these problems by simply writing down all the powers of each of the three generators:

power of	111	91	15
1	111	91	15
2	30	87	225
3	197	205	1
4	177	98	
5	126	1	
6	8		
7	165		
8	240		
9	130		
10	211		
11	44		
12	64		
13	115		
14	233		
15	76		
16	1		

From the table we see that

$$\begin{aligned} 177 &= 111^4 \\ 87 &= 91^2 \\ 1 &= 15^3. \end{aligned}$$

Since  $111^x = 177 = 111^4$ , and 111 has order 16 in  $U_{241}$ , the exponent  $x$  must be congruent to 4 modulo 16. Since  $91^x = 87 = 91^2$ , and 91 has order 5,  $x$  must be congruent to 2 modulo 5. Since  $15^x = 1 = 15^0$ , and 15 has order 3,  $x$  must be congruent to 0 modulo 3. Thus  $x$  must satisfy the system of congruences

$$\begin{aligned} x &\equiv 4 \pmod{16} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 0 \pmod{3}. \end{aligned}$$

By the Chinese Remainder Theorem, there is a unique solution of this set of congruences modulo 240, namely  $x = 132 \pmod{240}$ .

So,  $7^{132} \equiv 6 \pmod{241}$ , and  $\log_7(6) = 132$ .

The strategy of the example generalizes easily. Try doing Exercise 13.32.

## 13.10 Shanks' Baby Step-Giant Step Algorithm

Let  $p$  be a prime and let  $\langle g \rangle$  be a cyclic subgroup of  $U_p$  of order  $h$ . For  $h$  fairly large, the method of solving the discrete logarithm problem in  $\langle g \rangle$  by just writing down the  $h$  different powers of  $g$ , as we did in the last example, becomes impractical. Here is an alternative which is faster, called the “baby step-giant step” algorithm, due to Daniel Shanks (1971).

Instead of writing down all of the powers of  $g$ , let  $m$  be the smallest integer greater than  $\sqrt{h}$  and write down the first  $m$  powers of  $g$ .

Suppose we wish to solve the discrete logarithm problem  $a = g^x$  for some  $a$  in  $\langle g \rangle$ . We write  $x = mq + r$  (Division Theorem) with  $0 \leq r < m$ . Note that since  $x < h$  = the order of  $g$ , and  $m \geq \sqrt{h}$ , we have  $q < \sqrt{h}$ . Now

$$a = g^x = g^{mq+r} = g^{mq}g^r.$$

So

$$a(g^{-m})^q = g^r.$$

We already have the list of the first  $m$  powers of  $g$ , so that list contains  $g^r$ . We begin generating another list, namely the list of  $a(g^{-m})^q$  for  $q = 1, 2, \dots$ . When we find some  $q$  so that  $a(g^{-m})^q \equiv g^r \pmod{p}$  for some  $r$  on the first list, then

$$a = (g^m)^q g^r = g^{mq+r}$$

so we have found  $x = mq + r$  that solves the discrete logarithm problem for  $a$  in  $\langle g \rangle$ .

*Example 13.32* Let  $p = 383$ , a safeprime. Then 5 is a primitive root modulo 383. We work in  $\mathbb{Z}_{383}$ , so congruence always means modulo 383 unless specified otherwise.

Suppose we want to find  $x$  so that

$$5^x \equiv 122.$$

The smallest integer  $> \sqrt{383}$  is 20. So we generate the first 20 powers of 5, find  $5^{-20} \equiv 48$  and then generate the elements  $122 \cdot (48^q)$  for  $q = 1, \dots, 20$ . We obtain the following table (done in Excel):

$r$		$5^r \bmod 383$	$q$	$5^{-20q}$	$5^{-20q} \bmod 383$	$122 \cdot 5^{-20q}$	$\bmod 383$
1	5	5	1	48	48	5856	111
2	25	25	2	2304	6	732	349
3	125	125	3	288	288	35136	283
4	625	242	4	13824	36	4392	179
5	1210	61	5	1728	196	23912	166
6	305	305	6	9408	216	26352	308
7	1525	376	7	10368	27	3294	230
8	1880	348	8	1296	147	17934	316
9	1740	208	9	7056	162	19764	231
10	1040	274	10	7776	116	14152	364
11	1370	221	11	5568	206	25132	237
12	1105	339	12	9888	313	38186	269
13	1695	163	13	15024	87	10614	273
14	815	49	14	4176	346	42212	82
15	245	245	15	16608	139	16958	106
16	1225	76	16	6672	161	19642	109
17	380	380	17	7728	68	8296	253
18	1900	368	18	3264	200	24400	271
19	1840	308	19	9600	25	3050	369
20	1540	8	20	1200	51	6222	94

The third column contains the powers of 5 modulo 383. The rightmost column contains 122 multiplied by the powers of  $5^{-20}$  modulo 383.

We are looking for a common value in the third and eighth columns.

If we isolate the first, third, eighth and fourth columns (copying in Excel just the values of the table above, and not the formulas), then sort the new first two columns by increasing values in the new second column, and sort the other two columns by increasing values in the new third column, we obtain:

$r$	$5^r \bmod 383$	$122 \cdot 5^{-20q} \bmod 383$	$q$
1	5	82	14
20	8	94	20
2	25	106	15
14	49	109	16
5	61	111	1
16	76	166	5
3	125	179	4
13	163	230	7
9	208	231	9
11	221	237	11
4	242	253	17
15	245	269	12
10	274	271	18
6	305	273	13
19	<b>308</b>	283	3
12	339	<b>308</b>	6
8	348	316	8
18	368	349	2
7	376	364	10
17	380	369	19

From this table it is easy to find the common number in the second and third column:

$$5^{19} \equiv 308 \equiv 122 \cdot 5^{-20 \cdot 6} \pmod{383}.$$

Hence

$$122 \equiv 5^{20 \cdot 6 + 19} = 5^{139} \pmod{383}.$$

Setting up the two lists of powers  $g^r$  for  $1 \leq r < m$  and  $g^{-mq}$  for  $1 \leq q < m$  requires writing down at most  $2\sqrt{p}$  powers. We could have shortened the process somewhat by writing down the list of powers  $g^r$  and then writing down the powers  $g^{-mq}$  for  $q \geq 1$  only until we get a match with the first list. Finding a match in that way, assuming an efficient way to do the matching, means that on average we would compute  $\sqrt{p} + \sqrt{p}/2$  powers of  $g$ . This compares well with the method of just writing down all the powers of  $g$  and looking for  $a$  in the list, which on average takes about  $p/2$  steps.

In our example, the baby step-giant step strategy would have found the discrete logarithm of 122 by computing 26 numbers: the first 20 powers of 5, and 122 multiplied by the first six powers of  $5^{-20}$ . The naive method of just writing down powers of 5 until we found 122 would have required computing 139 powers of 5.

Since the publication of [DH76], there has been a lot of research on the discrete logarithm problem. For more discussion of discrete logarithms, see, for example, [Od85], [JOP14] and the books [CP05] and [HPS10].

We'll return to the problem of finding the discrete logarithm in the group of units  $U_p$  in Chapter 17. The Index Calculus method in Section 17.5 can be viewed as a generalization of the Baby Step-Giant Step algorithm.

**A possible weakness in the implementation of RSA.** The idea behind the Baby Step-Giant Step algorithm, namely, comparing two lists of numbers, is the basis of a possible attack on RSA.

To share 36-bit private keys for use in a fast private-key cryptosystem, Alice and Bob have set up an RSA cryptosystem with a modulus  $m$  that is a product of two 256-bit primes. Bob sends Alice a fairly small encrypting exponent  $e$  (such as  $e = 2^{16} + 1$ , the largest known Fermat prime). Alice chooses a random 36-bit private key  $w$  and sends Bob  $c = w^e \pmod{m}$ . (Since  $w$  is chosen randomly,  $w$  is unlikely to be prime: see Section 9.5.)

Eve intercepts  $m$ ,  $e$  and  $c$  and hopes that the random private key  $w$  happens to factor into a product  $w = w_1 w_2$  where both factors are  $< 2^{20} < 1.04 \times 10^6$ . If so, then  $c = w^e = w_1^e w_2^e$ .

Eve attempts to determine  $w$  by an analogue of the Shanks Baby Step-Giant Step algorithm: she computes and stores  $w_1^e \pmod{m}$  for  $w_1 = 1, 2, \dots, 2^{20}$ , then computes  $c w_2^{-e} \pmod{m}$  for  $w_2 = 1, 2, \dots$  and compares each result with the stored list. If for some  $w_1$  and  $w_2$ ,  $c w_2^{-e} \equiv w_1^e \pmod{m}$ , then

$$c \equiv w_1^e w_2^e \equiv w^e \pmod{m}$$

so Eve has found  $w = w_1 w_2$ .

The point of this example is that before encrypting and sending a plaintext word using RSA (or DH), it is important to first transform the plaintext (by some easily reversible function known to both Alice and Bob) into a word whose size is close to that of the modulus. As Boneh, Joux and Nguyen [BJN00] state: "Our results demonstrate that preprocessing messages prior to encryption is an essential part of both systems."

## Exercises

Some of the exercises involve computing modular powers. If you don't want to spend time doing them by the XS binary method (except in Exercise 13.2), there are online resources, such as [Tr09], that can help.

- 13.1. Let  $p(x) = x^{10} + 8x^7 + 4x^3 + 1$ . Use the table in Example 13.5 to compute  $f(9)$  modulo 11.
- 13.2. The groups of units  $U_{101}$  and  $U_{107}$  are cyclic groups, both with 2 as a primitive root. To test the difficulty of the discrete logarithm problem using a very slow computer (= you), get a pencil and some scrap paper and a calculator that only does addition, subtraction, multiplication and division, and, timing yourself separately on each part:
  - (i) In  $U_{101}$ , find  $\log_2(61)$ —that is, find the exponent  $e$  so that  $2^e \equiv 61 \pmod{101}$ . How did you go about doing it? How many minutes did it take you?
  - (ii) In  $U_{107}$  find  $2^{73}$ —that is, find the number  $b < 101$  so that  $2^{73} \equiv b \pmod{101}$ . How did you go about doing it? How many minutes did it take you?
  - (iii) Which was easier to do, (i) or (ii)?
- 13.3. Alice and Bob use  $U_{89} = \langle 3 \rangle$  for a Diffie–Hellman key exchange. Alice chooses her secret exponent  $a = 66$ , computes  $3^{66} = 55$  and sends Bob  $A = 55$ . Bob chooses his secret exponent  $b = 23$ , computes  $3^{23} = 13$  and sends Alice  $B = 13$ . What is Alice and Bob's shared secret key?
- 13.4. Alice wants to send Bob the message 20, using an ElGamal cryptosystem. Using  $U_{83} = \langle 2 \rangle$ , Bob picks  $b = 25$ , computes  $2^{25} \equiv 22$ , and sends Alice  $B = 22$ . Alice chooses  $a = 37$  for her secret exponent, and uses it to encrypt her message.
  - (i) What does Alice send Bob?
  - (ii) Do the computations Bob must do to recover Alice's message  $M = 20$ .
- 13.5. Modulo 61, show that
  - (i)  $11^2 \equiv -1$
  - (ii)  $3^5 \equiv -1$
  - (iii)  $13^3 \equiv 1$ .
 Use those facts and Proposition 13.14 to find a primitive root modulo 61. Explain how you used those facts in finding your primitive root.
- 13.6. (i) Show that  $b$  is a primitive root modulo 73 if and only if  $b^{36} \not\equiv 1 \pmod{73}$  and  $b^{24} \not\equiv 1 \pmod{73}$ .
  - (ii) Show that
    - 2 has order 9 mod 73;
    - 3 has order 12 mod 73;
    - $3^{-1} \equiv 49$  has order 12 mod 73;
    - $5^2 \cdot 3 \equiv 2 \pmod{73}$ .
  - (iii) Show from (i) and (ii) that 5 is a primitive root modulo 73.
- 13.7. Prove Theorem 13.23.
- 13.8. Prove Corollary 13.24 assuming Theorem 13.23.
- 13.9. Let  $p = 2q + 1$  be a safeprime (so  $q$  and  $p$  are prime numbers). How many primitive roots are there modulo  $p$ ? How many elements are there in  $U_p$  of order  $\geq q$ ?
- 13.10. How many primitive roots are there modulo 61?
- 13.11. Let  $m = 2p$ ,  $p$  an odd prime. Suppose  $b$  is a primitive root modulo  $p$ . Find a primitive root modulo  $2p$ , as follows:
  - (i) Show that  $\phi(m) = \phi(p) = p - 1$ .

(ii) Let  $b$  be a primitive root modulo  $p$ . Let  $c$  be a solution of

$$\begin{aligned}x &\equiv b \pmod{p} \\x &\equiv 1 \pmod{2}.\end{aligned}$$

Show that  $c$  has order  $p - 1$  modulo  $2p$ , hence is a primitive root mod  $2p$ .

(iii) Find the element  $c$  of  $U_{22}$  that corresponds, as in (ii), to  $b = 6$ .

13.12. (i) What is the exponent of the group  $U_p$  of units modulo  $p$  for  $p$  a prime number?

(ii) What is the exponent of the group  $U_{221}$  of units modulo  $221 = 13 \cdot 17$ ?

13.13. For each element of  $U_{21}$ , find its order in the group  $U_{21}$ . What is the exponent of  $U_{21}$ ?

The next three exercises look at the exponent of  $U_{p^e}$  for  $e > 1$ .

13.14. (i) Show that 2, 12, 17 and 22 have order 4 modulo 5 and have order 20 modulo 25.

(ii) Show that 7 has order 4 modulo 5 and also has order 4 modulo 25.

13.15. Let  $p$  be an odd prime. Using the Binomial Theorem, show that for every number  $r \geq 1$  and every number  $d$ , there is a number  $d'$  so that

$$(1 + dp^r)^p = 1 + d'p^{r+1}$$

where  $d' \equiv d \pmod{p}$ .

13.16. Let  $p$  be an odd prime. Show that  $b = 1 + p$  has order  $p^{r-1}$  modulo  $p^r$  for every  $r > 1$ .

13.17 (i) Let  $p$  be an odd prime. Let  $s$  be a primitive root modulo  $p$ . Show that  $s^{p-1} \equiv 1 + t_1 p \pmod{p^2}$ . If  $t_1 = 0 \pmod{p}$  (so that  $s$  has order  $p$  modulo  $p^2$ ), then show that  $b = s + p$  satisfies  $b^{p-1} \equiv 1 + a_1 p \pmod{p^2}$  where  $a_1$  is coprime to  $p$ . (See Exercise 13.14 for examples with  $p = 5$ .)

(ii) Use the last exercise to show that if  $b$  is a primitive root modulo  $p$  and  $b^{p-1} \equiv 1 + a_1 p \pmod{p^2}$  with  $a_1$  coprime to  $p$ , then  $b$  is a generator of the group of units  $U_{p^r}$  for all  $r \geq 1$ , and therefore  $U_{p^r}$  is a cyclic group for all odd primes  $p$  and all  $r \geq 1$ . In other words,  $b$  is a primitive root modulo  $p^r$  for all  $r \geq 1$ .

13.18. Find the order of  $U_m(m-1)$  when

- (i)  $m = 91 = 13 \cdot 7$ ,
- (ii)  $m = 51 = 17 \cdot 3$ ,
- (iii)  $m = 481 = 13 \cdot 37$ .

13.19. For any modulus  $m$  and any  $k$ , show that if  $U_m(k) = U_m$ , then  $k$  is a multiple of the exponent  $\lambda(m)$  of  $U_m$ .

13.20. Find  $U_{15}(e)$  for  $1 \leq e \leq 10$ .

13.21. Let  $m = pq$ , a product of two distinct primes. For all numbers  $e$ , show that  $(e, \phi(m)) = 1$  if and only if  $(e, \lambda(m)) = 1$ .

13.22. Show that if  $m \geq 3$ , then  $\lambda(m)$  is an even number.

13.23. Let  $e$  be an encrypting exponent for an RSA cryptosystem based on the modulus  $m = pq$ , a product of two distinct primes.

(i) Show that every number  $f$  satisfying  $ef \equiv 1 \pmod{\lambda(m)}$  will serve as a corresponding decrypting exponent.

(ii) Show that there is a unique decrypting exponent  $f$  for  $e$  with  $1 < f < \lambda(m)$ .

13.24. Suppose  $m = pq$  is an RSA modulus, and  $p$  and  $q$  are distinct safeprimes  $\geq 11$ . What are the possibilities for  $[p-1, q-1]$ ?

Suppose you use RSA to encrypt a numerical word  $w$  where  $w < m$ , the modulus. Let  $e$  be an encrypting exponent. In the exercises of Chapter 11 we asked if there are words so that  $w^e \equiv w \pmod{m}$ . Here are two more problems on that issue.

- 13.25. Let  $m = pq$ ,  $p, q$  odd primes. Let  $e$  be odd and coprime to  $\phi(m)$ . Show that if  $(e - 1, \lambda(m)) = 2$ , then there are exactly nine numbers  $w$  with  $0 \leq w < m$  so that  $w^e \equiv w \pmod{m}$ .
- 13.26. Let  $m = pq$ ,  $p, q$  odd primes, both  $> 2^{20}$  and congruent to 3 modulo 4. Let  $e = 65537 = 2^{16} + 1$ , a prime number. Show that there are exactly nine numbers  $w$  with  $0 \leq w < m$  so that  $w^e \equiv w \pmod{m}$ .

The next four exercises relate to a characterization of finite cyclic groups.

- 13.27. Let  $(G, *)$  be a cyclic group of finite order  $n$ .
  - (i) Show that for  $r$  a divisor of  $n$ , there are exactly  $r$  solutions of  $x^r = 1$  in  $G$ . Hence the subgroup  $G(r)$  of  $r$ -th roots of unity in  $G$  has order  $r$ .
  - (ii) Show that for every number  $s$ , there are at most  $(s, n)$  solutions of  $x^s = 1$  in  $G$  (where  $(s, n)$  is the greatest common divisor of  $s$  and  $n$ ).
- 13.28. Show that if  $(G, *)$  is an abelian group of finite order  $n$  and is not cyclic, then there is some number  $m$  so that  $x^m = 1$  has more than  $m$  solutions in  $G$ .
- 13.29. Use the last two exercises to conclude that a finite abelian group  $G$  is cyclic if and only if for every number  $m > 0$ , the equation  $x^m = 1$  has at most  $m$  solutions in  $G$ .
- 13.30. Use the last exercise to show that if  $G$  is a finite cyclic group and  $H$  is a subgroup of  $G$ , then  $H$  is a cyclic group.
- 13.31. Let  $m = 241001 = 401 \cdot 601$ , a product of two prime numbers. If  $e = 7$  is an encrypting exponent for an RSA system with modulus  $m$ , find the smallest  $d > 1$  so that  $ed \equiv 1 \pmod{\phi(m)}$ . Then find the smallest  $d' > 1$  so that  $ed' \equiv 1 \pmod{\lambda(m)}$ .
- 13.32. In  $U_{73}$ , 5 is a primitive root. Find some  $x$  so that  $5^x \equiv 11 \pmod{73}$ , using the Pohlig-Hellman method:
  - Find a generator of the subgroup of  $U_{73}$  of order 8;
  - Find a generator of the subgroup of  $U_{73}$  of order 9.
  - Find a pair of congruences modulo 72 that  $x$  must satisfy. Then solve the congruences for  $x$ .
- 13.33. Eve intercepts the public data of Exercise 13.3, namely  $p = 89$ ,  $g = 3$ ,  $A = 55$  and  $B = 13$  that Alice and Bob sent to each other. She wants to find the secret key  $K$ . Help Eve find  $K$  by using the Baby Step-Giant Step algorithm to find  $\log_3(13)$ .
- 13.34. What is the maximum number of powers that the Baby Step-Giant Step algorithm would need to compute in order to find  $\log_5(3876)$  in Example 13.6?

The next exercise shows that using the cyclic group  $U_{p^e}$  for discrete logarithm cryptography is not appropriate for small primes  $p$ .

- 13.35. There is an explicitly computable  $p$ -adic logarithm function  $\log_p(1 + dp)$  for  $1 + dp$  in the cyclic subgroup  $H = \langle 1 + p \rangle$  of  $U_{p^e}$ , which has the property that if

$$(1 + dp)^t = 1 + sdp$$

in  $U_p$ , then

$$t = \frac{\log_p(1 + sdp)}{\log_p(1 + dp)}.$$

Given that function  $\log_p(-)$ , show that one can solve the discrete logarithm in  $U_{p^e}$  for small  $p$  and large  $e$ , by a strategy somewhat analogous to the Baby Step-Giant Step method. The problem is: given a generator  $g$  of  $U_{p^e}$  and an element  $k$  in  $U_{p^e}$ , find the exponent  $e$  so that

$k = g^e$ . Solve it as follows:

- Let  $g$  be a generator of  $U_{p^e}$ . Show that  $g, g^2, \dots, g^{p-1}$  is a complete set of residues modulo  $p$ .
- Show that  $g^{p-1} = 1 + dp \pmod{p^e}$  with  $(d, p) = 1$ .
- Show that  $1 + dp$  generates the cyclic subgroup  $H$  of  $U_{p^e}$  of order  $p^{e-1}$ .

Let  $k$  be in  $U_{p^e}$ . Find  $\log_g(k)$  as follows:

- Show that there is a unique  $r$  with  $1 \leq r \leq p - 1$  so that

$$kg^{(p-1)-r} \equiv 1 \pmod{p}.$$

Then  $kg^{(p-1)-r} = 1 + sdp$  for some  $s$ . [To find  $r$ , just write down  $kg^{(p-1)-r}$  for  $r = 0, 1, \dots, (p-1)$  until you get a number  $\equiv 1 \pmod{p}$ . This step is feasible if  $p$  is sufficiently small.]

- Use the  $p$ -adic logarithm function  $\log_p(1+x)$  for  $x$  a multiple of  $p$  to find  $t$  so that

$$1 + sdp = (1 + dp)^t = g^{(p-1)t}.$$

- Conclude that  $kg^{(p-1)-r} = g^{(p-1)t}$ , so

$$k = g^{(p-1)(t-1)+r}$$

and  $\log_g(k) = (p-1)(t-1) + r$ .

(The  $p$ -adic logarithm function is

$$\log_p(1+x) = \sum_{i=1}^{\infty} (-1)^{i-1} \frac{x^i}{i}.$$

If  $x = dp$  in  $U_{p^e}$ , then  $x^e = 0$ , so the sum is finite. See [Co00, 4.2.7, 4.2.8] for a discussion of the  $p$ -adic logarithm function).

- 13.36. To avoid the attack on RSA discussed just before the exercises in this chapter, explain why a preprocessing function should not preserve multiplication modulo  $m$ .
- 13.37. Suppose we construct an RSA cryptosystem with distinct prime numbers  $p$  and  $q$  and modulus  $m = pq$ . Let  $e$  be an encrypting exponent. Show that the smallest decrypting exponent for  $e$  is the number  $d'$  with  $0 < d' < \lambda(m)$  which is the inverse of  $e$  modulo  $\lambda(m)$ .
- 13.38. (i) Suppose  $p$  and  $q$  are safeprimes,  $m = pq$  and we construct an RSA cryptosystem with modulus  $m$  and encrypting exponent  $e$ . Show that  $\phi(m) = 2\lambda(m)$ .  
(ii) If  $d'$  is the smallest decrypting exponent (as in Exercise 13.37) for the cryptosystem in (i) and  $d$  is the decrypting exponent found by solving  $ed = 1 \pmod{\phi(m)}$ , show that  $d = d'$  or  $d = d' + \lambda(m)$ .

# Chapter 14

## Applications of Cosets



In Chapter 10 we defined a (left) coset of a subgroup  $H$  of a finite group  $G$ . We showed that

- $G$  splits up into a disjoint union of cosets of  $H$
- Each coset has the same number of elements as  $H$ .

Defining the index of  $H$  in  $G$  to be the number of distinct cosets of  $H$  in  $G$  these two facts give the counting formula:

$$(\text{the order of } H \text{ times} (\text{the index of } H \text{ in } G) = (\text{the order of } G),$$

which is Lagrange's Theorem, and implies that the order of any subgroup of  $G$  divides the order of  $G$ .

In this chapter we use the idea of cosets, and the counting formula obtained from looking at cosets, in several settings: solutions of non-homogeneous equations, Hamming codes, an alternative proof of Euler's Theorem, factoring of Carmichael numbers. These ideas have application to issues related to primality testing: in Section 14.5 we prove a weak version of Rabin's Theorem that repeated use of the strong  $a$ -pseudoprime test for randomly chosen  $a$  on an odd composite number  $m$  will, with very high probability, prove that  $m$  is composite. And in Section 14.6 we prove Boneh's Theorem on the security of RSA: in an RSA cryptosystem with modulus  $m$  and encrypting exponent  $e$ , if Eve can find any decrypting exponent, then, with very high probability, she can factor  $m$ .

These results hopefully support the idea that the concepts of group, subgroup and cosets can contribute useful insights in number theory, cryptography and error correction.

All of the groups considered in this chapter are abelian, so every left coset  $a * H$  is, as a subset of  $G$ , equal to the right coset  $H * a$ . So we omit “left” when discussing cosets.

### 14.1 Group Homomorphisms, Cosets and Non-homogeneous Equations

We begin this chapter with some general observations about cosets, Lagrange's Theorem, and homomorphisms.

We recall some definitions from Section 12.5.

A function  $f$  from a group  $G$  to a group  $H$  is a group homomorphism if

$$f(g * g') = f(g) * f(g')$$

(where we call the operations in both  $G$  and  $H$  by  $*$ ) and  $f$  sends the identity element  $e_G$  of  $G$  to the identity element  $e_H$  of  $H$ .

Associated to the homomorphism  $f$  is the kernel of  $f$ ,

$$K = \{g \text{ in } G : f(g) = e_H\}.$$

Since  $f$  is a homomorphism,  $K$  is a subgroup of  $G$ . The homomorphism  $f$  is a one-to-one function if and only if  $K$  contains only the identity element  $e_G$  of  $G$ .

The range of  $f$  is the subset  $f(G)$  of  $H$  consisting of all  $h$  in  $H$  so that  $h = f(g)$  for some  $g$  in  $G$ . Connecting these ideas with cosets, we have:

**Proposition 14.1** *Let  $G$  be a finite group and let  $f : G \rightarrow H$  be a homomorphism with kernel  $K$ . Then  $f$  induces a bijection  $\bar{f}$  from the set  $G/K$  of cosets of  $K$  in  $G$  to the range  $f(G)$  of  $f$ , by the correspondence:*

$$\bar{f}(g * K) = f(g).$$

This proposition is the analogue for group homomorphisms of Proposition 12.12, part of the Fundamental Homomorphism Theorem, Theorem 12.13 for ring homomorphisms. The only thing missing here that is in the Fundamental Theorem is the idea that the set of cosets of  $K$  in  $G$  is a group and  $\bar{f} : G/K \rightarrow f(G)$  is a ring homomorphism. See Remark 14.7 at the end of this section.

Here is how these ideas relate to equations.

Let  $f : G \rightarrow H$  be a group homomorphism. Suppose we ask: for  $h$  in  $H$ , is there some  $g_0$  so that  $f(g_0) = h$ ? That is the same as asking, is there a solution in  $G$  to the equation  $f(x) = h$ . Then, suppose we've found some  $g_0$  in  $G$  so that  $f(g_0) = h$ . Can we find the set of all solutions of the equation  $f(x) = h$ ? How many solutions of  $f(x) = h$  are there? And finally, for how many  $h$  in  $H$  is there a solution of  $f(x) = h$ ? That is, what is the size of the range of  $f$ ?

We can answer these questions.

**Corollary 14.2** *Let  $f : G \rightarrow H$  be a homomorphism of finite groups. Let  $K$  be the kernel of  $f$ .*

- (i) *The set of solutions  $x$  of  $G$  with  $f(x) = e$  is the kernel  $K$ .*
- (ii) *If  $h$  in  $H$  is in the range of  $f$ , so that  $h = f(g_0)$  for some  $g_0$  in  $G$ , then the set of solutions of the equation  $f(x) = h$  is the coset  $g_0 * K$ . Hence the number of solutions of  $f(x) = h$  is equal to the order of the kernel  $K$ .*
- (iii) *The number of elements in the range  $f(G)$  of  $f$  is equal to the order of  $G$  divided by the order of the kernel  $K$  of  $f$ .*

Fact (i) just restates Proposition 14.1.

Fact (ii) is given by Proposition 10.30, a key step in the proof of Lagrange's Theorem.

Fact (iii) is a consequence of Lagrange's Theorem and the one-to-one correspondence of Proposition 14.1.

Let's see how these facts relate to the examples of group homomorphisms introduced in Section 12.5.

**Additive groups.** Let  $f_a : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$  be the “multiplication by  $a$ ” homomorphism:  $f_a(x) = ax$ . Then  $f_a$  is a homomorphism from the additive group  $(\mathbb{Z}_m, +)$  to  $(\mathbb{Z}_m, +)$ .

The kernel of  $f_a$  is  $K = \{x \text{ in } \mathbb{Z}_m : ax = 0\}$ . If  $d$  is the greatest common divisor of  $a$  and  $m$ , and  $dm' = m$ , then the kernel of  $f_a$  is the set

$$\{m', 2m', \dots, dm' = m = 0\}$$

of multiples of  $m'$  in  $\mathbb{Z}_m$ . So the kernel has order  $d$ .

Letting  $da' = a$ , the range of  $f_a$  is the set

$$\{a, 2a, \dots\}$$

of multiples of  $a$  in  $\mathbb{Z}_m$ .

Since the range of  $f_a$  is equal to the number of cosets of the kernel  $K$ , Lagrange's Theorem says that there are  $m' = m/d$  multiples of  $a$  in the range of  $f_a$ . So the range of  $f_a$  consists of

$$\{a, 2a, \dots, m'a = 0\}.$$

*Example 14.3* Since  $(12, 57) = 3$ , the solutions of

$$12x \equiv 0 \pmod{57}$$

are the three multiples of  $19 = 57/3$  modulo 57. So the kernel of  $f_{12} : \mathbb{Z}_{57} \rightarrow \mathbb{Z}_{57}$  is the additive subgroup

$$K = \{0, 19, 38\} \pmod{57}.$$

The range of  $f_{12}$  is the set of numbers  $b$  modulo 57 so that  $12x \equiv b \pmod{57}$ , so the range is the set of nineteen multiples of 12 modulo 57. So the order of  $K$ , multiplied by the number of numbers in the range of  $f_{12}$ , is equal to the order of  $\mathbb{Z}_{57}$ :  $3 \cdot 19 = 57$ .

Now 42 is in the range of  $f_{12}$ , since  $12 \cdot 13 \equiv 42 \pmod{57}$ . Since the kernel  $K$  has three elements, by Corollary 14.2(iii), there are three solutions of  $12x \equiv 42 \pmod{57}$ , namely  $13 = 13 + 0$ ,  $32 = 13 + 19$  and  $51 = 13 + 38$ .

**Groups of units.** For the group  $U_m$  of units modulo  $m$ , the analogue of the homomorphism  $f_a$  is the “raise to the  $e$ -th power” homomorphism  $g_e : U_m \rightarrow U_m$  given by  $g_e(x) = x^e \pmod{m}$ .

The kernel of  $g$  is the set of units  $b$  in  $U_m$  that satisfy

$$b^e \equiv 1 \pmod{m}.$$

This set of units is the group  $U_m(e)$  of  $e$ -th roots of unity in  $U_m$ .

Here, the application of Corollary 14.2(i) is:

Let  $c$  be in  $U_m$ . If  $c = b^e$  is an  $e$ -th power in  $U_m$ , then the set of solutions in  $U_m$  to the equation  $x^e = c$  is the coset

$$bU_m(e) = \{bh \mid h \text{ in } U_m(e)\}.$$

And Corollary 14.2(iii) says that the number of  $e$ -th powers in  $U_m$  is equal to  $\phi(m)$ , the order of  $U_m$ , divided by the number of  $e$ -th roots of unity in  $U_m$ .

*Example 14.4* Let  $G = U_{29}$  and let  $g_7 : G \rightarrow G$  given by  $g_7(x) = x^7$ . Then the kernel of  $g_7$  is

$$K = U_{29}(7) = \{a \in U_{29} \mid a^7 = 1\} = U_{29}(7).$$

To find  $K$  we can verify that 2 is a primitive root modulo 29 (since  $2^4 \equiv 16$ ,  $2^7 \equiv 12$  and  $2^{14} \equiv 144 \equiv -1 \pmod{29}$ ). So, since  $U_{29}$  has  $28 = 4 \cdot 7$  elements, the kernel of  $g_7$  consists of the seven 4th powers in  $U_{29}$ :

$$K = U_{29}(7) = \{2^{4k} \mid 0 \leq k \leq 6\} = \{16, 24, 7, 25, 23, 20, 1\}.$$

The range of  $g_7$  consists of the 7th powers in  $U_{29}$ , namely,  $2^7, 2^{14}, 2^{21}, 2^{28}$ . So Corollary 14.2(ii) is confirmed here:  $4 \cdot 7 = 28 = \phi(29)$ .

Since  $2^7 \equiv 12 \pmod{29}$ , Corollary 14.2(i) says that there are seven solutions of  $x^7 \equiv 12 \pmod{29}$ , namely, the numbers in the coset

$$2U_{29}(7) = \{3, 19, 14, 21, 17, 11, 2\}.$$

Then Proposition 14.1 gives a one-to-one correspondence  $\overline{g_7}$  from cosets of  $U_{29}(7)$  to the range of  $g_7$ . The cosets of  $U_{29}(7)$  are the cosets  $2H, 4H, 8H$  and  $1H = H$ , which are mapped by  $\overline{g_7}$  to the four seventh powers  $2^7 = 12, 4^7 = 2^{14} = -1, 8^7 = 2^{21} = -12$  and  $1^7 = 1$ , respectively.

Corollary 14.2(ii) is a bit less obvious when  $U_m$  is not cyclic.

*Example 14.5* Consider  $U_{15} = \{1, 2, 4, 7, -7, -4, -2, -1\}$ . Let  $g_e$  be the  $e$ -th power map on  $U_{15}$ . Then the kernel of  $g_e$  is the subgroup  $U_{15}(e)$  of  $e$ -th roots of unity. To see what  $U_{15}(e)$  looks like for small  $e$ , we write down a table of the powers of elements of  $U_{15}$ :

	1	2	3	4	5
1	1	1	1	1	1
2	2	4	-7	1	2
4	4	1	4	1	4
7	7	4	-2	1	7
-7	-7	4	2	1	-7
-4	-4	1	-4	1	-4
-2	-2	4	7	1	-2
-1	-1	1	-1	1	-1.

We get the following counts, illustrating Corollary 14.2(ii):

$$\#G = \#\{\text{eth powers in } G\} \times \#\{\text{eth roots of unity in } G\}.$$

$e$	$\#U_{15}(e)$	# eth powers
1	1	8
2	4	2
3	1	8
4	8	1
5	1	8.

**Linear transformations over  $\mathbb{F}_p$ .** For a third class of examples, we look at a well-known result in elementary linear algebra.

Let  $T : V \rightarrow W$  be a linear transformation  $T : V \rightarrow W$  from a vector space  $V$  of dimension  $n$  to a vector space  $W$  of dimension  $m$ . Then the dimension of the null space of  $T$  plus the dimension of the range of  $T$  is equal to the dimension of  $V$ .

In linear algebra textbooks, this is called “... one of the most important results in linear algebra,” (Hoffman and Kunze) [HK71]. It is half of what is called “The Fundamental Theorem of Linear Algebra” (Strang)[St06].

For those familiar with the reduced row echelon form of a matrix, here is a concrete way to see why this result is true.

Let  $F$  be a field, let  $V, W$  be  $F$ -vector spaces of dimensions  $n, m$ , respectively. If we choose some bases for  $V$  and  $W$ , then with respect to those bases,  $V$  and  $W$  are represented as the vector spaces  $F^n, F^m$ , respectively, of column vectors with entries in  $F$ , and  $T$  is represented as multiplication of vectors in  $F^n$  by an  $m \times n$  matrix  $\mathbf{A}$  with entries in the field  $F$ . If we choose suitable bases of  $V$  and  $W$  we can assume that  $\mathbf{A}$  is in reduced row echelon form with columns  $\mathbf{c}_1, \dots, \mathbf{c}_n$ .

Since  $\mathbf{Av} = v_1\mathbf{c}_1 + \dots + v_n\mathbf{c}_n$  (see Chapter 7), the range of  $\mathbf{A}$  is equal to the subspace of  $F^m$  spanned by the columns of  $\mathbf{A}$ .

The columns of  $\mathbf{A}$  containing the leading ones form a basis of the column space of  $\mathbf{A}$ . So the dimension of the range of  $\mathbf{A}$  is equal to the number of columns with leading ones.

The dimension of the null space is equal to the number of columns of  $\mathbf{A}$  without leading ones, which equals the number of free variables in the system of equations corresponding to  $\mathbf{Av} = 0$ .

The number of columns with leading ones plus the number of columns without leading ones is equal to  $n$ , the number of columns of  $\mathbf{A}$ . So the dimension of the column space plus the dimension of the null space = the dimension of  $V$ , the domain of  $T$ .

To see how closely related Lagrange's Theorem is to the linear algebra theorem, we prove:

**Theorem 14.6** *Let  $p$  be prime and let  $\mathbb{F}_p$  be the field  $\mathbb{Z}_p$  of  $p$  elements. Let  $T : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^m$  be a linear transformation. Then the dimension of the null space of  $T$  + the dimension of the range of  $T = n$ .*

*Proof* Let  $G = \mathbb{F}_p^n$ , the domain of  $T$ . Then  $G$  is an abelian group under addition, and  $T$  is a group homomorphism from  $G$  to  $G' = \mathbb{F}_p^m$ .

Let  $K$  be the null space of  $T$ , namely, the set of solutions in  $G$  of  $T(\mathbf{u}) = 0$ . Viewing  $T$  as a group homomorphism from  $G$  to  $G'$ , the null space  $K$  of  $T$  is the kernel of  $T$ , a subgroup of  $G$ .

Let  $R \subset \mathbb{F}_p^m$  be the range of  $T$ :

$$R = \{\mathbf{y} \text{ in } \mathbb{F}_p^m : \text{there is some } \mathbf{x} \text{ in } \mathbb{F}_p^n \text{ so that } T(\mathbf{x}) = \mathbf{y}\}.$$

Then Corollary 14.2(i) says that for each  $\mathbf{y}$  in  $R$ , the set of solutions  $\mathbf{x}$  of  $T\mathbf{x} = \mathbf{y}$  is a coset of  $K$ , because if  $T(\mathbf{x}_1) = \mathbf{y}$ , then for every  $\mathbf{u}$  in  $K$  (and for no other vectors in  $G$ ),  $T(\mathbf{x}_1 + \mathbf{u}) = \mathbf{y}$ . So, as in Proposition 14.1, the homomorphism  $T$  induces a bijection from the cosets of  $K$  in  $G$  onto  $R$ .

Corollary 14.2(iii) says that the order of the null space  $K$ , times the number of vectors in the range  $R$ , is equal to the order of  $G$ .

Since the dimension of  $G$  is  $n$ ,  $G$  has  $p^n$  elements. Since  $K$  is a subgroup of  $G$ ,  $K$  has  $p^k$  elements for some  $k \leq n$ , so has dimension  $k$  as a vector space. By Lagrange's Theorem, the number of cosets of  $K$  in  $G$  is  $p^n/p^k = p^{n-k}$ . The number of cosets of  $K$  in  $G$  is equal to the number of elements of the range  $R$  of  $T$ . Since  $R$  is a subspace of  $\mathbb{F}_p^m$ , it has a dimension, and that dimension must be  $n - k$ . The theorem follows.  $\square$

Corollary 14.2(i) may be interpreted in the linear algebra setting as follows. Let  $T : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^m$  be multiplication by an  $m \times n$  matrix  $\mathbf{A}$ . Let  $\mathbf{w}$  be in the range of  $\mathbf{A}$ , so that there is a vector  $\mathbf{v}_0$  in  $\mathbb{F}_p^n$  so that  $\mathbf{Av}_0 = \mathbf{w}$ . Then the set of vectors  $\mathbf{v}$  in  $\mathbb{F}_p^n$  so that  $\mathbf{Av} = \mathbf{w}$  is the set of vectors of the form  $\mathbf{v}_0 + \mathbf{u}$  where  $\mathbf{Au} = 0$ . In linear algebra language: any solution of  $\mathbf{Av} = \mathbf{w}$  is a particular solution  $\mathbf{v}_0$  of  $\mathbf{Av} = \mathbf{w}$  plus any solution of the corresponding homogeneous equation  $\mathbf{Au} = 0$ .

We'll see an application of these results for Hamming codes in the next section.

Lagrange's Theorem is a result on counting finite sets, so it applies only to linear transformations on vector spaces of finite dimension over fields with finitely many elements. It doesn't show up in a course on elementary linear algebra because those courses usually assume that the field is the field of real numbers.

*Remark 14.7* In general, a subgroup  $W$  of a vector space  $V$  over a field such as the real numbers is usually not a subspace of  $V$ , because a subgroup of  $W$  need not be closed under scalar multiplication. For example, let  $V = \mathbb{R}^1$ , and view  $V$  as the set of points on the real line. Consider the cyclic subgroup  $H$  generated by 1. Then  $H$  consists of all vectors obtained from 1 and  $-1$  by addition, and hence consists of the set of integers, which visually looks like a collection of points spread out one unit apart on the real line. If you multiply an element of  $H$  by a real number such as  $1/2$  or  $\sqrt{2}$ , you don't get an element of  $H$ . So  $H$  is not closed under scalar multiplication.

But if the field of scalars of a vector space is the field  $\mathbb{F}_p = \mathbb{Z}_p$ , then scalar multiplication by an element of  $\mathbb{F}_p$  can be achieved by addition. Viewing  $\mathbb{F}_p$  as the set of integers modulo  $p$ , if  $r$  is an element of  $\mathbb{F}_p$  with  $1 \leq r \leq p$ , then, using distributivity, for  $\bar{v}$  in  $V$ ,

$$\begin{aligned} r\bar{v} &= (1 + 1 + \dots + 1)\bar{v} \\ &= 1 \cdot \bar{v} + 1 \cdot \bar{v} + \dots + 1 \cdot \bar{v} \quad (r \text{ summands}) \\ &= \bar{v} + \bar{v} + \dots + \bar{v}. \end{aligned}$$

Thus for vector spaces  $V$  over  $\mathbb{F}_p$ , subgroups  $H$  of  $V$  are closed under scalar multiplication, so are subspaces of  $V$ .

Note however that for every field  $F$  other than  $F = \mathbb{F}_p$  for  $p$  prime, non-zero vector spaces over  $F$  have subgroups that are not subspaces.

Similarly, the concepts of ideal and subgroup (under addition) coincide for the ring of integers  $\mathbb{Z}$ , but for no other rings except for the rings  $\mathbb{Z}_m$  for all  $m$ .

*Remark 14.8* Proposition 14.1 stated that if  $G$  is a finite group and  $f : G \rightarrow H$  is a group homomorphism with kernel  $K$ , then  $f$  induces a bijection  $\bar{f}$  from the set of cosets of  $K$  in  $G$  onto the range of  $f$  in  $H$ .

The only thing that made Proposition 14.1 different from the Fundamental Homomorphism Theorem, Theorem 12.13, is that there was no discussion of  $\bar{f}$  as a homomorphism.

In Section 12.6 we introduced the concept of normal subgroup: a subgroup  $K$  of a group  $G$  is a normal subgroup of  $G$  if for every  $a$  in  $G$ ,  $a * K = K * a$ : in words, every left coset is a right coset (and every right coset is a left coset). If  $K$  is a normal subgroup of  $G$ , then the set  $G/K$  of left cosets of  $K$  in  $G$  is a group, as noted in Section 12.6.

In fact, if  $f : G \rightarrow H$  is a group homomorphism with kernel  $K$ , then  $K$  is a normal subgroup of  $G$  (as is easily proved). Then the bijection  $\bar{f}$  from the set  $G/K$  of cosets to the range  $f(G) \subseteq H$  of  $f$  is also a group homomorphism (also easily proved), and hence  $\bar{f} : G/K \rightarrow f(G)$  is an isomorphism of groups. This result is sometimes known as the First Isomorphism Theorem for groups. See, for example, [DF99], Theorem 16, page 98.

## 14.2 On Hamming Codes

We look at the Hamming (8,4) error-correcting code from Chapter 7 that corrects one error and detects two errors. The numbers in this section are in  $\mathbb{F}_2 = \{0, 1\}$  (so  $1 + 1 = 0$  and  $-1 = 1$ ).

Recall that Alice wishes to send Bob the information word  $\mathbf{W} = (a, b, c, d)$ . To encode, Alice constructs

$$\mathbf{C} = \begin{pmatrix} w \\ x \\ y \\ a \\ z \\ b \\ c \\ d \end{pmatrix}$$

where the redundant digits  $w, x, y, z$  satisfy the equations

$$\begin{aligned} w + a + b + c &= 0 \\ x + a + b + d &= 0, \\ y + a + c + d &= 0, \\ z + b + c + d &= 0. \end{aligned}$$

The code vectors  $\mathbf{C}$  are the vectors that satisfy the equation  $\mathbf{H}\mathbf{C} = \mathbf{0}$ , where

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

We can view this situation in terms of groups.

The set of all column vectors with 8 components from the field  $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$  forms a group under addition, with  $2^8 = 256$  elements, which we'll denote by  $\mathbb{F}_2^8$ .

Since there are  $2^4 = 16$  information words, there are 16 code vectors. They are characterized by the property that  $\mathbf{H}\mathbf{C} = \mathbf{0}$ . If  $T : \mathbb{F}_2^8 \rightarrow \mathbb{F}_2^4$  is the group homomorphism given by multiplication by the matrix  $H$ , then the set  $\mathcal{C}$  of code vectors of the (8-4) code is the kernel of  $T$ .

By Lagrange's Theorem, there are  $256/16 = 16$  cosets of  $\mathcal{C}$  in  $\mathbb{F}_2^8$ .

Suppose Alice sends a code vector to Bob, and Bob receives  $\mathbf{R}$ . Bob wants to decide which code vector Alice sent. So he wants to find an error vector  $\mathbf{E}$  so that

- $\mathbf{R} + \mathbf{E} = \mathbf{C}$  is a code vector, and
- $\mathbf{E}$  contains the fewest possible 1's.

Recall that the reason for the second condition is the assumption that when Alice transmits a code vector  $\mathbf{C}$  to Bob and Bob receives  $\mathbf{R}$ , then each error is independently unlikely, so more errors are less likely than fewer errors. Each 1 in the error vector  $\mathbf{E} = \mathbf{C} - \mathbf{R}$  corresponds to an error, a bit of  $\mathbf{C}$  that was changed in the transmission of  $\mathbf{C}$  to get  $\mathbf{R}$ .

One way for Bob to decide on  $\mathbf{C}$ , given  $\mathbf{R}$ , is to observe that:

**Proposition 14.9** *The coset of the subgroup  $\mathcal{C}$  that contains the received vector  $\mathbf{R}$  contains all of the possible error vectors for  $\mathbf{R}$ .*

*Proof* The coset of the code subgroup  $\mathcal{C}$  containing  $\mathbf{R}$  consists of all 16 vectors of the form  $\mathbf{R} + \mathbf{C}$  for  $\mathbf{C}$  in  $\mathcal{C}$ . If  $\mathbf{E}$  is a vector in the coset of  $\mathbf{R}$ , then  $\mathbf{E} = \mathbf{R} + \mathbf{C}$ , so  $\mathbf{R} = \mathbf{C} + \mathbf{E}$  (operations are mod 2, so  $+ = -$ ), so  $\mathbf{E}$  is a possible error vector. (Note that the zero vector is in  $\mathcal{C}$ , so  $\mathbf{R}$  itself is a possible error vector.)

If  $\mathbf{V}$  is a vector in any coset of  $\mathcal{C}$  other than the one containing  $\mathbf{R}$ , then  $\mathbf{R} - \mathbf{V}$  is not in  $\mathcal{C}$ , which means that  $\mathbf{R} - \mathbf{V}$  is not a code vector. Hence  $\mathbf{V}$  cannot be an error vector for  $\mathbf{R}$ .  $\square$

Suppose Bob receives  $\mathbf{R}$ . One (inefficient) way for Bob to determine  $\mathbf{C}$ , given  $\mathbf{R}$ , is to look at the coset  $\mathbf{R} + \mathcal{C}$ , which contains all the possible error vectors, and pick the error vector with the fewest 1's. Of course the Hamming code is designed so that if there are no errors, then  $\mathbf{H}\mathbf{R} = \mathbf{0}$  and if there is one error, then  $\mathbf{H}\mathbf{R}$  is a column of  $\mathbf{H}$ : correcting the corresponding component of  $\mathbf{R}$  will yield the code word  $\mathbf{C}$ .

But what if  $\mathbf{H}\mathbf{R}$  is neither 0 nor a column of  $\mathbf{H}$ ? Then there are at least two errors in  $\mathbf{R}$ , and looking at the coset  $\mathbf{R} + \mathcal{C}$  can be useful.

*Example 14.10* Suppose that  $\mathbf{R} = (0, 0, 0, 1, 1, 1, 0, 1)$ . Then

$$\mathbf{H}\mathbf{R} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix},$$

which is not a column of  $\mathbf{H}$ . So  $\mathbf{R}$  contains an even number of errors.

To decide how to decode, Bob can look at the coset  $\mathbf{R} + \mathcal{C}$  to see which error vector has the fewest ones. Writing down the sixteen vectors in  $\mathcal{C}$  and adding  $\mathbf{R}$  to each gives the sixteen vectors in  $\mathbf{R} + \mathcal{C}$ . They are the columns of the matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

As can be seen, the vector  $\mathbf{R}$  is in this coset, the tenth vector from the left.

Each of the vectors in the coset of  $\mathbf{R}$  could be a possible error vector  $\mathbf{E}$  for  $\mathbf{R}$ . To decode  $\mathbf{R}$ , we would choose the error vector  $\mathbf{E}$  in the coset of  $\mathbf{R}$  with the fewest 1's. But inspecting the coset vectors, we find four error vectors with two 1's:

$$\begin{aligned} &(1 & 0 & 0 & 0 & 0 & 1 & 0 & 0)^T \\ &(0 & 1 & 0 & 0 & 1 & 0 & 0 & 0)^T \\ &(0 & 0 & 0 & 1 & 0 & 0 & 1 & 0)^T \\ &(0 & 0 & 1 & 0 & 0 & 0 & 0 & 1)^T. \end{aligned}$$

Adding any of these to  $\mathbf{R}$  would give a code vector, and each code vector is two errors from  $\mathbf{R}$ . So Bob can only guess the correct way to decode  $\mathbf{R}$ .

This example shows explicitly why the Hamming (8,4) code cannot correct a received vector with two errors.

### 14.3 Euler's Theorem

Returning to groups of units  $U_m$  and cosets of  $U_m$ , the idea of cosets gives a deceptively quick proof of Euler's Theorem:

**Theorem 14.11** Let  $m \geq 2$  and let  $b$  be an integer coprime to  $m$ . Then

$$b^{\phi(m)} \equiv 1 \pmod{m}.$$

*Proof* Since  $U_m$  is an abelian group, multiplication in  $U_m$  is associative and commutative, that is, for all  $a, b, c$  in  $U_m$ ,  $a(bc) = (ab)c$ , and  $ab = ba$ . That implies that given any set  $a_1, \dots, a_n$  of elements of  $U_m$ , the elements  $a_1(a_2(\dots(a_{n-1}a_n)\dots))$  and  $a_{i_1}a_{i_2}\dots a_{i_n}$  are equal, where the set  $\{a_{i_1}, a_{i_2}, \dots, a_{i_n}\}$  is just the set  $\{a_1, a_2, \dots, a_n\}$  in a different order and the second product is associated any way we wish. This is a consequence of Generalized Associativity—any two ways of associating a product of  $n$  elements of a group give the same result, and Generalized Commutativity—all possible products of  $n$  elements of a group are the same no matter how they are ordered in the product.

Generalized Associativity and Commutativity can be proved by induction, but require some care. For proofs, see [Ja85, Section 1.4].

To prove Euler's Theorem, that  $b^{\phi(m)} = 1$  for every element  $b$  of  $U_m$ , the idea is to look at  $U_m$  as a subgroup of itself. Then  $U_m$  has only one coset, which can be represented by any element of  $U_m$ . So we represent that coset by  $b$ , and also by 1.

Then the cosets  $U_m = 1U_m$  and  $bU_m$  are equal. Let  $u_1, u_2, \dots, u_{\phi(m)}$  be the  $\phi(m)$  elements of  $U_m$ . Then the cosets

$$U_m = 1 \cdot U_m = \{u_1, u_2, \dots, u_{\phi(m)}\}$$

and

$$b \cdot U_m = \{bu_1, bu_2, \dots, bu_{\phi(m)}\}$$

both contain all of the elements of  $U_m$ .

So the product of all the elements of  $b \cdot U_m$ , written in the order as shown, is equal to the product of all the elements of  $U_m$ , in the order as shown:

$$bu_1 \cdot bu_2 \cdot \dots \cdot bu_{\phi(m)} = u_1 \cdot u_2 \cdot \dots \cdot u_{\phi(m)}.$$

Then we may rearrange the factors in the left side any way we want. So we move all the factors of  $b$  to the left. We obtain

$$b^{\phi(m)} \cdot u_1 \cdot u_2 \cdot \dots \cdot u_{\phi(m)} = u_1 \cdot u_2 \cdot \dots \cdot u_{\phi(m)}.$$

To finish the proof, we simply cancel the common factors  $u_1, \dots, u_{\phi(m)}$ . We're left with

$$b^{\phi(m)} = 1,$$

which is Euler's Theorem. □

This is a standard proof in many books in number theory, such as [NZ72].

There are several reasons why this proof of Euler's Theorem is not as desirable as the proof via Lagrange's Theorem.

One reason is that we just assumed that Generalized Associativity and Generalized Commutativity are true. If we included proofs of them, then the proof of Euler's Theorem would be much longer.

A second reason why our deceptively quick proof of Euler's Theorem is less desirable than Lagrange's Theorem proof is that it only implies that the order of an element of a group divides the order of the group. That fact implies that the order of a *cyclic* subgroup of  $G$  divides the order of  $G$ . But we also have a need to look at not necessarily cyclic subgroups of groups. For example, for  $m = pq$ , a product of two odd primes, then  $U_m$  is not cyclic, and there is no reason to believe that the subgroup of  $k$ -th roots of unity  $U_m(k)$  is a cyclic subgroup (and in fact it usually isn't, for example, for  $k = 2$  and  $m$  odd and composite). So the deceptively quick proof of Euler's Theorem is useless for showing that the order of  $U_m(2)$  divides  $\phi(m)$ , the order of  $U_m$ .

A third reason why our deceptively quick proof of Euler's Theorem is less desirable than the Lagrange's Theorem proof is that it doesn't work at all in a group  $G$  that is not abelian, such as the group  $GL_2(\mathbb{F}_2)$  mentioned in Section 10.7.

Finally, Lagrange's Theorem says that given a group and a subgroup, the group partitions into a disjoint union of cosets of the subgroup, and each coset has the same number of elements as the subgroup. As we've seen, this fact is interesting for reasons other than proving that the order of a subgroup divides the order of the group. We'll see this fact used in each of the next three sections of this chapter.

These are reasons why we hid the deceptively quick proof of Euler's Theorem in the middle of this chapter.

## 14.4 A Probabilistic Compositeness Test

The idea of cosets and the proof of Lagrange's theorem yields information on Fermat's theorem as a primality test (or, more accurately, as a test for compositeness).

Let  $m$  be an odd number  $> 2$ , and let  $U_m$  be the group of units of  $\mathbb{Z}_m$ . Then  $U_m$  is an abelian group containing  $\phi(m)$  elements.

Recall (from Chapter 10) that

$$U_m(m-1) = \{a \text{ in } U_m \mid a^{m-1} = 1\}$$

is the group of  $(m-1)$ -st roots of unity in  $\mathbb{Z}/m\mathbb{Z}$ . Then

$$U_m(m-1) = \{a \text{ in } U_m \mid m \text{ passes the } a\text{-pseudoprime test}\}.$$

Since  $U_m(m-1)$  is a subgroup of  $U_m$ , either  $U_m(m-1) = U_m$  or  $U_m(m-1) \neq U_m$  (obviously). The case  $U_m(m-1) = U_m$  always occurs if  $m$  is prime, by Fermat's theorem. A Carmichael number is a composite number  $m$  for which  $U_m(m-1) = U_m$ .

Each coset of  $U_m(m-1)$  has the same number of elements as  $U_m(m-1)$ .

Suppose  $m$  is not prime and also not Carmichael. Then  $U_m(m-1)$  is a proper subgroup of  $U_m$ , so it has at least two cosets in  $U_m$ . So at least half of the elements of  $U_m$  are not in  $U_m(m-1)$ . This implies that  $m$  will fail the  $a$ -pseudoprime test for at least half of the units modulo  $m$ . Since  $m$  will also fail the  $a$ -pseudoprime test for numbers  $a$  not coprime to  $m$  (why?), we have

**Proposition 14.12** *If  $m$  is not prime and not a Carmichael number, then  $m$  will fail the  $a$ -pseudoprime test for more than half of the numbers  $a$  with  $1 \leq a \leq m$ .*

This fact has practical significance for testing a number to see if it is composite. Suppose we have a number  $m$  which we wish to test. Pick, say, 20 numbers  $a$ ,  $1 < a < m$ , at random, and subject  $m$  to the  $a$ -pseudoprime test for each  $a$ .

- If  $m$  is prime,  $m$  will pass all of the  $a$ -pseudoprime tests.
- If  $m$  is Carmichael and all  $a$  are chosen coprime to  $m$ , then  $m$  will pass all of the  $a$ -pseudoprime tests.
- If  $m$  is composite and not Carmichael, then the chance that  $m$  passes the  $a$ -pseudoprime test for any single randomly chosen  $a$  is less than  $1/2$ . So the chance that  $m$  passes the  $a$ -pseudoprime test for all 20 randomly chosen numbers  $a$  is less than  $1/2^{20}$ , or less than one in a million.

Carmichael numbers are very scarce, compared to prime numbers. So, provided we are not so unlucky to have selected a Carmichael number  $m$  (or the use we have for  $m$  requires only that  $m$  be prime or Carmichael), this is a good probabilistic primality test, in the following sense. We have less than one chance in a million of being wrong if a number passes our 20  $a$ -pseudoprime tests, and based on that result we conclude that  $m$  is prime.

## 14.5 There Are No Strong Carmichael Numbers

In this section we prove a weak version of Rabin's Theorem [Rab80], stated as Theorem 9.11, that there are no “strong Carmichael numbers”. This means: if  $m$  is a Carmichael number, then  $m$  will fail the strong  $a$ -pseudoprime test for some number  $a$  coprime to  $m$ .

To do so, we first need to prove that Carmichael numbers are squarefree.

**Proposition 14.13** *Suppose  $m$  is odd and divisible by  $p^r$  for some prime  $p$  with  $r > 1$ . Then  $m$  is not a Carmichael number.*

*Proof* We find a number  $b$  coprime to  $m$  so that  $m$  is not a  $b$ -pseudoprime.

Write  $m = p^r q$  where  $r > 1$  and  $(p, q) = 1$ . (Here  $q$  could be = 1.) Then

$$U_m \cong U_{p^r} \times U_q$$

by Proposition 12.27, and  $U_{p^r}$  is cyclic of order  $p^{r-1}(p-1)$  by Exercise 13.17. Since  $r > 1$ ,  $U_{p^r}$  has an element of order  $p$ . So  $U_m$  has an element  $b$  of order  $p$ .

Then  $m$  is not a  $b$  pseudoprime. For if  $b^m \equiv 1 \pmod{m}$ , then since  $p$  is the order of  $b$ ,  $p$  would have to divide  $m - 1 = p^r q - 1$ , which is obviously not so. Thus  $m$  is not a Carmichael number.  $\square$

So if  $m$  is a Carmichael number, we can assume that  $m = q_1 q_2$ , where  $q_1$  and  $q_2$  are coprime, odd and squarefree.

Let  $m$  be an odd number. Then  $m - 1$  is even, so we write  $m - 1 = 2^f q$  where  $q$  is odd and  $f > 0$ . In the strong  $b$ -pseudoprime test for an odd number  $m$ , we take the unit  $b$  modulo  $m$  and suppose  $b^{m-1} \equiv 1 \pmod{m}$ . If there is some  $e$  with  $1 \leq e < f$  so that

$$\begin{aligned} b^{2^e q} &\equiv 1 \pmod{m} \text{ and} \\ b^{2^{e-1} q} &\not\equiv 1 \text{ or } -1 \pmod{m}, \end{aligned}$$

then 1, -1 and  $c = b^{2^{e-1} q}$  are three roots of the polynomial  $x^2 - 1$  in  $\mathbb{Z}_m$ , which implies by D'Alembert's Theorem (Chapter 6) that  $\mathbb{Z}_m$  is not a field, hence  $m$  is not prime.

With that setup, we have the following weak version of Rabin's Theorem:

**Theorem 14.14** *Let  $m = q_1 q_2$  be an odd Carmichael number (hence the two factors  $q_1$  and  $q_2$  of  $m$  are odd, squarefree and coprime). Then  $m$  fails the strong  $a$ -pseudoprime test for at least half of all elements  $a$  in  $U_m$ .*

Rabin's Theorem (Theorem 9.5) replaces “half” by “three-fourths”. The “three-fourths” is as large as possible: see Exercise 14.14.

*Proof* Since  $m$  is Carmichael, we know that  $U_m = U_m(m - 1)$ : that is,  $a^{m-1} \equiv 1 \pmod{m}$  for every  $a$  coprime to  $m$ . Since  $m$  is odd,

$$m - 1 = 2^f r$$

for some  $f \geq 1$  and odd  $r$ . Then  $U_m(r) \neq U_m$ , because  $-1$  is not in  $U_m(r)$  but is in  $U_m(m-1) = U_m$ . Let  $e \geq 1$  be the smallest number so that

$$U_m(2^e r) = U_m, \text{ while } U_m(2^{e-1} r) \neq U_m.$$

The idea of the proof is to find some unit  $b$  so that

$$b^{2^{e-1}r} \not\equiv 1 \text{ or } -1 \pmod{m}.$$

For as noted above, then  $m$  fails the strong  $b$ -pseudoprime test.

We have two cases. Both cases involve looking at cosets.

Case 1. Suppose no  $b$  in  $U_m$  has  $b^{2^{e-1}r} \equiv -1 \pmod{m}$ . Pick any  $b$  in  $U_m$  but not in  $U_m(2^{e-1}r)$  and let  $c = b^{2^{e-1}r}$ . Then  $c \not\equiv 1$ , and  $c \not\equiv -1 \pmod{m}$ , but  $c^2 = b^{2^e r} \equiv 1$  because  $U_m = U_m(2^e r)$ . So  $m$  fails the strong  $b$ -pseudoprime test.

Now  $U_m(2^{e-1}r)$  is a proper subgroup of  $U_m$ . So it has at least two cosets in  $U_m$ . For every number  $a$  in a coset of  $U_m(2^{e-1}r)$  other than the coset  $1 \cdot U_m(2^{e-1}r) = U_m(2^{e-1}r)$ ,  $m$  fails the strong  $a$ -pseudoprime test.

Thus in this case  $m$  fails the strong  $a$ -pseudoprime test for at least half of all elements of  $U_m$ .

Case 2. Let  $b$  in  $U_m$  satisfy  $b^{2^{e-1}r} \equiv -1 \pmod{m}$ . Then every unit  $c$  in  $U_m$  that satisfies  $c^{2^{e-1}r} \equiv -1 \pmod{m}$  is in the coset  $bU_m(2^{e-1}r)$  because

$$(cb^{-1})^{2^{e-1}r} \equiv 1 \pmod{m},$$

so  $cb^{-1}$  is in  $U_m(2^{e-1}r)$ , and  $c = b(cb^{-1})$ .

Recall that  $m = q_1 q_2$  with  $q_1, q_2$  coprime. By the Chinese Remainder Theorem, we can find a unique number  $s$  modulo  $m$  so that

$$\begin{aligned} s &\equiv 1 \pmod{q_1} \\ s &\equiv b \pmod{q_2}, \end{aligned}$$

and a unique number  $t$  modulo  $m$  so that

$$\begin{aligned} t &\equiv b \pmod{q_1} \\ t &\equiv 1 \pmod{q_2}. \end{aligned}$$

Then

$$s^{2^{e-1}r} \equiv 1 \pmod{q_1} \text{ and } s^{2^{e-1}r} \equiv b^{2^{e-1}r} \equiv -1 \pmod{q_2},$$

while

$$t^{2^{e-1}r} \equiv b^{2^{e-1}r} \equiv -1 \pmod{q_1} \text{ and } t^{2^{e-1}r} \equiv 1 \pmod{q_2}.$$

Then we have at least four pairwise disjoint cosets of the subgroup  $U_m(2^{e-1}r)$  of  $U_m$ , namely:

$$U_m(2^{e-1}r), bU_m(2^{e-1}r), sU_m(2^{e-1}r), \text{ and } tU_m(2^{e-1}r).$$

These four cosets are pairwise disjoint, because every number  $a$  in the first coset satisfies

$$a^{2^{e-1}r} \equiv 1 \pmod{q_1} \text{ and } a^{2^{e-1}r} \equiv 1 \pmod{q_2};$$

every number  $ba$  in the second coset satisfies

$$(ba)^{2^{e-1}r} \equiv -1 \pmod{q_1} \text{ and } (ba)^{2^{e-1}r} \equiv -1 \pmod{q_2};$$

every number  $sa$  in the third coset satisfies

$$(sa)^{2^{e-1}r} \equiv 1 \pmod{q_1} \text{ and } \equiv -1 \pmod{q_2},$$

so  $(sa)^{2^{e-1}r}$  is not congruent to 1 or  $-1$  modulo  $m$ ; and every number  $ta$  in the fourth coset satisfies

$$(ta)^{2^{e-1}r} \equiv -1 \pmod{q_1} \text{ and } \equiv 1 \pmod{q_2}.$$

so  $(ta)^{2^{e-1}r}$  is not congruent to 1 or  $-1$  modulo  $m$ .

If  $c$  in  $U_m$  satisfies  $c^{2^{e-1}r} \equiv 1 \pmod{m}$ , then  $c$  is in  $U_m(2^{e-1}r)$ ; and if  $c$  in  $U_m$  satisfies  $c^{2^{e-1}r} \equiv -1 \pmod{m}$ , then by Case 2,  $c$  is in  $bU_m(2^{e-1}r)$ . So only the two cosets  $U_m(2^{e-1}r)$  and  $bU_m(2^{e-1}r)$  contain elements  $a$  of  $U_m$  so that  $a^{2^{e-1}r} = 1$  or  $-1 \pmod{m}$ . The cosets of  $s$  and  $t$ , and any other cosets we didn't look at, all consist of elements  $a$  so that  $m$  fails the strong  $a$ -pseudoprime test.

Since every coset contains the same number of elements as  $U_m(2^{e-1}r)$ , at least half of the elements  $a$  of  $U_m$  have the property that  $m$  fails the strong  $a$ -pseudoprime test.

Thus in either case, the theorem is proved.  $\square$

## 14.6 Boneh's Theorem

In Chapter 9 we observed in an exercise that if Alice and Bob are communicating using an RSA cryptosystem with modulus  $m = pq$ , and Eve learns or can deduce  $\phi(m)$ , then she can factor the modulus  $m$ . In this section we prove a stronger result due to Dan Boneh, that given a public modulus  $m$  and a public encrypting exponent  $e$ , if an adversary, Eve, somehow obtains some decrypting exponent  $d$  for  $e$ , then Eve can factor  $m$  with very high probability.

We observed earlier that if  $m$  is a Carmichael number and  $m$  fails a strong  $a$ -pseudoprime test, then  $m$  is easy to factor. For suppose  $c$  is a number so that  $c$  is not congruent to 1 or  $-1 \pmod{m}$ , but  $c^2 \equiv 1 \pmod{m}$ . Then  $m$  divides  $c^2 - 1 = (c + 1)(c - 1)$  but doesn't divide  $c + 1$  or  $c - 1$ . So  $(m, c + 1)$  and  $(m, c - 1)$  are non-trivial proper factors of  $m$ .

This idea shows up in the method described in Boneh's Theorem:

**Theorem 14.15** Suppose given an RSA cryptosystem with public modulus  $m = pq$ , where  $p$  and  $q$  are secret odd primes, and public encrypting exponent  $e$ . Suppose an adversary, Eve, somehow obtains a decrypting exponent  $d$  so that  $w^{ed} \equiv w \pmod{m}$  for all integers  $w$ . Then with very high probability, Eve can factor  $m$ .

*Proof* Assume Eve knows  $m, e$  and some  $d$  so that

$$w^{ed} \equiv w \pmod{m}$$

for all numbers  $w$ . Then

$$w^{ed-1} \equiv 1 \pmod{m}$$

for every unit  $w$  of  $U_m$ . Set  $k = ed - 1$ , then  $U_m(k) = U_m$ . So  $k$  is a multiple of the exponent  $\lambda(m)$  of  $U_m = U_p \times U_q$ . Now  $\lambda(m)$  is even, because the order of  $-1$  divides  $\lambda(m)$ . So  $k$  is even. And Eve knows  $k$ . Write

$$k = 2^g r$$

with  $g \geq 1$  and  $r$  odd. Then  $U_m(2^g r) = U_m$ . But  $U_m(r) \neq U_m$ : in particular,  $(-1)^r = -1$ , so  $-1$  is not in  $U_m(r)$ .

So Eve picks random units  $w$  modulo  $m$  and computes

$$w^r, w^{2r}, \dots, w^{2^g r} = w^k = w^{ed-1} = 1.$$

If she finds some  $f$  with  $1 \leq f \leq g$  so that

$$c = w^{2^{f-1}r} \neq 1 \text{ or } -1$$

and

$$c^2 = w^{2^f r} = 1,$$

then  $c^2 \equiv 1 \pmod{m}$  and  $c \neq 1$  or  $-1$ , so  $(c+1, m)$  and  $(c-1, m)$  are non-trivial factors of  $m$ .

The proof will show that if Eve chooses  $n$  random numbers  $w$ , then the probability that Eve will not find some  $w$  and  $f$  so that  $c = w^{2^{f-1}r} \neq 1$  or  $-1$  and  $c^2 = w^{2^f r} = 1$  is less than  $\frac{1}{2^n}$ .

We know that  $U_m(2^g r) = U_m$  since  $2^g r = k = ed - 1$  and  $w^{ed-1} \equiv 1 \pmod{m}$  for all  $w$  in  $U_m$ .

Let  $f$  be the smallest exponent so that  $U_m(2^f r) = U_m$ . Then  $U_m(2^{r-1}r)$  is a proper subgroup of  $U_m$ . We then have two cases, as in the proof of Theorem 14.14.

Case 1. Suppose no  $b$  in  $U_m$  has  $b^{2^{f-1}r} \equiv -1 \pmod{m}$ . Let  $b$  be any element of  $U_m$  that is not in  $U_m(2^f r)$ , and let  $c = b^{2^{f-1}r}$ . Then  $c^2 \equiv 1$  but  $c \not\equiv 1$  or  $-1 \pmod{m}$ . So  $m$  divides  $c^2 - 1 = (c+1)(c-1)$ , but  $m$  does not divide  $c+1$  or  $c-1$ . Thus  $1 < (m, c+1) < m$  and  $1 < (m, c-1) < m$  are non-trivial divisors of  $m$ . Since they are coprime, one must be  $p$ , the other  $q$ .

Since  $U_m(2^{f-1}r)$  is a proper subgroup of  $U_m$ , at least half of the elements of  $U_m$  are not in  $U_m(2^{f-1}r)$  by Lagrange's Theorem. So if we choose elements out of  $U_m$  at random, the probability of choosing a number  $b$  in  $U_m(2^{f-1}r)$  that does not yield a factorization of  $m$  is  $\leq 1/2$ .

Case 2. Let  $b$  in  $U_m$  satisfy  $b^{2^{f-1}r} \equiv -1 \pmod{m}$ . Now  $m = pq$  with  $p, q$  distinct primes. So there is a unique number  $s$  modulo  $m$  so that

$$\begin{aligned} s &\equiv 1 \pmod{p} \\ s &\equiv b \pmod{q}, \end{aligned}$$

and there is a unique number  $t$  modulo  $m$  so that

$$\begin{aligned} t &\equiv b \pmod{p} \\ t &\equiv 1 \pmod{q}. \end{aligned}$$

Then

$$s^{2^{f-1}r} \equiv 1 \pmod{p}, s^{2^{f-1}r} \equiv -1 \pmod{q},$$

while

$$t^{2^{f-1}r} \equiv -1 \pmod{q}, t^{2^{f-1}r} \equiv 1 \pmod{p}.$$

Then, just as in the proof of Theorem 14.14, we have at least four pairwise disjoint cosets of the subgroup  $U_m(2^{f-1}r)$  of  $U_m$ , namely:

$$U_m(2^{f-1}r), bU_m(2^{f-1}r), sU_m(2^{f-1}r), \text{ and } tU_m(2^{f-1}r).$$

Thus in this case there are at least (in fact, exactly) four cosets of  $U_m(2^{f-1}r)$  in  $U_m$ . Only two of those cosets, namely  $U_m(2^{f-1}r)$  and  $bU_m(2^{f-1}r)$ , have elements  $a$  of  $U_m$  so that  $a^{2^{f-1}r} \equiv 1$  or  $-1 \pmod{m}$ . The other two cosets have elements  $a$  so that

$$a^{2^{f-1}r} \equiv c$$

and  $c$  satisfies  $c \equiv 1 \pmod{p}$ ,  $c \equiv -1 \pmod{q}$  or  $c \equiv -1 \pmod{p}$ ,  $c \equiv 1 \pmod{q}$ . Either way,  $c \not\equiv 1 \pmod{m}$  and  $c \not\equiv -1 \pmod{m}$ .

Each of the four cosets of  $U_m(2^{f-1}r)$  contains the same number of elements as  $U_m(2^{f-1}r)$ , and two of those cosets contain elements  $b$  so that  $b^{2^{f-1}r} = c$  where  $c \neq 1$  or  $-1$  modulo  $m$ , and hence yields a factorization of  $m$ . So in Case 2, as in Case 1, picking a random element out of  $U_m$  will fail to yield a factorization of  $m$  with probability  $= 1/2$ . So if we pick  $n$  elements  $b$  at random from  $U_m$  the probability is  $1/2^n$  that we will fail to find a number  $c \equiv b^{2^{f-1}r}$  that will yield a factorization of  $m$ . So in practice we will be able to factor  $m$ .  $\square$

The idea of factoring a number  $m$  by finding numbers  $b$  and  $a$  so that  $m$  divides  $b^2 - a^2$  but doesn't divide  $b + a$  or  $b - a$  will show up again in Chapter 16, and in a systematic fashion in Chapter 17.

Boneh's Theorem does not imply that the security of RSA is always assured as long as the modulus cannot be factored. See [BV98], or the discussions in Section 11.3(iii) or at the end of Section 13.10.

## Exercises

- 14.1. Without looking at Chapter 10, prove that if  $H$  is a subgroup of a finite group  $G$ , and  $a$  is in  $G$ , then the number of elements in the coset  $a * H$  is equal to the number of elements of  $H$ .
- 14.2. Let  $g_4$  be the “raise to the fourth power” homomorphism from  $U_{63}$  to  $U_{63}$ . Find the kernel of  $g_4$ . How many fourth powers are there in  $U_{63}$ ? (Hint: look at the kernel of  $g_4$  on  $U_7$  and on  $U_9$  and then use the CRT or Proposition 12.30.)
- 14.3. Do Example 14.5 with  $U_{21}$  and  $e \leq 6$ .
- 14.4. (i) Show that  $x = 11$  is a solution to

$$\begin{aligned} 6x &\equiv 26 \pmod{40} \\ 9x &\equiv 9 \pmod{30}. \end{aligned}$$

- (ii) Define the function  $f_{(6,9)} : \mathbb{Z} \rightarrow \mathbb{Z}_{40} \times \mathbb{Z}_{30}$  by  $f_{(6,9)}(x) = (6x, 9x)$ . Show that  $f_{(6,9)}$  is a group homomorphism from  $(\mathbb{Z}, +)$  to the group  $\mathbb{Z}_{40} \times \mathbb{Z}_{30}$  under componentwise addition (as in Section 12.6).
- (iii) Find the kernel of  $f_{(6,9)}$
- (iv) Show that every solution to the system of congruences in (i) can be written as  $x = 11 + t$  where  $t$  is an element of the kernel of  $f_{(6,9)}$ .
- 14.5. Generalize Exercise 14.4: if  $x_0$  is a solution to the pair of congruences

$$\begin{aligned} ax &\equiv b \pmod{m} \\ cx &\equiv d \pmod{n}, \end{aligned}$$

describe all solutions to the pair of congruences as a coset of the kernel of a homomorphism from  $\mathbb{Z}$  to  $\mathbb{Z}_m \times \mathbb{Z}_n$ .

- 14.6. In the Hamming (8, 4) code, let  $\mathbf{R} = (0, 1, 0, 0, 0, 0, 1, 0)^T$ .

Find the four code vectors that have a Hamming distance of 2 from  $\mathbf{R}$  by

(i) comparing  $\mathbf{R}$  with the list of code vectors found in Chapter 7;

(ii) Finding all ways to add two columns of the matrix  $\mathbf{H}$  to get the vector  $\mathbf{HR}$ .

- 14.7. A student came up with the following proof that for any modulus  $m \geq 2$  and any number  $a$  coprime to  $m$ ,

$$a^{m-1} \equiv 1 \pmod{m},$$

with the following steps:

(i) if  $(a, m) = 1$ , then  $\{a, 2a, \dots, (m-2)a, (m-1)a, ma\}$  is a complete set of representatives for  $\mathbb{Z}_m$ .

(ii) Since  $\{1, 2, \dots, m-2, m-1, m\}$  is also a complete set of representatives modulo  $m$ , we have (omitting  $m$  and  $ma$ )

$$a \cdot 2a \cdot \dots \cdot (m-2)a, (m-1)a \equiv 1 \cdot 2 \cdot \dots \cdot m-2 \cdot m-1 \pmod{m},$$

or, rearranging the left side,

$$a^{m-1} \cdot (m-1)! \equiv (m-1)! \pmod{m}.$$

Cancelling  $(m-1)!$  from both sides yields

$$a^{m-1} \equiv 1 \pmod{m}.$$

Write down some feedback for the student—praise, criticism, whatever you think is appropriate.

- 14.8. Show that the group of units  $U_{91}$  is the disjoint union of  $U_{91}(90)$  and  $2U_{91}(90)$ , where

$$2U_{91}(90) = \{a \in U_{91} \mid a^{90} = 64\}.$$

- 14.9. (i) Find  $a_1, a_2$  and  $a_3$  so that  $a_1^{10}, a_2^{10}$  and  $a_3^{10}$  are the three 10th powers in  $U_{31}$ .

(ii) Show that  $U_{31}(10) = \langle -2 \rangle$ .

(iii) Show the three cosets of  $U_{31}(10)$  are  $a_i \cdot U_{31}(10)$  where  $a_1, a_2$  and  $a_3$  are the three elements you found in (i).

- 14.10. Find some number  $e > 1$  dividing 30 so that the subgroup  $U_{77}(e)$  of  $U_{77}$  is not cyclic, and some number  $f > 1$  dividing 30 so that  $U_{77}(f)$  is cyclic. (Hint: use the isomorphism  $U_{77} \cong U_7 \times U_{11}$ .)

- 14.11. (i) Let  $m = 35$ . Find the four elements of  $U_m(2)$ .

(ii) Find all solutions to  $x^2 \equiv 14 \pmod{m}$ .

- 14.12. Suppose you found an RSA cryptosystem with  $(m, e) = (69841, 13)$  and you learned that  $d = 1777$  is a decrypting exponent. Use that information to factor  $m$  by the strategy in the proof of Boneh's Theorem.

- 14.13. Suppose Alice, a financial advisor, has two clients, Bob and Evan, on opposing sides of a family dispute. She uses the same RSA modulus  $m$  for both clients. To authenticate messages, Alice gives Bob a secret signature exponent  $d_B$  and Evan a secret signature exponent  $d_E$ , and makes public the modulus  $m$  and the corresponding decrypting exponents  $e_B$  and  $e_E$  (so that everyone in the family can know what the messages are and who sent them.) Explain how Evan can factor  $m$  and then send fraudulent orders in Bob's name [Del84].

The next exercise shows that the “three-fourths” in Rabin's Theorem (Theorem 9.5) cannot be increased.

- 14.14. The number  $8911 = 7 \cdot 19 \cdot 67$  is a Carmichael number, and  $8910 = 2 \cdot 4455$ .
- (i) Show that  $U_{8911}(2)$  has exactly eight elements: denote them by  $e_1, e_2, \dots, e_8$ , where  $e_1 = 1, e_2 = -1$ .
  - (ii) Show that for each  $e_i$  in  $U_{8911}(2)$ ,  $e_i^{4455} \equiv e_i \pmod{8911}$ .
  - (iii) Show that  $U_{8911}(4455)$  has index 8 in  $U_{8911}$ , and  $e_1, e_2, \dots, e_8$  are coset representatives for the eight cosets of  $U_{8911}(4455)$ .
  - (iv) Show that 8911 is a strong  $a$ -pseudoprime if and only if  $a$  is in the coset  $U_{8911}(4455)$  or the coset  $(-1)U_{8911}(4455)$ .
  - (v) Conclude that  $m = 8911$  is a strong  $a$ -pseudoprime for exactly one-fourth of the units modulo 8911.
- 14.15. (i) Show that Case 2 of the proof of Theorem 14.15 does not apply where  $m = 1105$ .
- (ii) Show that Case 2 of the proof does apply when  $m$  is a Carmichael number and  $\frac{m-1}{2}$  is odd (for example, when  $m = 8911$ ).

# Chapter 15

## An Introduction to Reed–Solomon Codes



This chapter introduces Reed–Solomon codes, first published in 1960 in a five page article by Irving Reed and Gustave Solomon [RS60]. Reed–Solomon codes are multiple error correcting codes defined over a finite field. They were used to protect communication from spacecraft starting in the late 1970s and were used in compact discs beginning in the early 1980s. They continue to be widely used in practice because of their effectiveness in dealing with bursts of errors.

There are several approaches to Reed–Solomon codes. In this chapter we adopt the original approach of the authors, in which encoding is done by taking a polynomial whose coefficients correspond to the plaintext word, and evaluating the polynomial at a fixed set of elements of the field to yield the code word. Decoding is done by the Welch–Berlekamp procedure, which takes the received word and solves a system of linear equations for the coefficients of two unknown polynomials. Dividing one polynomial by the other will give the original plaintext polynomial, provided that not too many errors occurred in the received word.

### 15.1 The Setting

Reed–Solomon codes can be defined over any sufficiently large finite field. In this chapter we’ll assume the field is  $F = \mathbb{F}_p = \mathbb{Z}_p$ , integers modulo a prime  $p$ . In Chapter 19 we’ll look at an example over a finite field with 8 elements.

Alice has a plaintext message, an  $m$ -tuple of elements of  $F$ . She encodes the message and sends it through a noisy channel to Bob. Bob retrieves the encoded message, with up to  $e$  errors in it. Because of the redundancy in Alice’s encoding, Bob is able to reconstruct Alice’s original plaintext message. (Bob could be Alice herself at a later point in time—the “sending” for Alice might be the storing of the data on an imperfect storage device for later retrieval.) How to encode and decode is what we’ll explain in this chapter.

We assume that the message we wish to encode is a sequence of bits (zeroes and ones). We need to convert the message into a sequence of elements of  $\mathbb{F}_p$ . A simple way is to find  $n$  so that  $2^n < p$  and split up the sequence of bits into a sequence of  $n$  bit words, which we then view as the base 2 representation of a number  $< p$ .

*Example 15.1* Suppose  $p = 257 = 2^8 + 1$  and the plaintext message is

100, 100, 101, 011, 000, 111, 111, 100, 000, 001, 001, 110, 100, 1

(where the commas are added only for readability.) Group the bits into sequences of eight bit words:

10010010, 10110001, 11111100, 00000100, 11101001.

View each eight-bit word as the base 2 representation of a number  $< 256$ :

$$\begin{aligned} 10010010 &\longleftrightarrow 128 + 16 + 2 = 146 \\ 10110001 &\longleftrightarrow 128 + 32 + 16 + 1 = 177 \\ 11111100 &\longleftrightarrow 128 + 64 + 32 + 16 + 8 + 4 = 252 \\ 00000100 &\longleftrightarrow 4 \\ 11101001 &\longleftrightarrow 128 + 64 + 32 + 8 + 1 = 233. \end{aligned}$$

The plaintext message is now the sequence of elements of  $\mathbb{F}_{257}$ :

$$146, 177, 252, 4, 233.$$

If the message is English text, we can convert it to a sequence of bits as described in Section 2.4.

Turning our message of bits into a sequence of elements of  $\mathbb{F}_{257}$  makes the Reed–Solomon code effective in correcting bursts of errors. A Reed–Solomon code corrects errors in messages made up of elements of the field, in this case  $\mathbb{F}_{257}$ . Errors occur to bits. When we view a sequence of seven-bit words as a sequence of elements of the field  $\mathbb{F}_{257}$ , then a cluster of errors to, say, 6 consecutive bits, does not count as 6 errors of elements of  $\mathbb{F}_{257}$ , but rather as one or two errors, depending on whether the consecutive erroneous bits all lie in the bit representation of a single element of  $\mathbb{F}_{257}$  in the message, or overlap between two consecutive elements of  $\mathbb{F}_{257}$  in the message.

A Hamming code, such as the Hamming (8, 4) code (Chapter 7), can detect two errors but can only correct one error per word. We estimated the probability that the Hamming code would be accurate in decoding, based on the assumption that the probability of an error in a given bit is independent of whether there is an error in an adjacent bit. But if that assumption is false—if, in fact, an error in one bit makes it more likely that an error will also occur in an adjacent bit, then a Hamming code would be less effective than claimed in Chapter 7.

By viewing a block of adjacent bits as a single element of the finite field, a Reed–Solomon code deals equally well with an isolated bit error in a block or with a cluster of several bit errors in the block. So Reed–Solomon codes are effective at correcting the kinds of errors that are likely to show up on compact discs. See Example 15.6 below for an example.

In fact, Reed–Solomon codes are built into the encoding on a compact disc. The data on a compact disc are encoded by a method called cross-interleaved Reed–Solomon coding. According to K. A. S. Immink [Im94], one of the inventors of the CD, the resulting coding “can completely correct error bursts up to 4000 bits, or about 2.5 mm on the disc surface. This code is so strong that most CD playback errors are almost certainly caused by tracking errors that cause the laser to jump track, not by uncorrectable error bursts.”

By 1993 Reed–Solomon codes had become “ubiquitous” [Ci93]. They continue to be important, for example for storing and recovering data in the “cloud”. Optimizing their performance in that setting is the subject of current research: see, for example, [GW16].

## 15.2 Encoding a Reed–Solomon Code

Let  $F$  be a field with  $q$  elements. Choose  $m$  and  $e$  so that  $m + 2e = n \leq q - 2$ . We construct a Reed–Solomon code that takes a plaintext word made up of  $m + 1$  elements of  $F$  and turns the word into a code word made up of  $n + 1$  elements of  $F$  in such a way that up to  $e$  errors in the code word can be corrected.

The parameters of a Reed–Solomon code are the field  $F$ , numbers  $m$  and  $e$ , and a set of  $n + 1$  distinct elements

$$a_0, a_1, \dots, a_n$$

of the field  $F$ .

Alice begins with a plaintext word, an  $m + 1$ -tuple

$$W = (w_0, w_1, \dots, w_m)$$

of elements of  $F$ . To encode  $W$  she forms the plaintext polynomial

$$W(x) = w_0 + w_1x + w_2x^2 + \dots + w_mx^m$$

of degree  $m$ , whose coefficients are the elements of the plaintext word. Then she evaluates  $W(x)$  at the  $n + 1$  prechosen elements  $a_0, a_1, \dots, a_n$  of  $F$  to obtain the code word

$$C = (C_0, \dots, C_n) = (W(a_0), W(a_1), W(a_2), \dots, W(a_n)).$$

of elements of  $F$ .

Alice sends the code word  $C$  to Bob.

Since Alice started with  $m + 1$  elements of  $F$ , the plaintext word, and ended up with  $n + 1 = m + 1 + 2e$  elements of  $F$ , the code word, she has added  $2e$  elements of redundancy to each word. The redundancy will enable Bob to find  $W(x)$  even in the presence of up to  $e$  errors.

*Example 15.2* Suppose the field is  $\mathbb{F}_p$  where  $p$  is some prime  $> 7$ . Let  $m = 2$ . Then Alice's message words are sequences of three numbers  $< p$  that she makes the coefficients of a polynomial  $W(x)$  of degree 2. Suppose we want to correct up to two errors in each word. Then  $e = 2$  and  $m + 2e = n = 6$  is the degree of the polynomial  $C(x)$ . A polynomial of degree 6 has 7 coefficients, so we need to evaluate the plaintext polynomial  $W(x)$  at seven distinct elements of  $F$ . To keep the numbers small in this example, we choose those seven elements of  $F$  to be the elements

$$(a_0, \dots, a_6) = (-3, -2, -1, 0, 1, 2, 3) \pmod{p}.$$

Alice wants to send the plaintext message YES. For this example, for convenience let us assume that  $p > 27$  and just convert letters to their place numbers in the alphabet, then view those numbers as elements of the field  $\mathbb{F}_p$ : thus YES becomes  $W = (25, 5, 19)$  modulo  $p$ . Alice forms the polynomial

$$W(x) = 25 + 5x + 19x^2$$

of degree  $m = 2$ . She evaluates  $W(x)$  at  $-3, -2, -1, 0, 1, 2, 3$  and forms the code vector with seven components, all defined modulo  $p$ :

$$\begin{aligned} C &= (W(-3), W(-2), W(-1), W(0), W(1), W(2), W(3)) \\ &= (181, 91, 39, 25, 49, 111, 211). \end{aligned}$$

She sends the vector  $C$  through a possibly noisy channel to Bob.

**Decoding a no-error code.** Before showing how to decode a Reed–Solomon code, we first look at the situation where we assume no errors and just want to recover  $W$ , given  $C$ . We let  $m = n$  and fix  $m + 1$  distinct elements  $a_0, a_1, \dots, a_m$  of  $F$ .

Suppose Alice has a message word

$$W = (w_0, w_1, \dots, w_m).$$

She constructs the plaintext polynomial

$$W(x) = w_0 + w_1x + \dots + w_mx^m,$$

and computes the code vector

$$C = (c_0, c_1, \dots, c_m)$$

by

$$c_0 = W(a_0), c_1 = W(a_1), \dots, c_m = W(a_m).$$

Given  $C = (c_0, c_1, \dots, c_m)$ , and assuming no errors, how would Bob recover  $W$  from  $C$ ? In other words, let  $W(x)$  be an unknown polynomial of degree  $m$ . If Bob knows the values of  $W(x)$  at  $m + 1$  points of the field  $F$ , how does he recover the coefficients  $w_0, w_1, \dots, w_m$  of  $W(x)$ ?

Bob writes down the equations that define the components of  $C$ :

$$\begin{aligned} W(a_0) &= w_0 + w_1a_0 + w_2a_0^2 + \dots + w_ma_0^m = c_0 \\ W(a_1) &= w_0 + w_1a_1 + w_2a_1^2 + \dots + w_ma_1^m = c_1 \\ &\vdots \\ W(a_m) &= w_0 + w_1a_m + w_2a_m^2 + \dots + w_ma_m^m = c_m. \end{aligned}$$

To find  $W$  from  $C$ , he lets

$$V = \begin{pmatrix} 1 & a_0 & a_0^2 & \dots & a_0^m \\ 1 & a_1 & a_1^2 & \dots & a_1^m \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_m & a_m^2 & \dots & a_m^m \end{pmatrix}$$

be the square matrix of known coefficients of this system of equations. Then in matrix form, the equations become

$$VW^T = C^T$$

(where the exponent  $T$  means “transpose”). The problem is then: given  $C$ , find  $W$ .

The coefficient matrix  $V$  is called a Vandermonde matrix. It is known that if  $a_0, \dots, a_m$  are distinct elements of the field  $F$ , then  $V$  is an invertible matrix.

So given the vector  $C$  of values of  $W(x)$  at  $x = a_0, a_1, \dots, a_m$ , there is a unique solution

$$W^T = V^{-1}C^T$$

of the matrix equation above for the vector  $W$  of coefficients of  $W(x)$ . So the plaintext message is uniquely determined from the encoded message. So in our no-error example, Bob can just find the inverse of  $V$ , the Vandermonde matrix of coefficients, and multiply  $V^{-1}C^T$  to recover  $W^T$ .

The Vandermonde matrix depends only on the numbers  $a_0, a_1, \dots, a_m$ . For  $m = 3$  and  $(a_0, a_1, a_2) = (1, 2, 3)$ , the Vandermonde matrix is

$$\begin{pmatrix} 1^0 & 1^1 & 1^2 \\ 2^0 & 2^1 & 2^2 \\ 3^0 & 3^1 & 3^2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix}$$

with inverse

$$\begin{pmatrix} 3 & -3 & 1 \\ -5 \cdot 2^{-1} & 4 & -3 \cdot 2^{-1} \\ 2^{-1} & -1 & 2^{-1} \end{pmatrix}$$

(where  $2^{-1}$  is the number  $(p + 1)/2$  in  $\mathbb{F}_p$ ).

Returning to the general situation, with errors, the fact that we have available not just  $m + 1$  values of  $W(x)$  but  $n + 1 = m + 1 + 2e$  values of  $W(x)$  adds redundancy, enough that even with  $e$  errors, that is, even if  $e$  of the components of  $C$  are changed in the process of being sent from Alice to Bob, Bob will still be able to determine  $W$ , as we now show.

### 15.3 Decoding

The approach we take to decoding is perhaps the easiest method to understand since, like the last example (where  $m = n$ ), decoding involves nothing more than solving a set of linear equations.

Let  $m + 2e = n$ , where  $e$  is the maximal number of errors the code can correct per word.

Recall that  $W(x)$  is the polynomial of degree  $m$  with coefficients formed from the plaintext word of Alice.

Alice has sent Bob the sequence

$$C = (W(a_0), W(a_1), W(a_2), \dots, W(a_n))$$

of elements of  $F$ , where  $n = m + 2e$ .

Bob receives the sequence

$$R = (r_0, r_1, r_2, \dots, r_n),$$

with perhaps some errors in the transmission from Alice to Bob. If at most  $e$  errors occurred, then at least  $(n + 1) - e$  components of the vectors  $C$  and  $R$  are equal. But we don't know which components they are.

Let

$$E(x) = (x - a_{i_1})(x - a_{i_2}) \cdots (x - a_{i_k})$$

be the error location polynomial, so that  $a_{i_1}, \dots, a_{i_k}$  are the elements among  $\{a_0, a_1, \dots, a_n\}$  where  $r_i \neq W(a_i)$ . Thus  $r_j = W(a_j)$  for all other  $j$ .

*Example 15.3* Suppose  $a_0 = -4, a_1 = 3, a_2 = 14$  and  $a_3 = 10$ ,

$$C = (3, 5, 14, 8), \text{ and } R = (4, 5, 14, 2).$$

Then  $W(a_0) = W(-4)$  and  $W(a_3) = W(10)$  were changed during the transmission of  $C$  from Alice to Bob. So

$$E(x) = (x - a_0)(x - a_3) = (x - (-4))(x - 10).$$

Returning to the general case, Bob has received  $R = (r_0, \dots, r_n)$  and wants to find  $W(x)$ , Alice's original polynomial. He does so by solving a set of  $n + 1$  equations in  $n + 2$  unknowns.

He doesn't know  $E(x)$ , because he doesn't know which coefficients of  $R(x)$  are wrong. But he assumes that  $E(x)$  has degree at most  $e$ .

Let  $G(x) = W(x)E(x)$ . Bob doesn't know  $W(x)$  or  $E(x)$ , so he doesn't know  $G(x)$ . All he knows is that  $W(x)$  has degree at most  $m$ . So he assumes that  $G(x)$  has degree at most  $m + e$ .

The only information Bob has about  $E(x)$  and  $G(x)$  is the set of components  $r_j$  of  $R$  for  $j = 0, \dots, n$  and the following:

**Proposition 15.4** *For all  $a_j$ ,  $j = 0, 1, \dots, n$ ,*

$$G(a_i) = r_i E(a_i).$$

*Proof* To verify the equations in Proposition 15.4, there are two cases:

If  $a_j$  is not an error location in

$$C = (W(a_0), W(a_1), W(a_2), \dots, W(a_n)),$$

then  $r_j = W(a_j)$ , and so

$$G(a_j) = W(a_j)E(a_j) = r_j E(a_j).$$

On the other hand, if  $a_j$  is an error location in  $C$ , then  $E(a_j) = 0$ , and so

$$G(a_j) = W(a_j)E(a_j) = 0,$$

and hence

$$G(a_j) = r_j E(a_j)$$

because both sides of the equation are 0. □

Thus Bob knows that whatever the unknown polynomials  $E(x)$  and  $G(x) = W(x)E(x)$  are, they satisfy

$$G(a_j) = r_j E(a_j)$$

for all  $j$  with  $j = 0, 1, \dots, n$ . And Bob knows all the  $r_j$ .

In particular, for the  $m + 1 + e$  values  $a_j$  where  $r_j = W(a_j)$ ,

$$G(a_j) = W(a_j)E(a_j).$$

All of what we just presented describes a model for how Bob can proceed to try to find  $W(x)$ .

Bob can try to find  $W(x)$  by finding polynomials  $G^*(x)$ ,  $E^*(x)$  so that

$$G^*(a_j) = r_j E^*(a_j)$$

for all  $j = 1, \dots, n + 1$ .

When he does, can he then conclude that  $G^*(x) = W(x)E^*(x)$ ? The answer is “yes”, as long as there aren't too many errors in  $R$ :

**Proposition 15.5** *Suppose  $W(a_j) = r_j$  for at least  $n + 1 - e$  of the numbers  $a_0, \dots, a_n$ . Then  $G^*(x) = W(x)E^*(x)$ .*

*Proof* We know that  $G^*(x)$  and  $E^*(x)$  are constructed with the property that for all of the  $n + 1$  numbers  $j$  with  $0 \leq j \leq n$ ,

$$G^*(a_j) = r_j E^*(a_j).$$

In particular, this is true for the  $n + 1 - k \geq n + 1 - e$  values of  $j$  for which  $W(a^j) = r_j$ . So for  $n + 1 - e = m + e + 1$  or more values of  $j$ ,

$$G^*(a^j) = W(a^j)E^*(a^j).$$

Now  $G^*(x)$  and  $W(x)E^*(x)$  each have degree  $\leq m + e$ . So we conclude by Corollary 6.9, an immediate consequence of D'Alembert's Theorem, that

$$G^*(x) = W(x)E^*(x).$$

□

So if there are at most  $e$  errors in going from  $C$  to  $R$ , Bob can find  $E^*(x)$  and  $G^*(x)$ , and then recover  $W(x)$  and decode the message by dividing  $G^*(x)$  by  $E^*(x)$ .

To find  $E^*(x)$  and  $G^*(x)$ , we set up and solve a matrix equation corresponding to the equations

$$G^*(a_j) = r_j E^*(a_j)$$

for all  $j = 0, 1, \dots, n$ .

Let

$$\begin{aligned} G^*(x) &= t_0 + t_1 x + t_2 x^2 + \dots + t_{m+e} x^{m+e} \\ E^*(x) &= s_0 + s_1 x + \dots + s_e x^e, \end{aligned}$$

with unknown coefficients  $t_0, \dots, t_{m+e}, s_0, \dots, s_e$ . For each  $j$ , write down the equation  $G^*(a_j) - r_j E^*(a_j) = 0$ :

$$t_0 + t_1 a_j + t_2 a_j^2 + \dots + t_{m+e} a_j^{m+e} - r_j (s_0 + s_1 a_j + \dots + s_e a_j^e) = 0.$$

This is a linear equation in the  $(m + e + 1) + (e + 1) = m + 2e + 2 = n + 2$  unknown coefficients of  $G^*(x)$  and  $E^*(x)$ . Collecting together these  $n + 1$  equations, one for each  $a_j$  with  $j = 0, 1, \dots, n$ , gives a system of  $n + 1$  homogeneous linear equations in  $n + 2$  unknowns.

It is well known from linear algebra that a system of  $n + 1$  homogeneous linear equations in  $n + 2$  unknowns always has a non-zero solution.

A standard algorithm for solving a homogeneous system of linear equations is to take the matrix of coefficients of the system and transform it into reduced row echelon form by a sequence of row operations. Then the solutions of the system can be found easily.

Let  $t_0^*, t_1^*, \dots, t_{m+e}^*, s_0^*, s_1^*, \dots, s_e^*$  be a non-trivial (i.e., non-zero) solution of the system of  $n + 1$  equations. Let

$$\begin{aligned} G^*(x) &= t_0^* + t_1^* x + t_2^* x^2 + \dots + t_{m+e}^* x^{m+e} \\ E^*(x) &= s_0^* + s_1^* x + \dots + s_e^* x^e \end{aligned}$$

be the corresponding polynomials. By choosing  $s_e^* = 1$ , we can choose  $E^*(x)$  to be monic.

Bob can then divide  $G^*(x)$  by  $E^*(x)$  to obtain a polynomial  $W^*(x)$ . Bob assumes that there are at most  $e$  errors in  $R$ . By Proposition 15.5, he concludes that  $W^*(x) = W(x)$ , the message that Alice sent.

In summary, Bob decodes by finding a non-trivial solution to a set of  $n + 1$  homogeneous linear equations in  $m + 2e + 2 = n + 2$  variables in the field  $F$ .

## 15.4 An Example

For a Reed–Solomon code, the parameters are

$m \geq 1$ , the degree of the plaintext polynomial  $W(x)$ ,

$e \geq 1$ , the maximum number of errors to be corrected, and

a set of  $n + 1$  distinct values  $a_0, a_1, \dots, a_n$  of the field  $F$ , where  $m + 2e = n$ .

The code vector  $C$  has  $n + 1$  components, obtained by evaluating  $W(x)$  at the elements  $a_0, a_1, \dots, a_n$  of  $F$ . Thus the field  $F$  must have at least  $n + 1$  elements.

In our example, we'll let  $F = \mathbb{F}_p$  where  $p$  is an unspecified prime, and we'll actually do all the computations in  $\mathbb{Z}$ . Then we'll reduce modulo  $p$  at the end, where we assume that  $p > n + 1$ .

Each example requires solving a system of  $n + 2$  linear equations in  $n + 1$  unknowns.

*Example 15.6* Let  $m = 2$ , the degree of  $W(x)$ , the plaintext polynomial, and  $e = 2$ , the number of errors we wish to correct. Then  $n = m + 2e = 6$ . Let  $F = \mathbb{F}_p$  where  $p$  is an unspecified prime  $> 7$ . For the  $n + 1$  elements of the field, we choose

$$(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (0, 1, 2, 3, 4, 5, 6).$$

**Encoding.** Suppose Alice wants to sent the plaintext word  $W = (3, 0, 7)$ , or equivalently,

$$W(x) = 3 + 7x^2.$$

She evaluates  $W(x)$  at the numbers 0 through 6 to form the coded word

$$\begin{aligned} C &= (W(0), W(1), W(2), W(3), W(4), W(5), W(6)) \\ &= (3, 10, 31, 66, 115, 178, 255), \end{aligned}$$

where the entries are defined modulo  $p$ .

**Error-correcting capability.** Before turning to Bob's decoding problem, we look at what the code can do. Let's suppose, for example, that  $p = 521$ , a prime  $> 2^9$ . Then, turning the entries of the coded word into base 2 numbers of length 10, the word becomes the sequence of the following ten-bit numbers.

$$3 \leftrightarrow 2 + 1 = (0000000011)$$

$$10 \leftrightarrow 8 + 2 = (0000000110)$$

$$31 \leftrightarrow 16 + 8 + 4 + 2 + 1 = (0000011111)$$

$$66 \leftrightarrow 64 + 2 = (0001000010)$$

$$115 \leftrightarrow 64 + 32 + 16 + 2 + 1 = (0001110011)$$

$$178 \leftrightarrow 128 + 32 + 16 + 2 = (0010110010)$$

$$255 \leftrightarrow 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = (0011111111).$$

Thus the coded word is a sequence of 70 bits.

Suppose there was a burst of static or a storage defect that changed the last two ten-bit numbers from

$$(0010110010), (001111111)$$

to

$$(0010000000), (0000000111),$$

so that eight 1's are changed to 0. If the 70 bits were the output of an encoding of ten plaintext words by the Hamming (7, 4) code (to give ten 7 bit encoded words), then three of the ten received words would

have at least two errors in them. The Hamming code can correct 1 error in a 7 bit received word, but cannot correct two or more errors in a word, so would incorrectly decode the last three words. But for the Reed–Solomon code, what that burst or defect did was to turn the last two numbers, 178 and 255, into 128 and 7, respectively—two errors among the seven received elements of  $\mathbb{F}_{521}$ . Our Reed–Solomon code can correct them.

**Decoding.** Returning to our example, Alice sends  $C$  through a noisy channel to Bob. Let us suppose that what comes out for Bob is

$$\begin{aligned} R &= (r_0, r_1, r_2, r_3, r_4, r_5, r_6) \\ &= (3, 10, 11, 66, 115, 178, 5). \end{aligned}$$

So there are two errors, to  $W(2)$  and  $W(6)$ . (Viewed in terms of bit errors, there would be 8 changed bits. But we're not correcting bits directly, but rather correcting elements of a field of  $p$  elements.)

Of course Bob, the receiver, doesn't know where or what the errors are. To find them, Bob writes down the polynomials  $G^*(x)$  and  $E^*(x)$  with unknown coefficients,

$$\begin{aligned} G^*(x) &= t_0 + t_1x + t_2x^2 + t_3x^3 + t_4x^4, \\ E^*(x) &= s_0 + s_1x + s_2x^2. \end{aligned}$$

He knows that the elements  $(a_0, a_1, \dots, a_6) = (0, 1, \dots, 6)$ . So he writes down the equations

$$G^*(a_j) - r_j E^*(a_j) = 0$$

by setting  $x = a_j = j$  for  $j = 0, 1, 2, \dots, 6$ . With  $R = (3, 10, 11, 66, 115, 178, 5)$ , here are the equations:

$$\begin{aligned} t_0 - 3s_0 &= 0 \\ t_0 + t_1 + t_2 + t_3 + t_4 - 10s_0 - 10s_1 - 10s_2 &= 0 \\ t_0 + 2t_1 + 4t_2 + 4t_3 + 16t_4 - 11s_0 - 22s_1 - 44s_2 &= 0 \\ t_0 + 3t_1 + 9t_2 + 27t_3 + 81t_4 - 66s_0 - 198s_1 - 594s_2 &= 0 \\ t_0 + 4t_1 + 16t_2 + 64t_3 + 256t_4 - 115s_0 - 460s_1 - 1840s_2 &= 0 \\ t_0 + 5t_1 + 25t_2 + 125t_3 + 625t_4 - 178s_0 - 890s_1 - 4450s_2 &= 0 \\ t_0 + 6t_1 + 36t_2 + 216t_3 + 1296t_4 - 5s_0 - 30s_1 - 180s_2 &= 0. \end{aligned}$$

In matrix form, they become the matrix equation

$$\left( \begin{array}{ccccccc} 1 & 0 & 0 & 0 & 0 & -3 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & -10 & -10 & -10 \\ 1 & 2 & 4 & 8 & 16 & -11 & -22 & -44 \\ 1 & 3 & 9 & 27 & 81 & -66 & -198 & -594 \\ 1 & 4 & 16 & 64 & 256 & -115 & -460 & -1840 \\ 1 & 5 & 25 & 125 & 625 & -178 & -890 & -4450 \\ 1 & 6 & 36 & 216 & 1296 & -5 & -30 & -180 \end{array} \right) \begin{pmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \\ t_4 \\ s_0 \\ s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

(All entries represent elements of  $\mathbb{F}_p$ .) Let  $A$  be the matrix of coefficients of this equation.

Note that there is a pattern in the columns of  $\mathbf{A}$ : the first five columns have the form

$$\begin{pmatrix} a_0^j \\ a_1^j \\ a_2^j \\ a_3^j \\ a_4^j \\ a_5^j \\ a_6^j \end{pmatrix}$$

(where  $0^0 = 1$ ) and the last three columns are the first three columns with each entry multiplied by the corresponding component of  $R$ .

To solve the matrix equation, we need to reduce the coefficient matrix  $\mathbf{A}$  to its row echelon form  $\mathbf{A}_e$ . I did it by putting the matrix  $A$  in a row operation calculator found online, and determined the reduced row echelon form (in  $\mathbb{Z}$ ) to be

$$\mathbf{A}_e = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & -36 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 24 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -87 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 56 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -7 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -12 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 8 \end{pmatrix}.$$

For any coefficient matrix  $\mathbf{A}$ , the set of solutions of the matrix equation  $\mathbf{Ax} = \mathbf{0}$  is the same as the set of solutions of the matrix equation  $\mathbf{A}_e\mathbf{x} = \mathbf{0}$ , where  $\mathbf{A}_e$  is the reduced row echelon form of  $\mathbf{A}$ . (We learn early in an elementary linear algebra course that the point of finding the reduced row echelon form of  $\mathbf{A}$  is to turn the original system of equations into another system with the same solutions, where the solutions are easy to write down.)

Since the matrix of coefficients has rank 7, there is only one parameter in the solutions, namely  $s_2$ , the variable whose coefficients are the numbers in the last column. The equations corresponding to the last two rows of  $\mathbf{A}_e$  are

$$s_1 + 8s_2 = 0, \text{ so } s_1 = -8s_2; \text{ and}$$

$$s_0 - 12s_2 = 0 \text{ so } s_0 = 12s_2.$$

If we set  $s_2 = 1$ , then the polynomial  $E^*(x)$  is monic, and

$$E^*(x) = s_0 + s_1x + s_2x^2 = 12 - 8x + x^2 = (x - 6)(x - 2).$$

( $E^*(x)$  turns out to be the error polynomial  $E(x)$ .) Also from the reduced row echelon form, we find that  $G^*(x)$  is

$$36 - 24x + 87x^2 - 56x^3 + 7x^4.$$

Dividing  $G^*(x)$  by  $E^*(x)$  by polynomial long division, we obtain a quotient of  $3 + 7x^2$  and a remainder of 0.

By Proposition 15.5, we know that the quotient  $7x^2 + 3 = W(x)$ , the original plaintext polynomial. The decoding is complete.

We did all the computations in  $\mathbb{Z}$ , and so the results would also be valid in  $\mathbb{Z}_p = \mathbb{F}_p$  for any prime  $p > 10$ , such as  $p = 11$  or  $p = 521$ .

*Example 15.7* Suppose we change the last example so that there is only one error. Then as we'll see, the coefficient matrix has rank six, so there will be two parameters in the solution. Assume

$$C = (3, 10, 31, 66, 115, 178, 255)$$

and suppose

$$\begin{aligned} R &= (r_0, r_1, r_2, r_3, r_4, r_5, r_6) \\ &= (3, 10, 11, 66, 115, 178, 255). \end{aligned}$$

Then the equation

$$G(x) = W(x)E(x)$$

becomes, in matrix form, the equation

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -3 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & -10 & -10 & -10 \\ 1 & 2 & 4 & 8 & 16 & -11 & -22 & -44 \\ 1 & 3 & 9 & 27 & 81 & -66 & -198 & -594 \\ 1 & 4 & 16 & 64 & 256 & -115 & -460 & -1840 \\ 1 & 5 & 25 & 125 & 625 & -178 & -890 & -4450 \\ 1 & 6 & 36 & 216 & 1296 & -255 & -1530 & -9180 \end{pmatrix} \begin{pmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \\ t_4 \\ s_0 \\ s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Reducing the coefficient matrix to reduced row echelon form yields the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 6 & 12 \\ 0 & 1 & 0 & 0 & 0 & 0 & -3 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 14 & 25 \\ 0 & 0 & 0 & 1 & 0 & 0 & -7 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -7 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The corresponding equations are

$$t_0 = -6s_1 - 12s_2$$

$$t_1 = 3s_1$$

$$t_2 = -14s_1 - 25s_2$$

$$t_3 = 7s_1$$

$$t_4 = 7s_2$$

$$s_0 = -2s_1 - 4s_2.$$

If we set  $s_2 = 0$  and  $s_1 = 1$ , then we get the solution

$$s_0 = -2,$$

so

$$E^*(x) = x - 2.$$

Also,

$$(t_0, t_1, t_2, t_3, t_4) = (-6, 3, -14, 7, 0)$$

so

$$G^*(x) = 7x^3 - 14x^2 + 3x - 6.$$

Then

$$G^*(x)/E^*(x) = 7x^2 + 3 = W(x).$$

When there are fewer than  $e$  errors, as in this example (with  $e = 2$ ), the solution of the matrix equation arising from the equations

$$G^*(a_j) = r_j E^*(a_j)$$

will have more than one parameter, that is, more than one variable we may choose at will. So we choose the parameters so that the corresponding polynomial  $E^*(x)$  is monic of minimal degree. In our example, the two parameters were  $s_1$  and  $s_2$ . We set  $s_2 = 0$  and  $s_1 = 1$ , so that  $E^*(x)$  is monic of degree 1. Since the original unknown polynomial  $E(x)$  is chosen to be monic, then  $E^*(x) = E(x)$ .

**Remarks.** 1. Alice’s plaintext consists of integers that represent elements of  $\mathbb{F}_p$  for some prime  $p$ . Hence we can view  $W(x)$  as having integer coefficients; and the error polynomial  $E(x)$  as a monic polynomial with integer coefficients. If we multiply  $E(x)W(x)$  in  $\mathbb{Q}[x]$  to get  $G(x)$ , then  $G(x)$  also has integer coefficients. So the system of equations has an integer solution in which the variable that is the coefficient  $s_e$  of the highest power of  $x$  in  $E(x)$  (in particular,  $s_2$  in the example above) is equal to 1. Using  $s_e$  as the parameter, as we did above, then setting  $s_e = 1$  or  $-1$  will always yield a solution of the system of equations where the solution is in  $\mathbb{Z}$ .

Thus if there are  $e$  errors, and the last column of the matrix  $A$  of coefficients is the set of coefficients of the unknown  $s_e$  in the system of equations, then the reduced row echelon form of  $A$  will always have entries in  $\mathbb{Z}$ .

This means that the matrix computations involved in the decoding and error correction can take place in  $\mathbb{Z}$ , a substantial benefit when online matrix computers (such as [Bg13]) don’t understand modular arithmetic.

However, if you put a matrix with integer entries into a program that computes in the rational numbers, and ask for the reduced row echelon form, there may be issues. Even if the reduced row echelon form contains only integers, the program may obtain it using row operations using fractions with denominators divisible by the prime  $p$ . If the field you are using for the code is  $\mathbb{Z}_p$ , then the reduced row echelon form will be incorrect. So I computed reduced row echelon forms using a program that allowed me to do individual row operations of my choice, to be certain that fractions never occurred.

To use a Reed–Solomon code in “the real world”, part of the implementation would involve finding a matrix calculator that could work accurately in your choice of finite field.

2. Reed–Solomon codes begin with a plaintext message, a sequence  $W$  of elements of the field, which become the coefficients of the polynomial  $W(x)$ . The version of Reed–Solomon codes presented here encodes  $W$  by forming a vector of values of the polynomial  $W(x)$  on a fixed set of  $n + 1$  values of the field.

There is another version of Reed–Solomon codes that encodes  $W$  by replacing  $W(x)$  by  $C(x) = W(x)x^k + Z(x)$ , where the resulting polynomial  $C(x)$  is divisible by a polynomial  $m(x)$  of degree  $k$  whose roots of  $m(x)$  are low powers of a primitive root of the field. So the coefficients of  $W(x)$  are the high-degree coefficients of  $C(x)$ . In that version of Reed–Solomon codes are closely related to BCH codes, a class of multiple error-correcting codes discovered in 1960 by Bose, Chaudhuri and Hocquenghem, and which use finite fields that contain  $\mathbb{F}_2$  as a subfield. Describing the alternate version and showing the equivalence of the two versions would take us beyond the scope of this book. There are various standard textbooks on error correcting codes, such as [VL82], [MS83] and [Ple98], that present BCH codes and other forms of error correction, and there is also a lot of material on the web about Reed–Solomon codes.

3. The decoding method described here, the Welch-Berlekamp method, was one of the first important mathematical algorithms to receive a patent from the U.S. Patent Office, in 1986. That patent, and the 1988 patent for the even more famous Karmarkar algorithm for solving linear programming problems in polynomial time, created much controversy over the idea of granting patents to abstract mathematical ideas. See Section 6 of [Ha03] for some discussion on this issue. Two news articles involving public key cryptography and patents, which include a snippet on the history of public key cryptography, are [Mu13a], [Mu13b].

The Karmarkar and Welch-Berlekamp patents have expired and the algorithms are now in the public domain. Patents on the Diffie-Hellman key exchange and on the RSA cryptosystem also expired, in 1997 and 2000, respectively.

4. Chapter 18 introduces finite fields other than  $\mathbb{Z}_p$  for  $p$  prime. Some widely known applications of Reed-Solomon codes have used the field  $\mathbb{F}_{256}$ . These include implementations on compact discs and DVDs, and on Voyager expeditions for transmitting digital images from the outer planets.

In Chapter 19 we will revisit Reed-Solomon codes, look at an example over  $\mathbb{F}_8$ , and see how to use the discrete Fourier transform to reduce the computation needed to solve the decoding matrix equation.

## Exercises

- 15.1. Similar to Example 15.2, consider the two error correcting Reed-Solomon code with  $(m, e, n) = (2, 2, 6)$ , with the field  $F = \mathbb{F}_p$  with  $p$  a large prime. Use

$$(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (-3, -2, -1, 0, 1, 2, 3).$$

You want to send the plaintext message  $w = (15, 1, -2)$  to Bob, and want Bob to be able to correct two errors. You and Bob agree to use the Reed-Solomon code as just described. Find the encoded 7-tuple  $C$  for the plaintext message  $w$  that you send to Bob.

- 15.2. Alice encoded a message  $w = (w_0, w_1, w_2)$  that she sent to you, using the Reed-Solomon code of Example 15.2 with  $(a_0, \dots, a_6) = (-3, -2, -1, 0, 1, 2, 3)$ . You received

$$R = (-17, -2, 7, -17, 7, -2, 10).$$

Assume that at most two errors occurred.

- (i) Set up the matrix equation whose solution will give the coefficients of the polynomials  $E(x)$  and  $G(x)$  so that  $W(x)E(x) = G(x)$ .
- (ii) Solve the equation to find Alice's plaintext message  $w$ .

- 15.3. What is the efficiency of the code of Example 15.2? (Efficiency is defined in Chapter 7.)

Suppose you use the code of Exercise 15.1 with  $p = 127 = 2^7 - 1$  (a prime). Then each element of  $\mathbb{F}_{127}$  is uniquely representable by a number  $m$  with  $0 \leq m < 127$ , which in turn corresponds to a seven-tuple of bits, the digits in the base 2 representation of the number  $m$ . (For example, 113 corresponds to 1110001:  $113 = 64 + 32 + 16 + 1$ .) A coded message  $C$  is a seven-tuple of elements of  $\mathbb{F}_{127}$ , each element in turn representable by a seven-tuple of bits. Hence  $C$  corresponds to a bit message with 49 bits. Then  $R$  also has 49 bits.

- 15.4. (a) In Exercise 15.1 with  $\mathbb{F}_{127}$ , suppose that a single burst of consecutive bit errors occurred in the transmission of  $C$ . What is the smallest number of consecutive bit errors that the code would fail to correct?  
 (b) What is the answer to (a) if instead of  $\mathbb{F}_{127}$ , the code as above used the field  $\mathbb{F}_p$  where the prime  $p = 8191 = 2^{13} - 1$
- 15.5. Let  $m = 1, e = 1, n = 3$ . Set up a Reed–Solomon code, using the field  $\mathbb{F}_p$  where  $p$  is a large prime, that sends two information bits and corrects one error. Suppose the plaintext word is  $W = (w_0, w_1)$ . If you evaluate the corresponding polynomial  $W(x) = w_0 + w_1x$  at  $x = 0, 1, 2, 3$ , you obtain the code word

$$C = (W(0), W(1), W(2), W(3)).$$

Let  $R = (r_0, r_1, r_2, r_3)$  be the received word. Then the matrix of coefficients of the equations to solve to find the unknown coefficients of the polynomials  $E^*(x) = s_0 + s_1x$  and  $G^*(x) = t_0 + t_1x + t_2x^2$  is the matrix of coefficients of the system of homogeneous equations

$$\begin{aligned}t_0 + t_1 \cdot 0 + t_2 \cdot 0 - s_0r_0 - s_1r_0 \cdot 0 &= 0 \\t_0 + t_1 \cdot 1 + t_2 \cdot 1 - s_0r_1 - s_1r_1 \cdot 1 &= 0 \\t_0 + t_1 \cdot 2 + t_2 \cdot 2^2 - s_0r_2 - s_1r_2 \cdot 2 &= 0 \\t_0 + t_1 \cdot 3 + t_2 \cdot 3^2 - s_0r_3 - s_1r_3 \cdot 3 &= 0.\end{aligned}$$

Suppose  $R = (3, 5, 7, 11)$  and assume one error occurred.

- (i) Write down the matrix of coefficients of the system of equations.
  - (ii) Find a non-zero solution of the system of equations. The numbers in your solution should all be integers. (Make sure your proposed solution really is a solution of the system of equations.)
  - (iii) Write down  $E^*(x)$  and  $G^*(x)$ , and find  $W(x)$  by dividing  $E^*(x)$  into  $G^*(x)$  by long division of polynomials.
- 15.6. Suppose given the same Reed–Solomon code as in Exercise 15.5, but suppose that you evaluate  $W(x)$  at  $x = -1, 0, 1, 2$  instead of at  $0, 1, 2, 3$ , to get

$$C = (W(-1), W(0), W(1), W(2)).$$

Suppose  $R = (8, -3, 2, 7)$ . Write down the corresponding system of equations and the corresponding matrix of coefficients.

- 15.7. What is the efficiency of the code of Exercise 15.5?

# Chapter 16

## Blum-Goldwasser Cryptography



In this chapter we introduce a modern, secure version of the additive Vigenère cryptosystem. As with RSA, security depends on the difficulty of factoring a large number into a product of primes. The cryptosystem uses sequences of “pseudorandom numbers”, which are numbers that look random but aren’t. Pseudorandom numbers arose early in the development of computers, because they are helpful in a variety of settings other than cryptography.

### 16.1 Vernam Cryptosystems

We recall the Vernam or one-time-pad cipher from Section 1.3. It works as follows:

Suppose Alice wants to send Bob the message I\_LUV\_U (with two spaces). She transforms her message into a sequence of bits. For example, I\_LUV\_U, becomes the sequence of numbers 9, 0, 12, 21, 22, 0, 21, which in base 2 are 01001, 00000, 01100, 10101, 10110, 00000, 10101. The plaintext message is then the sequence of bits:

$$w = (01001; 00000; 01100; 10101; 10110; 00000; 10101)$$

(where the semicolons are added for readability).

Suppose Alice and Bob have a shared secret key  $k$ , consisting of a random sequence of bits of the same length as the message. For example, suppose

$$k = (10100; 01001; 01010; 10001; 01000; 00101; 11111).$$

Then Alice’s ciphertext message is the sum  $w + k$ , viewed as row vectors with entries in  $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ :

$$\begin{aligned} c &= w + k \\ &= (0 + 1, 1 + 0, 0 + 1, 0 + 1, 1 + 1; 0 + 0, 0 + 1, 0 + 0, 0 + 0, 0 + 1; \\ &\quad 0 + 0, 1 + 0, 1 + 0, 0 + 1, 0 + 0; \text{ etc.}) \\ &= (11110; 00110; 01110; \text{ etc.}) \end{aligned}$$

To decrypt  $c$ , Bob computes  $c + k$ . Since  $k + k = 0$  (where 0 is the sequence consisting of all zeros), it follows that  $c + k = w$ , the plaintext message.

Given the key  $k$ , encrypting and decrypting is extremely fast.

Moreover, if the key  $k$  is truly random, then the probability of any given bit being 0 is  $p = 1/2$ , and that probability is independent of the value of any other bit. Adding  $k$  to any fixed sequence of bits will yield a sequence of bits with the same property. So without knowing the key  $k$ , Eve has no chance to determine  $w$  from  $c$ : no frequency analysis based on English can be successful. Even a “brute force”

attack—try every random sequence—would fail. If the message and the key are 256 bits long, then Eve would need to try  $2^{256} \sim 10^{77}$  keys, and even if such a method were practical (which it is not), the result would be the same as the “infinite monkeys” thought experiment—every piece of text of 256 characters could be generated, and in particular, every meaningful piece of text of that size could be generated, such as GO AWAY. How to decide which meaningful text is the correct decryption?

So if the list of shift numbers  $k_1, k_2, \dots$  is truly random and secret, then the Vernam cipher is unbreakable.

However, the Vernam cipher is difficult to implement securely. It requires that Alice and Bob have a shared secret key, namely a list of randomly generated bits as long as the message. If Alice and Bob are physically separated and communicate frequently, the secret key would need to be very long. Storage and accuracy issues for shared long keys would become an issue.

A modern implementation of the Vernam cipher would want to use a long sequence of numbers that look random, but are generated in a way that storage is not a problem. So it is natural to consider using a sequence of pseudorandom numbers for a key.

**Pseudorandom numbers.** Random numbers have been of interest in computer science almost since the development of computers in the 1940s. They are needed in ways having nothing to do with cryptography. Some examples are:

- To introduce randomness into web-based homework and quizzes for math students, and into computer games;
- In statistics, to generate a collection of random data sets having a certain distribution, to help decide if a given data set is, or is not, likely to have that distribution.
- To pick numbers  $a$  for testing a large number for primeness by the strong  $a$ -pseudoprime test. See Chapter 9.

Pseudorandom numbers are numbers that look random by various statistical tests, but are generated by a deterministic process (and hence are not random).

An early method for creating sequences of pseudorandom numbers or bits was proposed by D. H. Lehmer in 1949, as follows: pick a large prime  $p$ , pick a primitive root  $b$  modulo  $p$  and a starting number  $x_0$ , and define the sequence  $x_1, x_2, \dots$  by multiplying each number in the sequence by  $b$  to obtain the next number:

$$x_i \equiv x_{i-1}b \equiv x_0b^i \pmod{p}.$$

To get a sequence of pseudorandom rational numbers between 0 and 1, let  $r_i = x_i/p$ . Or to get a sequence of pseudorandom bits (zeros and ones), let  $r_i = x_i \pmod{2}$ . Thus  $r_i$  is 1 if  $x_i$  is odd,  $r_i = 0$  if  $x_i$  is even.

*Example 16.1* Let  $p = 41$ ,  $b = 13$ ,  $x_0 = 38$ . Then 13 is a primitive root modulo 41. The sequence  $\{x_i\}$  of numbers  $(\text{mod } 41)$  is then defined by  $x_{i+1} = 13x_i \pmod{41}$ :

$$\begin{aligned} & 38, 2, 26, 10, 7, 9, 35, 4, 11, 20, \\ & 14, 18, 29, 8, 22, 40, 28, 36, 17, 16, \\ & 3, 39, 15, 31, 34, 32, 6, 37, 30, 21, \\ & 27, 23, 12, 33, 19, 1, 13, 5, 24, 25, \\ & 38, 2, 26. \dots \end{aligned}$$

The sequence repeats only every 40 numbers, because  $b = 13$  has order 40 modulo 41. The corresponding sequence of bits is

$$\begin{aligned} & 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, \\ & 0, 0, 1, 0, 0, 0, 0, 0, 1, 0 \\ & 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, \\ & 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, \\ & 0, 0, 0, \dots \end{aligned}$$

In a Lehmer sequence, the period of the sequence is equal to the order of  $b$  modulo  $p$ . Thus a Lehmer sequence can be set up with a period of any desired length. Just choose a primitive root modulo a sufficiently large prime number  $p$ , then the sequence will have period  $p - 1$ .

The key for generating the sequence consists of the prime  $p$ , the primitive root  $b$  modulo  $p$  and the starting number  $x_0$ .

But for Vernam-type cryptography, there are issues. One is that a Lehmer sequence does not look all that random, when subjected to statistical tests for randomness [PM88], [FM82], and some examples are notoriously far from random. See [Knu98], Chapter 3 for more discussion.

More seriously for cryptography, a Lehmer sequence can't be used for a public key cryptosystem. An eavesdropper, Eve, who learns  $p$  and two consecutive numbers in a Lehmer sequence,  $x_i$  and  $x_{i+1}$ , can find  $b$  by  $b = x_{i+1}/x_i$  and then determine the rest of the sequence, in both directions—both after  $x_{i+1}$  and before  $x_i$ . And no one has come up with a way for Bob and Alice to publicly give each other enough information about how to generate the sequence, without giving everyone, including Eve, enough information to construct the sequence. Once Eve has the sequence, she can decrypt any message Alice sends Bob using that sequence.

So for cryptography, a way to efficiently generate a more secure sequence of pseudorandom numbers is needed.

## 16.2 Blum, Blum and Shub's Pseudorandom Number Generator

L. Blum, M. Blum, and M. Shub [BBS86] proposed a pseudorandom number generator that has the property: given a number  $x_k$  in the sequence, it is essentially impossible to find the previous number  $x_{k-1}$  in the sequence without special knowledge.

A Blum, Blum, Shub (BBS) sequence is computed as follows.

Pick a suitable modulus  $m$  and a starting number  $x_0$ , let  $x_1 = x_0^2 \pmod{m}$ , and generate the sequence  $x_1, x_2, \dots$  of numbers  $< m$  by successively squaring modulo  $m$ :  $x_{k+1} = (x_k^2 \pmod{m})$  for all  $k \geq 1$ . Given the sequence  $(x_1, x_2, \dots, x_n, \dots)$ , we then may obtain a sequence of bits (0's and 1's) by defining  $b_k = x_k \pmod{2}$ , that is,  $b_k = 0$  if  $x_k$  is even,  $b_k = 1$  if  $x_k$  is odd.

Here is an example.

*Example 16.2* Let  $m = 437 = 19 \cdot 23$  and let  $x_0 = 5$ . The sequence  $x_1, x_2, x_3, \dots$  is then obtained by successively squaring modulo 437:  $x_1 = 5^2 \equiv 25 \pmod{437}$ ,  $x_2 = 25^2 \equiv 188 \pmod{437}$ , etc. Thus the sequence is

25, 188, 384, 187, 9, 81, 6, 36, 422, 225,  
 370, 119, 177, 302, 308, 35, 351, 404, 215, 340,  
 232, 73, 85, 233, 101, 150, 213, 358, 123, 271,  
 25, 188, 384, 187, 9, ....

The corresponding sequence of bits  $b_i$  is

1, 0, 0, 1, 1, 0, 0, 0, 1  
 0, 1, 1, 0, 0, 1, 1, 0, 1, 0,  
 0, 1, 1, 1, 1, 0, 1, 0, 1, 1  
 1, 0, 0, 1, 1, ....

This sequence has period 30 (that is,  $x_{k+30} \equiv x_k \pmod{m}$  for all  $k \geq 0$ ).

In Excel it is easy to construct such a sequence. For example, to construct the sequence of the last example, put  $y = 5$  in cell B2, put  $=\text{Mod}(B2, 437)$  in cell C3, and put  $=C3^2$  in B3. Then highlight cells B3 and C3, and hit Ctrl C [copy]. Then highlight the cells B4 to B40 and C4 to C40, and hit Ctrl V [paste]. The BBS sequence should appear in column B.

For cryptography we obviously want a sequence with a very long period. Later we will show how to determine what the period of a given sequence is, and then how to find a BBS sequence with a long period.

But first, here is how BBS sequences are used in cryptography.

### 16.3 Blum-Goldwasser Cryptography

A BBS sequence can be used as an encrypting sequence for a Vernam-type cryptosystem, known as the Blum-Goldwasser cryptosystem [BG85]. The encrypting/decrypting sequence is a sequence of bits arising from a BBS sequence. The major difference from a Vernam cryptosystem is that the Blum-Goldwasser system uses a pseudorandom key sequence whose construction depends on a public key. The public key enables a receiver, Bob, to decrypt because, like the receiver in an RSA cryptosystem, he has special knowledge that no one else has, knowledge that enables him to construct the decrypting sequence from the public key.

Bob wants Alice to send encrypted messages. To do so, Bob begins by picking two large primes  $p$  and  $q$ , both congruent to 3 modulo 4. (We'll put additional conditions on  $p$  and  $q$  later.) Then  $m = pq$  is the modulus for a BBS sequence. He keeps  $p$  and  $q$  secret but sends  $m$  to Alice.

Alice has a message  $\bar{w} = (w_1, w_1, \dots, w_g)$  consisting of  $g$  bits (0's and 1's). She selects a random number  $x_0$  coprime to  $m$  and generates the BBS sequence

$$x_1 \equiv x_0^2, x_2 \equiv x_1^2, \dots, x_g \equiv x_{g-1}^2 \pmod{m}.$$

Then she reduces the BBS sequence modulo 2 to get  $\bar{k} = (k_1, k_2, \dots, k_g)$ , the encrypting vector of bits defined by  $k_j = x_j \pmod{2}$  for  $j = 1, \dots, g$ . Alice encrypts her message by

$$\bar{c} = \bar{w} + \bar{k},$$

with addition componentwise, mod 2 (that is, addition is in the vector space  $\mathbb{F}_2^g$  of  $g$ -tuples with entries in the field  $\mathbb{F}_2$  of two elements, 0 and 1). Then Alice sends Bob the pair  $(\bar{c}, \kappa)$  where  $\kappa = x_{g+1} = x_g^2 \pmod{m}$ . The vector  $\bar{c}$  is Alice's encrypted message, and  $\kappa$  is the public key for decrypting the message.

Note that Alice does not need to know how to factor  $m$  to encrypt. The factorization of  $m$  is needed only to decrypt.

Bob needs to construct the BBS sequence  $(x_1, x_2, \dots, x_g)$  and reduce it modulo 2 to find the encrypting vector  $\bar{k} = (k_1, k_2, \dots, k_g)$ . Then he can decrypt the message, because the encrypting vector is also the decrypting vector:  $\bar{w} = \bar{c} + \bar{k}$  (addition is mod 2).

So Bob takes the key  $\kappa = x_{g+1}$  and reconstructs Alice's BBS sequence from  $x_{g+1}$  by successively computing  $x_g, x_{g-1}, x_{g-2}, \dots, x_1$  modulo  $m$  by the function

$$x_{j-1} = \omega(x_j) \equiv x_j^{\frac{p_1 q_1 + 1}{2}} \pmod{m}$$

for  $j = g+1, g, \dots, 2$ , where  $p_1$  and  $q_1$  satisfy  $2p_1 + 1 = p$ ,  $2q_1 + 1 = q$ . He can find  $p_1$  and  $q_1$  because he knows the factors  $p$  and  $q$  of  $m = pq$ .

We will see below why that decrypting function works.

Having found Alice's BBS sequence  $(x_1, \dots, x_g)$  Bob obtains the encrypting/decrypting vector

$$\bar{k} = (k_1, \dots, k_g),$$

where  $k_j = (x_j \bmod 2)$ . He adds  $\bar{k}$  to Alice's encrypted message  $\bar{c}$  to recover her plaintext message  $\bar{w} = \bar{c} + \bar{k}$ .

We'll show soon that an eavesdropper, Eve, would need to know how to factor  $m$  into its prime factorization  $m = pq$  in order to use the key  $\kappa$  to construct the BBS sequence and the encrypting/decrypting vector  $\bar{k}$ .

*Example 16.3* Alice wants to send Bob a letter.

Bob chooses  $m = 209$  which he knows factors as  $11 \cdot 19$ . He sends Alice the number 209 but not the prime factorization.

The letter Alice wants to send Bob is "r", or 18, or  $\bar{w} = (10010)$  (base 2). She picks a random starting value  $x_0 = 13$  and computes a BBS sequence starting from  $x_0 = 13$  by successively squaring modulo  $m = 209$ :

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (169, 137, 168, 9, 81, 82).$$

She saves  $x_6 = \kappa = 82$ , the key, and reduces the other numbers mod 2 to get

$$\bar{k} = (1, 1, 0, 1, 1).$$

She finds  $\bar{c} = \bar{w} + \bar{k}$ :

$$\bar{c} = (1, 0, 0, 1, 0) + (1, 1, 0, 1, 1) = (0, 1, 0, 0, 1)$$

and sends the pair  $(\bar{c}, \kappa) = ((0, 1, 0, 0, 1), 82)$  to Bob.

Bob knows that  $209 = pq$  with  $p = 11, q = 19$ . To find the function  $\omega(z)$ , he finds  $p_1 = \frac{11-1}{2} = 5$  and  $q_1 = \frac{19-1}{2} = 9$ , then

$$\frac{p_1 q_1 + 1}{2} = \frac{45 + 1}{2} = 23.$$

So

$$\omega(z) = z^{23} \pmod{209}.$$

Using  $\omega(z)$  and starting with the key  $\kappa = 82$ , Bob reconstructs the BBS sequence backwards, by

$$82^{23} \equiv 81; 81^{23} \equiv 9; 9^{23} \equiv 168, 168^{23} \equiv 137; 137^{23} \equiv 169 \pmod{209}.$$

So Alice's BBS sequence is

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (169, 137, 168, 9, 81)$$

which mod 2 is

$$\bar{k} = (1, 1, 0, 1, 1).$$

Adding that sequence to  $\bar{c} = (0, 1, 0, 0, 1)$  gives  $\bar{w} = (1, 0, 0, 1, 0)$ , or the 18th letter, “r”.

There are issues to explore with BBS sequences and Blum-Goldwasser cryptology.

- One is to determine the period of a BBS sequence, so that we can find sequences with very long periods for cryptography.
- Another is to explain why the function  $\omega$  recreates the BBS sequence from the last term of the sequence.
- Finally, we'll deal with the issue of security, namely, why it is hard for Eve to recreate the sequence despite knowing  $m$  and  $\kappa$ .

We'll deal with these issues in the next three sections.

## 16.4 The Period of a BBS Sequence

A BBS sequence is obtained by successive squaring modulo  $m$ . Starting from an arbitrary number  $y$  coprime to  $m$ , the sequence is

$$x_0 = y, y^2, (y^2)^2 = y^{2^2}, (y^{2^2})^2 = y^{2^3}, y^{2^4}, y^{2^5}, \dots \pmod{m}.$$

Since  $y$  is a unit of  $\mathbb{Z}_m$ , it has an order  $d$ , the smallest  $d > 0$  so that  $y^d \equiv 1 \pmod{m}$ . The exponents  $2, 2^2, 2^3, \dots$  of  $y$  may all be viewed as elements of  $\mathbb{Z}_d$ , since  $y^r = y^s$  whenever  $r \equiv s \pmod{d}$  (Proof: if  $r = s + kd$ , then  $y^r \equiv y^{s+kd} = y^s(y^d)^k \equiv y^s \cdot 1^k \equiv y^s \pmod{m}$ .)

Here is how to obtain the period of the sequence, that is, the first point in the sequence where the sequence begins to repeat.

**Proposition 16.4** *Let  $m$  be a modulus,  $y$  a number coprime to  $m$ , and let  $d = 2^k f$  be the order of  $y$  modulo  $m$ , with  $f$  odd. Then the period of the BBS sequence*

$$y, y^2, y^{2^2}, y^{2^3}, y^{2^4}, y^{2^5}, \dots \pmod{m}$$

*is equal to the order of 2 modulo  $f$ , the odd part of the order of  $y$  modulo  $m$ .*

So to find the period of a BBS sequence modulo  $m$  starting with  $y$  coprime to  $m$ , we need to find the orders of two elements: first, the order  $d$  of  $y$  in the group  $U_m$  of units modulo  $m$ , which we write as  $d = 2^k f$  with  $f$  odd, and second, the order of 2 in the group  $U_f$  of units modulo  $f$ . That order is the period of the BBS sequence.

To prove Proposition 16.4, and also for examples, we first need:

**Lemma 16.5** *Let  $m = rs$  with  $(r, s) = 1$ . For  $y$  coprime to  $m$ , if the order of  $y$  modulo  $r$  is  $d$ , and the order of  $y$  modulo  $s$  is  $e$ , then the order of  $y$  modulo  $m = rs$  is  $[d, e]$ , the least common multiple of  $d$  and  $e$ .*

*Proof of the lemma* First,

$$y^{[d,e]} \equiv 1 \pmod{r}$$

and

$$y^{[d,e]} \equiv 1 \pmod{s}$$

since  $[d, e]$  is a multiple of the order of  $y$  modulo  $r$  and is a multiple of the order of  $y$  modulo  $s$ . Therefore  $r$  divides  $y^{[d,e]} - 1$  and so does  $s$ . So  $y^{[d,e]} - 1$  is a common multiple of  $r$  and  $s$ , so is a multiple of the least common multiple of  $r$  and  $s$ . Since  $r$  and  $s$  are coprime, their least common multiple is their product  $m = rs$ . So  $y^{[d,e]} \equiv 1 \pmod{m}$ .

Now we show that  $[d, e]$  is the order of  $y$  modulo  $m$ . Suppose  $y^k \equiv 1 \pmod{m}$ . Then  $y^k \equiv 1 \pmod{r}$ , so  $d$  divides  $k$ . Also  $y^k \equiv 1 \pmod{s}$ , so  $e$  divides  $k$ . That means:  $k$  is a common multiple of  $d$  and  $e$ . So  $k \geq [d, e]$ .

Thus if  $r$  and  $s$  are coprime,  $m = rs$  and  $y$  is coprime to  $m$ , then the smallest exponent  $k$  so that  $y^k \equiv 1 \pmod{m}$  is  $k = [d, e]$ .  $\square$

*Example 16.6* Let  $m = 209 = 11 \cdot 19$ , and suppose we start a BBS sequence with  $y = 13$ . Then the order of  $y$  modulo 11 is 10, and the order of  $y$  mod 19 is 18. So the order of  $y$  modulo 209 is  $[10, 18] = 90 = 2 \cdot 45$ . So the period of the sequence generated by  $y$  is equal to the order of 2 modulo 45. Now 2 has order 6 modulo 9, and has order 4 modulo 5. So 2 has order  $[6, 4] = 12$  modulo 45. So the period of the BBS sequence is 12.

*Example 16.7* Let  $m = 437 = 19 \cdot 23$  and we begin a BBS sequence with  $y = 5$ . The order of 5 modulo 437 is the least common multiple of the order of 5 modulo 19 and the order of 5 modulo 23.

Now 2 is a primitive root modulo 19, and  $2^{16} \equiv 5 \pmod{19}$ , so 5 has order  $18/(18, 16) = 9$  modulo 19.

Also, 2 is a primitive root modulo 23, and  $2^{17} \equiv 5 \pmod{23}$ , so 5 has order  $22/(22, 17) = 22$  modulo 23. Hence 5 has order  $[22, 9] = 198$  modulo 437.

The odd part of  $198 = 2 \cdot 99$  is 99, so the period of the BBS sequence starting with 5 is the order of 2 modulo 99. By Lemma 16.5, the order of 2 modulo 99 is the least common multiple of the order of 2 modulo 11 (namely, 10) and the order of 2 modulo 9 (namely 6). So the period =  $[10, 6] = 30$ , as we found by explicit computation in Example 16.2, above.

*Example 16.8* Let  $m = 43 \cdot 23 = 989$ . We let  $y = 7$  and we compute

$$7, 7^2, 7^{2^2}, 7^{2^3}, 7^{2^4}, 7^{2^5}, \dots \pmod{989}.$$

This sequence turns out to have period 10:

$$7, 49, 423, 909, 466, 565, 767, 823, 853, 694, 982, 49, 423, \dots$$

We check the validity of Proposition 16.4. The order of 7 modulo 989 is the least common multiple of the order of 7 modulo 23 and the order of 7 modulo 43. It turns out that 7 is a primitive root modulo 23, so has order 22, while 7 has order 6 modulo 43. Thus modulo  $989 = 23 \cdot 43$ , 7 has order  $66 = [22, 6]$ .

Proposition 16.4 then says that the period of the sequence of squares starting with  $7^2 = 49$  is equal to the order of 2 modulo the odd part of 66. The odd part of 66 is 33, and the order of 2 modulo 33 is easily seen to be 10, because  $2^5 = 32 \equiv -1 \pmod{33}$ . So Proposition 16.4 is again verified.

Now we prove Proposition 16.4, which determines the period of a BBS sequence.

*Proof* Recall that we start a BBS sequence with a number  $y$  of order  $d$  modulo  $m$ , and we repeatedly square each element of the sequence to get the next element of the sequence. Thus the BBS sequence starting with  $y$  is

$$y, y^2, y^{2^2}, y^{2^3}, y^{2^4}, y^{2^5}, \dots, \pmod{m}.$$

To see when the sequence starts to repeat, we look for  $r$  and the smallest  $e > 0$  so that the exponents  $2^{r+e}$  and  $2^r$  of  $y$  are congruent modulo the order  $d$  of  $y$  modulo  $m$ . That is, we look for  $r$  and  $e > 0$  so that

$$2^{r+e} \equiv 2^r \pmod{d},$$

that is,

$$2^{r+e} \equiv 2^r \pmod{2^k f}.$$

The least  $e > 0$  for which this congruence holds is the period of the BBS sequence. Once this congruence holds for some  $r$ , it holds for  $r + 1, r + 2, \dots$ . So we can assume  $r \geq k$ . Then we have

$$2^r 2^e = 2^r + (2^k f)t$$

for some integer  $t$ . Since  $r \geq k$ , write  $r = k + g$  for some  $g \geq 0$ . Then we have

$$2^{k+g} 2^e = 2^{k+g} + (2^k f)t.$$

Cancel the common factor  $2^k$  in this last equation to leave

$$2^g 2^e = 2^g + ft.$$

Turn this into a congruence modulo  $f$ :

$$2^g 2^e \equiv 2^g \pmod{f}.$$

Since  $f$  is odd, 2 is a unit modulo  $f$ , so we can cancel the common factor  $2^g$  from both sides of the congruence to get

$$2^e \equiv 1 \pmod{f}.$$

The least  $e > 0$  for which this holds is the order of 2 modulo  $f$ . So the period of the BBS sequence is the order of 2 modulo  $f$ .  $\square$

**Achieving a long period in a BBS sequence.** One way to achieve a large order for 2 modulo  $d$  is to use a modulus  $m = pq$  where  $p$  and  $q$  are “special” primes.

**Definition** A prime  $p$  is *special* if  $p = 2p_1 + 1$  and  $p_1 = 2p_2 + 1$  where  $p, p_1$  and  $p_2$  are all prime numbers. So a special prime  $p$  is a safeprime (so that  $p = 2p_1 + 1$  where  $p_1$  is prime), with the extra property that  $p_1$  is also a safeprime:  $p_1 = 2p_2 + 1$  where  $p_2$  is prime.

Examples of special primes  $p$  with  $(p_1, p_2)$  include 23 (11, 5); 47 (23, 11); and 167 (83, 41). Note that if  $p$  is a special prime, then  $p \equiv 3 \pmod{4}$ .

We show

**Proposition 16.9** *If  $p$  and  $q$  are distinct special primes, that is, primes so that  $p - 1 = 2p_1$ ,  $p_1 - 1 = 2p_2$  and  $q - 1 = 2q_1$ ,  $q_1 - 1 = 2q_2$  with  $p_1, p_2, q_1, q_2$  primes, then for almost all starting numbers  $y$ , the BBS sequence has period at least  $p_2 q_2$ .*

For example, if  $p = 47$  and  $q = 167$ , then the period of the BBS sequence starting with 5 is  $\geq 11 \cdot 41 = 451$ .

*Proof* We show that for  $p \neq q$ , both safeprimes, if  $y$  is any number coprime to  $p$  and  $q$  and not congruent to 1 or  $-1$  modulo  $p$  and modulo  $q$ , then  $y$  has order  $p_1 q_1$  or  $2p_1 q_1$  modulo  $m$ .

For if  $y$  is coprime to  $p$  and not congruent to 1 or  $-1$  modulo  $p$ , then the order of  $y$  divides  $p - 1 = 2p_1$  where  $p_1$  is prime, and the order of  $y$  is not 1 or 2. So the order of  $y$  modulo  $p$  is  $p_1$  or  $2p_1$  modulo  $p$ .

Similarly, if  $y$  is coprime to  $q$  and not congruent to 1 or  $-1$  modulo  $q$ , then  $y$  has order  $q_1$  or  $2q_1$  modulo  $q$ .

Since  $p_1 \neq q_1$ , the order of  $y$  mod  $m$  is  $d = p_1 q_1$  or  $2p_1 q_1$  by Lemma 16.5.

Hence  $y$  will generate a BBS sequence with period equal to the order of 2 modulo  $p_1 q_1$ , the odd part of the order of  $y$  modulo  $pq$ .

The order of 2 modulo  $p_1 q_1$  is the least common multiple of the orders of 2 modulo  $p_1$  and modulo  $q_1$ . Because  $p$  and  $q$  are special primes, the order of 2 modulo  $p_1$  divides  $p_1 - 1 = 2p_2$ , and the order of 2 modulo  $q_1$  divides  $q_1 - 1 = 2q_2$ , where  $p_2$  and  $q_2$  are primes.

For  $p, q > 5$ , the order of 2 modulo  $p_1$  must be  $p_2$  or  $2p_2$ , and the order of 2 modulo  $q_1$  must be  $q_2$  or  $2q_2$ . Thus the order of 2 modulo  $f = p_1 q_1$  is at least  $[p_2, q_2] = p_2 q_2$ .

Hence the period of the BBS sequence starting from almost every  $y$  coprime to  $m$  is at least  $p_2 q_2$ .  $\square$

Since  $p = 4p_2 + 3$  and  $q = 4q_2 + 3$ , we have

$$p_2 q_2 = \frac{(p-3)(q-3)}{16}.$$

If  $p$  and  $q$  each have 50 digits, then  $p_2 q_2$  has at least 98 digits.

*Example 16.10* Let  $m = 167 \cdot 47 = 7849$ , the product of two special primes. Consider the sequence

$$7, 7^2, 7^{2^2}, 7^{2^3}, 7^{2^4}, 7^{2^5}, \dots \pmod{7849}.$$

It turns out that 7 has order 83 modulo 167 and order 23 modulo 47, so has order  $83 \cdot 23 = 1909 = d = 2^e f$  modulo 7849. Since 1909 is odd, the period of the sequence is then the order of 2 modulo 1909. The order of 2 modulo 83 is 82, and the order of 2 modulo 23 is 11. So the order of 2 modulo  $f = 1909$  is  $[82, 11] = 902$ . Hence the sequence of squares modulo 7849 starting from 7 has period 902.

If we start the BBS sequence with 10, then the sequence has period  $[41, 11] = 451$ , because 10 has order 41 modulo 83 and order 11 modulo 23.

The question arises whether or not large special primes can be found. It is conjectured that there are arbitrarily large special primes. I found some respectably large special primes using the “safeprime” command in MAPLE,

$$(p_2, p_1, p) = (5130431863961, 10260863727923, 20521727455847)$$

and

$$(q_2, q_1, q) = (6553710049871, 13107420099743, 26214840199487)$$

in almost no time. For these 14-digit special primes, if  $m = pq$ , then the period of a BBS sequence starting from almost every random number  $y$  will be at least  $p_2 \cdot q_2 \geq 10^{25}$ .

## 16.5 Recreating a BBS Sequence from the Last Term

The feature of the BBS sequence that makes it potentially useful for cryptography is that with knowledge of how the modulus  $m$  factors, Bob can recreate a BBS sequence starting from the last term of the sequence.

To obtain that feature, we choose the modulus  $m$  to be the product of two primes, each  $\equiv 3 \pmod{4}$ . Then we have:

**Proposition 16.11** *Let  $m = pq$  with  $p$  and  $q$  distinct primes of the form  $p = 2p_1 + 1, q = 2q_1 + 1$  with  $p_1, q_1$  odd numbers (so that both  $p$  and  $q$  are congruent to 3 modulo 4). Let  $S_m$  be the subgroup of squares of the group of units  $U_m$  of  $\mathbb{Z}_m$ . Then the squaring function  $g_2 : S_m \rightarrow S_m$  is bijective with inverse  $\omega : S_m \rightarrow S_m$  defined by*

$$\omega(z) \equiv z^{\frac{p_1 q_1 + 1}{2}}.$$

*Proof* If  $z$  is a square in  $U_m$ , then every power of  $z$  is also a square. So  $g_2$  and  $\omega$  both send squares to squares in  $U_m$ , so are maps from  $S_m$  to  $S_m$ . To show they are inverse maps, we show that  $g_2\omega$  and  $\omega g_2$  are the identity maps on  $S_m$ . To do so, we show that for  $z$  in  $S_m$ ,

$$(z^2)^{\frac{p_1 q_1 + 1}{2}} \equiv z \pmod{m}.$$

But  $z$  is in  $S_m$ , so  $z \equiv w^2 \pmod{m}$  for some  $w$  in  $U_m$ . Then  $z \equiv w^2 \pmod{p}$  and  $z \equiv w^2 \pmod{q}$ . So

$$z^{p_1} \equiv w^{2p_1} \equiv w^{p-1} \equiv 1 \pmod{p};$$

also

$$z^{q_1} \equiv w^{2q_1} \equiv w^{q-1} \equiv 1 \pmod{q};$$

both by Fermat's Theorem. Thus

$$z^{p_1 q_1} \equiv 1 \pmod{p},$$

so

$$z^{p_1 q_1 + 1} \equiv z \pmod{p};$$

and the same is true modulo  $q$ . Since  $m = pq$ , we have

$$z^{p_1 q_1 + 1} \equiv z \pmod{m}.$$

Thus

$$(z^2)^{\frac{p_1 q_1 + 1}{2}} \equiv z^{p_1 q_1 + 1} \equiv z \pmod{m}.$$

This shows that the squaring map  $g_2$  and the “raising to the  $(p_1 q_1 + 1)/2$  power” map  $\omega$  are inverses of each other as functions on the subgroup  $S_m$  of squares of units modulo  $m$ .  $\square$

Proposition 16.11 shows how Bob can reconstruct a BBS sequence starting from Alice's key: he successively applies the function  $\omega$ , defined by

$$\omega(z) = z^{\frac{p_1 q_1 + 1}{2}}.$$

**Definition** Let  $m = pq$  with  $p, q$  both congruent to 3 modulo 4. Since  $g_2$  is a one-to-one function on  $S_m$ , for each element  $c$  of  $S_m$  there is a unique element  $b$  of  $S_m$  whose square is  $c$ , namely, the number  $b = \omega(c)$  given by applying inverse function  $\omega$  of  $g_2$  to  $c$ . The unique element  $b = \omega(c)$  of  $S_m$  that is both a square in  $U_m$  and a square root of  $c$  will be called the *square square root* of  $c$ .

*Example 16.12* Let  $p = 43 = 2 \cdot 21 + 1$ ,  $q = 31 = 2 \cdot 15 + 1$ . Then  $m = 1333$  and

$$\omega(x) = \frac{15 \cdot 21 + 1}{2} = 158.$$

If we begin with  $x_0 = 2$ , and continually square modulo 1333, we obtain the sequence

$$4, 16, 256, 219, 1306, 729, 188, 686, 47, 876, 901, 4, 16, \dots$$

If we begin with 16 and continually raise to the 158-th power modulo 1333, we obtain the sequence

$$4, 901, 876, 47, 686, 188, 729, 1306, 219, 256, 16, 4, 901 \dots$$

Thus the unique square square root modulo 1333 of 4 is 901, the unique square square root of 901 modulo 1333 is 876, etc. Notice that since 2 is not a square modulo 1333, the square square root of 4 is not 2, but  $901 \equiv 876^2 \pmod{1333}$ . Similarly,  $1306 \equiv -27 \equiv 219^2$  is the unique square square root of  $729 = 27^2$  modulo 1333. The number 27 is a square root of 729, but 27 is not a square modulo 1333.

The period of the BBS sequence is 12. This aligns with the theory in the last section. The order of 4 modulo 1333 =  $43 * 31$  is the least common multiple of the order of 4 modulo 43, namely 7, and the order of 4 modulo 31, namely 5. So the order of 4 mod 1333 is 35. Then the order of 2 mod 35 is the least common multiple of the order of 2 mod 7 (namely 3) and the order of 2 mod 5 (namely 4). So the order of 2 mod 35 is 12. Hence the period of the BBS sequence for  $m = 1333$  beginning with  $x_0 = 4$  is 12.

## 16.6 Security of the B-G Cryptosystem

In order for Eve to crack a B-G cryptosystem, Eve needs to take the key  $\kappa = x_{n+1}$  that Alice sent Bob, the number just past the end of the BBS sequence used for encrypting, and from it, reconstruct the pseudorandom sequence  $x_1, \dots, x_n$  that Alice used to encrypt her message. We show:

**Proposition 16.13** Suppose Eve can take any square  $c$  in  $S_m$  and find its unique square square root. Then with arbitrarily high probability, Eve can find the prime factorization of the modulus  $m$ .

This means: in practice, if Eve can't factor  $m$ , then Eve doesn't have a method for finding the square square root of a square, so Eve doesn't have a method for decrypting a B-G message.

Here is the idea.

**Proposition 16.14** Let  $b$  be an element of  $U_m$ . Let  $c = b^2$ . Then  $c$  is in  $S_m$ , the subgroup of the group of units  $U_m$  consisting of the squares of units. Let  $b_0$  be the square square root of  $c$ . If  $b_0 \neq b$  and  $b_0 \neq -b$  in  $U_m$ , then the greatest common divisors  $(m, b - b_0)$  and  $(m, b + b_0)$  are the factors  $p$  and  $q$  of  $m$ .

*Proof* If  $b \not\equiv b_0 \pmod{m}$ , then  $m$  does not divide  $b - b_0$ . If also  $b \not\equiv -b_0 \pmod{m}$ , then  $m$  does not divide  $b + b_0$ . But

$$(b - b_0)(b + b_0) = b^2 - b_0^2 \equiv c - c = 0 \pmod{m}.$$

So  $m$  divides  $(b - b_0)(b + b_0)$ . If  $m$  were coprime to  $b - b_0$ , then by the Coprime Divisibility Lemma,  $m$  would divide  $b + b_0$ , which we assumed above is not the case. If  $m$  were coprime to  $b + b_0$ , then  $m$  would divide  $b - b_0$ , also contrary to what we assumed. So the greatest common divisors  $(m, b - b_0)$  and  $(m, b + b_0)$  must be non-trivial proper factors of  $m$ , hence one must be  $p$  and the other  $q$ .  $\square$

So Eve's strategy is the following. She picks a random element  $b$  of  $U_m$ . Let  $c = b^2$  in  $S_m$ . Let  $b_0$  be the square square root of  $c$ . If  $b$  in  $U_m$  is not congruent to the square square root of  $b^2$  or the negative of the square square root of  $b^2$ , then she will be able to factor  $m$ . Let's call the act of picking a random  $b$  and comparing it to the square square root of  $b^2$  a *factor trial*.

If  $b$  is congruent to  $b_0$  or  $-b_0$ , the factor trial fails. She discards  $b$  and picks another random  $b$  and repeats. She keeps doing this until she finds some  $b$  for which the factor trial is a success.

What is the chance that a random element  $b$  of  $U_m$  will give a factorization of  $m$ ?

To see this, we will look at the cosets of  $S_m$  in  $U_m$ .

The group  $S_m$  of squares of units of  $\mathbb{Z}_m$  is a subgroup of  $U_m$ , so has cosets. Each coset of  $S_m$  contains the same number of elements as  $S_m$ , so the number of elements in  $S_m$ , multiplied by the number of cosets of  $S_m$  (= the index of  $S_m$  in  $U_m$ ) is equal to the order of  $U_m$  (Lagrange's Theorem).

We will show that there are at least four cosets of  $S_m$  in  $U_m$ .

To do so, we need

**Lemma 16.15** (Euler's Lemma) *Let  $p$  be an odd prime number and let  $a$  be in  $U_p$ , the group of units of  $\mathbb{Z}_p$ . Then  $a$  is a square modulo  $p$  if and only if*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

*Proof* We get half of this easily: if  $a \equiv c^2 \pmod{p}$  for some  $b$ , then by Fermat's Theorem,

$$a^{\frac{p-1}{2}} \equiv (c^2)^{\frac{p-1}{2}} = c^{p-1} \equiv 1 \pmod{p}.$$

For the other half, suppose

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Let  $c$  be a primitive root modulo  $p$ . Then the group  $U_p$  of units modulo  $p$  is the cyclic group generated by  $c$ , so  $a \equiv c^s \pmod{p}$  for some exponent  $s$ . Replacing  $a$  by  $c^s$  in the congruence gives

$$(c^s)^{\frac{p-1}{2}} = c^{\frac{s(p-1)}{2}} \equiv 1 \pmod{p}.$$

Since  $c$  is a primitive root modulo  $p$ , the order of  $c$  is  $p - 1$ . Therefore  $p - 1$  divides  $\frac{s(p-1)}{2}$ . So for some integer  $t$ ,

$$2(p-1)t = s(p-1),$$

so  $s = 2t$ , and so  $a \equiv c^s \equiv (c^t)^2 \pmod{p}$  is a square in  $U_p$ .  $\square$

An immediate consequence of Euler's Lemma is:

**Corollary 16.16** *Let  $p$  be an odd prime number. If  $p \equiv 3 \pmod{4}$ , then  $-1$  is not a square modulo  $p$ .*

For if  $p \equiv 3 \pmod{4}$ , then  $p - 1 \equiv 2 \pmod{4}$ , so  $\frac{p-1}{2}$  is odd, and  $-1$  raised to an odd power is  $= -1$ . So by Euler's Lemma,  $-1$  is not a square.

Now we look at cosets.

Let  $m = pq$  with  $p, q$  congruent to 3 modulo 4.

Let  $z$  be the unique number modulo  $pq$  satisfying the pair of congruences

$$\begin{aligned} z &\equiv 1 \pmod{p} \\ z &\equiv -1 \pmod{q}. \end{aligned}$$

**Lemma 16.17** *The cosets  $S_m$ ,  $(-1)S_m$ ,  $zS_m$  and  $(-z)S_m$  are disjoint cosets in  $U_m$ .*

*Proof* We characterize the elements of the four cosets.

An element  $c$  is in  $S_m$  if  $c = b^2$  for some  $b$  in  $U_m$ . Viewing  $b, c$  as integers,  $c \equiv b^2 \pmod{m}$ . Since  $m = pq$ , it follows that

$$\begin{aligned} c &\equiv b^2 \pmod{p} \\ c &\equiv b^2 \pmod{q}. \end{aligned}$$

That is,  $c$  is a square modulo  $p$  and  $c$  is a square modulo  $q$ .

An element  $c$  is in  $(-1)S_m$  if  $c = -b^2$  for some  $b$  in  $U_m$ . Then

$$\begin{aligned} c &\equiv -b^2 \pmod{p} \\ c &\equiv -b^2 \pmod{q}. \end{aligned}$$

Since  $-1$  is not a square modulo  $p$  or  $q$ , and a square times a non-square is a non-square, it follows that  $c$  is a non-square modulo both  $p$  and mod  $q$ . So  $c$  cannot be in  $S_m$ . So  $(-1)S_m$  and  $S_m$  are disjoint cosets of  $U_m$ .

An element  $c$  is in  $zS_m$  if  $c = zb^2$  for some  $b$  in  $U_m$ . Then

$$\begin{aligned} c &\equiv zb^2 \equiv b^2 \pmod{p} \\ c &\equiv zb^2 \equiv -b^2 \pmod{q}. \end{aligned}$$

So  $c$  is a square modulo  $p$ , but is not a square modulo  $q$ . So  $c$  can't be in  $S_m$  or in  $(-1)S_m$ . So  $zS_m$  is a different coset from  $S_m$  and  $(-1)S_m$ .

Finally, an element  $c$  is in  $(-z)S_m$  if  $c = (-z)b^2$  for some  $b$  in  $U_m$ . Then

$$\begin{aligned} c &\equiv (-z)b^2 \equiv -b^2 \pmod{p} \\ c &\equiv (-z)b^2 \equiv b^2 \pmod{q}. \end{aligned}$$

So  $c$  is not a square modulo  $p$ , but is a square modulo  $q$ . So  $c$  can't be in  $S_m$  or in  $(-1)S_m$  or  $zS_m$ . So  $(-z)S_m$  is a different coset from the other three. This proves the lemma.  $\square$

**Proposition 16.18** *The probability that a factor trial using a randomly selected  $b$  will factor  $m$  is at least  $1/2$ .*

For suppose we pick a random  $b$  in  $U_m$ . If  $b$  is in  $S_m$  or in the coset  $(-1)S_m$ , then the factor trial using  $b$  fails, because  $b \equiv b_0$  or  $-b_0$  modulo  $m$ . But if  $b$  is not in the coset  $S_m$  or the coset  $(-1)S_m$ , then the factor trial using  $b$  will succeed in factoring  $m$ . And there are at least four cosets of  $S_m$  in  $U_m$ .

Only two of those cosets contain elements  $b$  for which the factor trial using  $b$  fails. If  $b$  is in any other coset of  $S_m$ , the factor trial using  $b$  succeeds. Every coset of  $S_m$  in  $U_m$  contains the same number of elements, so the probability that our randomly chosen  $b$  is in one of the cosets  $S_m$  or  $(-1)S_m$  is  $\leq 1/2$ .

**Corollary 16.19** *The probability of failing to find a factorization of  $m$  after  $k$  random factor trials is  $\leq 1/(2^k)$ .*

To sum up, if Eve can find the square square root of elements of  $S_m$ , then unless she is amazingly unlucky, Eve can factor  $m$ .

So if Eve can't factor  $m$ , it's safe to assume that she can't find square square roots either. So she can't decrypt messages using a BBS sequence modulo  $m$ .

## 16.7 Implementation of the Blum-Goldwasser Cryptosystem

**Encryption.** Let us assume that the modulus  $m$  is a product of two 308 digit prime numbers  $p$  and  $q$ , so  $m$  is a 616 digit, or 2048 bit modulus. (This was the size recommended for an RSA modulus in 2015 for moderately high security.) Bob sends Alice the number  $m$ .

Following guidelines of Menezes, van Oorschot, and Vanstone [MvOV96], Alice takes a message to be encrypted and splits it up into a sequence  $\bar{w} = (w_1, w_2, \dots, w_t)$  of words, where each word  $w_i$  is a sequence of  $\log_2(2048) = 11$  bits.

To encrypt  $\bar{w}$ , Alice chooses a random number  $x_0 < m$  and computes the sequence

$$x_1 \equiv x_0^2 \pmod{m}, x_2 \equiv x_1^2 \pmod{m}, \dots, x_{t+1} \equiv x_t^2 \pmod{m}.$$

To encrypt  $\bar{w}$ , let

$$u_i \equiv x_i \pmod{2^{11}}$$

for  $i = 1, \dots, t$ , write  $u_i$  in base 2 to obtain an 11-tuple  $k_i$  of bits, and let

$$\bar{k} = (k_1, \dots, k_t),$$

a vector of  $11t$  bits.

The encrypted message is then

$$\bar{c} = \bar{w} + \bar{k}$$

where the addition is of vectors over  $\mathbb{F}_2$ .

**Decryption.** In order to decrypt  $\bar{c}$ , Bob needs to reconstruct the sequence  $x_1, x_2, \dots, x_t \pmod{m}$  starting from  $x_{t+1}$ . Instead of finding  $x_t, x_{t-1}, \dots$  by computing

$$x_r \equiv \omega(x_{r+1}) = x_{r+1}^{\frac{p_1 q_1 + 1}{2}} \pmod{m}$$

for  $r = t, t-1, \dots, 1$  directly, where  $p = 2p_1 + 1, q = 2q_1 + 1$ , [MvOV96] suggests a three-step process, analogous to using the Chinese Remainder Theorem to decrypt an RSA encryption.

The first step applies the following mod  $p$  version of Proposition 16.4 :

**Proposition 16.20** *For  $p$  a prime with  $p \equiv 3 \pmod{4}$ , the squaring function  $g_2 : S_p \rightarrow S_p$  on the group of squares modulo  $p$ , given by*

$$g_2(u) \equiv u^2 \pmod{p}$$

*is bijective with inverse  $\theta_p : S_2 \rightarrow S_2$ , given by*

$$\theta_p(u) \equiv u^{\frac{p+1}{4}} \pmod{m}.$$

*Proof* It suffices to show that for all squares  $u$ ,

$$u^{2(\frac{p+1}{4})} \equiv u \pmod{p}.$$

But

$$u^{2(\frac{p+1}{4})} = u^{\frac{p-1}{2}+1} \equiv u^{\frac{p-1}{2}} u \pmod{p}.$$

Since  $u$  is a square modulo  $p$ , Euler's Lemma says that

$$u^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

So  $g_2$  and  $\theta_p$  are inverse maps on the group  $S_p$  of squares modulo  $p$ .  $\square$

So instead of applying  $\omega : S_m \rightarrow S_m$  successively  $t$  times to reconstruct the sequence  $x_1, x_2, \dots, x_t$ , the idea is to

- (1) immediately compute  $x_1$  modulo  $p$ , and  $x_1$  modulo  $q$ , then
- (2) find  $x_1$  modulo  $m$  by the Chinese Remainder Theorem, and finally
- (3) compute Alice's encrypting sequence just the way she did, by finding  $x_{i+1} \equiv x_i^2 \pmod{m}$  for  $i = 1, \dots, t$ .

For the first step, to obtain  $x_1 \pmod{p}$  directly from  $x_{t+1}$ , we find

$$d_t = (\frac{p+1}{4})^t \pmod{p-1}$$

and then compute

$$u = x_{t+1}^{d_t} \pmod{p}.$$

Then do the same modulo  $q$ : find

$$e_t = (\frac{q+1}{4})^t \pmod{q-1}$$

and then compute

$$v = x_{t+1}^{e_t} \pmod{q}.$$

Then

$$u \equiv x_1 \pmod{p}, \quad v \equiv x_1 \pmod{q}$$

The second step is to find  $x_1$  by solving the pair of congruences

$$\begin{aligned} x &\equiv u \pmod{p} \\ x &\equiv v \pmod{q}. \end{aligned}$$

The solution will be  $x_1 \pmod{m}$ . As with RSA decrypting, Bob can solve that pair of congruences quickly by finding in advance Bezout's Identity for  $p$  and  $q$ :

$$1 = qa + pb.$$

Then  $x_1 = uqa + vpb \pmod{m}$ .

Finally, once  $x_1$  is found, then finding  $x_2, \dots, x_t$  is done by squaring  $x_1 \pmod{m}$ . Then Bob can construct the key  $\bar{k}$  in the same way Alice did. With the key  $\bar{k}$  in hand, Bob obtains Alice's plaintext message  $\bar{w}$  from her encrypted message  $\bar{c}$  by adding vectors in  $\mathbb{F}_2$ :

$$\bar{w} = \bar{c} + \bar{k}.$$

*Example 16.21* Let  $m = 989 = 23 \cdot 43$ . Alice wants to send Bob

$$\bar{w} = (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0).$$

She chooses  $x_0 = 49$ , then the sequence

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (423, 909, 466, 565, 767, 823).$$

Now 989 is a 10-bit number in base 2, and  $3 < \log_2 < 4$ . So following [MvOV96], we break up Alice's message into a sequence of five 3-bit words,

$$\bar{w} = (w_1, w_2, w_3, w_4, w_5) = (1, 1, 1; 0, 1, 1; 1, 0, 1; 0, 0, 0; 1, 1, 0).$$

Keeping  $x_6 = 823$  to send to Bob to reproduce the key, Alice takes the encrypting sequence and reduces in modulo 8 to get

$$(423, 909, 466, 565, 767) \equiv (7, 5, 2, 5, 7) \pmod{8}.$$

Writing  $(7, 5, 2, 5, 7)$  as bits, she obtains the key  $\bar{k} = (1, 1, 1; 1, 0, 1; 0, 1, 0; 1, 0, 1; 1, 1, 1)$ . Then viewing  $\bar{w}$  and  $\bar{k}$  as vectors of elements of  $\mathbb{F}_2$  with 15 components, she finds the encrypted vector:

$$\begin{aligned} \bar{c} &= \bar{w} + \bar{k} \\ &= (1, 1, 1; 0, 1, 1; 1, 0, 1; 0, 0, 0; 1, 1, 0) + (1, 1, 1; 1, 0, 1; 0, 1, 0; 1, 0, 1; 1, 1, 1) \\ &= (0, 0, 0; 1, 1, 0; 1, 1, 1; 1, 0, 1; 0, 0, 1). \end{aligned}$$

(Addition is componentwise modulo 2.) Alice sends Bob

$$(\bar{c}, \kappa) = ((0, 0, 0; 1, 1, 0; 1, 1, 1; 1, 0, 1; 0, 0, 1), 823).$$

Bob knows  $m = 989 = 23 \cdot 43$  and that Alice's message requires a sequence five numbers long. So he has computed ahead of time

$$\left(\frac{p+1}{4}\right)^5 = \left(\frac{43+1}{4}\right)^5 \equiv 11^5 \equiv 23 \pmod{43}$$

and

$$\left(\frac{q+1}{4}\right)^5 = \left(\frac{23+1}{4}\right)^5 \equiv 6^5 \equiv 10 \pmod{23}.$$

When he gets Alice's key  $\kappa = 823$ , he computes

$$\begin{aligned} u &= 823^{23} \equiv 6^{23} \equiv 36 \pmod{43}, \text{ and} \\ v &= 823^{10} \equiv 18^{10} \equiv 9 \pmod{23}. \end{aligned}$$

So

$$\begin{aligned} x_1 &\equiv 36 \pmod{43} \\ x_1 &\equiv 9 \pmod{23}. \end{aligned}$$

Knowing  $p$  and  $q$ , Bob already has Bezout's identity for  $p$  and  $q$ :

$$1 = 23 \cdot 15 - 43 \cdot 8 = 345 - 344.$$

So he computes

$$\begin{aligned} x_1 &= 36 \cdot 345 + 9 \cdot (-344) \\ &= 12420 - 3096 = 9324 \equiv 423 \pmod{989}. \end{aligned}$$

Once Bob finds  $x_1 = 423$ , he obtains the rest of the sequence by squaring modulo 989 to obtain Alice's sequence  $(423, 909, 466, 565, 767)$ , reduces the sequence modulo 8 to get the key  $\bar{k} = (1, 1, 1; 1, 0, 1; 0, 1, 0; 1, 0, 1; 1, 1, 1)$  and recovers Alice's message  $\bar{w} = \bar{c} + \bar{k}$ .

**Decrypting mod  $p$  and  $q$ .** The decrypting method on  $U_p$  and  $U_q$ , just described and illustrated, gives the same results as the decrypting method in  $U_m$  described in Section 16.3. To see this, we place the two decryption methods into the setting of the end of Chapter 12. There, we showed that if  $m = pq$  with  $p, q$  distinct primes, then

$$U_m \cong U_p \times U_q,$$

where the map from  $U_m$  to  $U_p \times U_q$  is given by sending  $b$  in  $U_m$  to  $(b \bmod p, b \bmod q)$ . This map is an isomorphism, with inverse

$$B : U_p \times U_q \rightarrow U_m$$

given by  $B(a, b) = asq + btp$  where Bezout's identity for  $p$  and  $q$  is

$$1 = sq + tp.$$

(This use of Bezout's identity is how we obtained the Chinese Remainder Theorem for two congruences in Section 11.1.)

The isomorphism between  $U_m$  and  $U_p \times U_q$  is easily seen to restrict to an isomorphism

$$S_m \cong S_p \times S_q$$

between the group of squares modulo  $m$  and the direct product of the groups of square modulo  $p$  and  $q$ . (See Exercise 16.6.)

This last isomorphism suggests that in doing computations in  $S_m$ , such as recreating a BBS sequence from its last term, it is possible, and more efficient, to pass from  $S_m$  to  $S_p \times S_q$ , do the computations in  $S_p$  and  $S_q$  separately and then use the CRT to go back to  $S_m$  at the end. This is in fact what we did in Example 16.21.

We want to explain the method in some generality.

Let  $m = pq$  where  $p$  and  $q$  are distinct primes of the form  $p = 2p_1 + 1, q = 2q_1 + 1$  with  $p_1, q_1$  odd. Recall that  $g_2 : S_m \rightarrow S_m$  is the squaring function:  $g_2(b) = b^2$ . We have also the map

$$\omega : S_m \rightarrow S_m, \omega(b) = b^{\frac{p_1 q_1 + 1}{2}}.$$

Then  $\omega$  and  $g_2$  are inverse functions from  $S_m$  to  $S_m$ .

On  $S_p$ , we have the map  $\theta_p : S_p \rightarrow S_p$ , given by  $\theta_p(b) = b^{\frac{p+1}{4}}$ . Then  $\theta_p$  and  $g_2$  are inverse functions from  $S_p$  to  $S_p$ , and similarly on  $S_q$ .

We will show: modulo  $p$ , the map  $\omega$  coincides with the map  $\theta_p$ .

More precisely, if we begin with  $b$  in  $S_m$ , map it to  $S_p$  by sending  $b$  to  $(b \bmod p)$ , and then apply  $\theta_p$ , the result is the same as beginning with  $b$ , applying the map  $\omega$ , and then reducing modulo  $p$ :

**Proposition 16.22** *For  $b$  in  $S_m$ ,*

$$\theta_p(b \bmod p) = (\omega(b) \bmod p).$$

*Proof* First note that since  $b$  is in  $S_m$ ,  $b \equiv c^2 \pmod{m}$  for some  $c$  in  $U_m$ . So  $b \equiv c^2 \pmod{p}$  and  $(c \bmod p)$  is in  $S_p$ .

Now, to find the right side we look at  $\omega(b)$  modulo  $p$ . We have

$$\omega(b) = b^{\frac{p_1 q_1 + 1}{2}}.$$

Since  $q_1 = 1 + 2k$  is odd, the exponent is

$$\begin{aligned}\frac{p_1 q_1 + 1}{2} &= \frac{p_1(1 + 2k) + 1}{2} \\ &= \frac{p_1 + 1}{2} + p_1 k.\end{aligned}$$

So modulo  $p$ ,

$$\begin{aligned}b^{\frac{p_1 q_1 + 1}{2}} &\equiv b^{\frac{p_1 + 1}{2}} b^{p_1 k} \\ &\equiv b^{\frac{p+1}{4}} \cdot (c^{2p_1})^k \\ &\equiv \theta_p(b) \pmod{p}\end{aligned}$$

since

$$c^{2p_1} = c^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Theorem.  $\square$

We can describe visually what we just proved using a diagram of maps:

$$\begin{array}{ccc} S_m & \xrightarrow{\omega} & S_m \\ \text{mod } p \downarrow & & \text{mod } p \downarrow \\ S_p & \xrightarrow{\theta_p} & S_p \end{array} \quad (16.1)$$

The diagram is “commutative”, in the sense that if you start with an element  $b$  in  $S_m$ , and map it down by  $\text{mod } p$  and then over by  $\theta_p$ , the resulting element of  $S_p$  is the same as if you map  $b$  over by  $\omega$  and then down by  $\text{mod } p$ : getting from the upper left to the lower right is the same by either route.

Iterating what we proved in Proposition 16.22 yields two different ways for Bob to get from  $x_{t+1}$  to  $x_1$  to recreate Alice's BBS sequence. He can apply  $\omega t$  times on  $S_m$ , or he can pass by  $(\text{mod } p, \text{ mod } q)$  to  $S_p \times S_q$ , apply  $\theta_p \times \theta_q t$  times on  $S_p \times S_q$ , and then go back to  $S_m$ . We can express the content of this last sentence by saying that the following diagram is commutative:

$$\begin{array}{ccc} S_m & \xrightarrow{\omega^{ot}} & S_m \\ (\text{mod } p, \text{ mod } q) \downarrow & & B \uparrow \\ S_p \times S_q & \xrightarrow{\theta_p^{ot} \times \theta_q^{ot}} & S_p \times S_q \end{array} \quad (16.2)$$

Here  $B : S_p \times S_q \rightarrow S_m$  is the inverse of the  $(\text{mod } p, \text{ mod } q)$  map, given by

$$B(a, b) = asq + btp \pmod{m}$$

where Bezout's identity for  $p$  and  $q$  is  $1 = sq + tp$ .

The conclusion from this is that we can get from the key  $\kappa = x_{t+1}$  to the first element  $x_1$  of the Blum-Goldwasser sequence either by directly applying  $\omega t$  times on  $x_{t+1}$  in  $S_m$ , or by passing to  $(x_{t+1} \text{ mod } p, x_{t+1} \text{ mod } q)$  in  $S_p \times S_q$ , then applying  $\theta_p \times \theta_q t$  times, and then moving back to  $S_m$ .

**Conclusions.** Using the decryption method working in  $S_p \times S_q$ , [MvOV96] suggests that the speed of encryption and decryption using a Blum-Goldwasser sequence is comparable to that of RSA.

They say, however, that “the Blum-Goldwasser scheme is vulnerable to a chosen-ciphertext attack that recovers the private key from the public key. It is for this reason that the Blum-Goldwasser scheme has not received much attention in practice.”

## Exercises

- 16.1. Alice wants to send Bob the letter “w”. Alice and Bob have agreed to use the modulus  $m = 209$ , as in Example 3. Alice decides to begin a BBS sequence with  $x_0 = 29$ . What does Alice send Bob?
- 16.2. In Example 16.3 with  $m = 209$ , Bob receives from Alice the pair  $((1, 1, 0, 1, 0), 104)$ . What letter did Alice send Bob? [You may want to utilize a modular power calculator in this problem.]
- 16.3. Suppose Bob chooses a modulus  $m = pq$ , sends  $m$  to Alice, and Alice picks a random starting value for a BBS sequence that happens to be a multiple of  $p$ . If Alice uses the resulting BBS sequence to send a message to Bob, will Bob be able to decrypt Alice’s message? Will Eve?
- 16.4. Consider the BBS sequence for  $m = 47 \cdot 83 = 3901$ , starting from  $y_0 = 5$ . What is its period?
- 16.5. (i) What is the the period of the BBS sequence for  $m = 1333 = 31 \cdot 43$ , starting from  $y = 7$ ? Find the orders of 7 modulo 31 and modulo 43.  
 (ii) Show that the period of the BBS sequence for  $m = 1333 = 31 \cdot 43$  starting from any unit  $y_0$  cannot be larger than 12.
- 16.6. Show that if  $m = rs$  with  $(r, s) = 1$ , then the map given by

$$(a \bmod m) \mapsto (a \bmod r, a \bmod s)$$

defines an isomorphism from  $S_m$  to  $S_r \times S_s$ . Show that the inverse map is the map that sends  $(b \bmod r, c \bmod s)$  to  $(a \bmod m)$ , where if Bezout’s identity for  $r$  and  $s$  is  $1 = zr + ws$ , then

$$a = wsb + zrac.$$

- 16.7. Let  $m = 21$ . In Lemma 16.17, find the number  $z$  so that  $z \equiv 1 \pmod{3}$  and  $z \equiv -1 \pmod{7}$  and list the elements of each of the cosets  $S_m$ ,  $-S_m$ ,  $zS_m$  and  $-zS_m$ . Show that every element of  $U_{21}$  is in exactly one of those cosets, so that the index of  $S_m$  in  $U_m$  is 4.
- 16.8. Generalize the last exercise:
  - (i) Show that the index of  $S_p$  in  $U_p$  is 2 for every odd prime  $p$ .
  - (ii) Show that if  $m = pq$  where  $p, q$  are distinct primes, then the index of  $S_m$  in  $U_m$  is 4. (Use Exercise 16.6 that  $S_m \cong S_p \times S_q$ .)
- 16.9. Find the four square roots of 100 in  $U_{209}$ . Identify the square square root of 100.
- 16.10. Find all solutions of the equation  $x^2 = 1$  in  $U_{65}$ . Which of your solutions are in the subgroup  $S_{65}$  of squares modulo 65?

- 16.11. An element  $b$  of  $U_m$  is a square and has a square square root if and only if  $b$  is the fourth power of an element of  $U_m$ .
- (i) Find all the elements of  $U_{17}$  that are fourth powers.
  - (ii) Find all the elements of  $U_{19}$  that are fourth powers.
- 16.12. Let  $p$  be an odd prime. Using Euler's Lemma, show that the squaring map  $g_2$  from  $S_p$  to  $S_p$  is a one-to-one function if and only if  $p \equiv 3 \pmod{4}$ .

# Chapter 17

## Factoring by the Quadratic Sieve



The RSA and Blum-Goldwasser cryptosystems introduced in Chapters 9 and 16 rely for their security on the difficulty of factoring a large number into a product of primes. The Diffie-Hellman key exchange relies on its security on the difficulty of finding the discrete logarithm of a given element of cyclic group. Since those cryptosystems were introduced in the 1970s, much research has focused on trying to find fast methods for factoring, and for finding discrete logarithms. With the widespread use of encryption throughout the internet, those research efforts are, if anything, intensifying.

As an introduction to this research, we introduce in this chapter two similar algorithms, the quadratic sieve method for factoring, proposed in 1982, and the index calculus method for finding discrete logarithms, developed in the late 1970s.

We begin with some elementary methods for factoring numbers.

### 17.1 Trial Division

The best known way to factor a number  $m$  is to try dividing  $m$  by numbers  $2, 3, 4, 5, \dots$ , until either we find a number  $d$  that is a divisor of  $m$ , that is, so that  $m/d = q$  is an integer, or we reach the largest number  $\leq \sqrt{m}$  without finding a divisor of  $m$ , in which case  $m$  is prime.

For example, to try to factor 319, we divide 319 by 2, 3, 4, 5, ... until we find that  $319 = 11 \cdot 29$ . To try to factor 317, we divide 317 by 2, 3, 4, 5, ... until we reach 17, the largest integer  $< \sqrt{317} = 17.8$ . Since none of those numbers divide 317, then 317 must be prime. (We can stop at 17 because, by Exercise 4.16, every composite number  $m$  is divisible by a number  $d \leq \sqrt{m}$ .)

Trial division is slow—it takes about  $\sqrt{m}$  divisions before one can be certain that  $m$  is prime, and nearly that many divisions to obtain a factorization of  $m$  if  $m$  is the product of two primes both close to  $\sqrt{m}$ . For example, to factor  $m = 98,929,813$  would require trial dividing by numbers almost up to 9946, the largest integer  $< \sqrt{m}$ , to discover that 9833 is a factor of  $m$ .

If  $m = pq$  is an RSA modulus and  $p$  and  $q$  are 100 digit prime numbers, trying to factor  $m$  by trial division is hopeless.

There are ways to make trial division slightly more efficient. Instead of trial dividing by all numbers up to  $\sqrt{m}$ , we could restrict trial division to division by primes  $< \sqrt{m}$ . But that requires having a list of those primes. An easier, low-memory alternative is to trial divide  $m$  by 2, 3 and 5, and then trial divide  $m$  only by numbers not divisible by 2, 3 or 5. It is a routine exercise involving the Chinese Remainder Theorem to show that a number  $d > 5$  is coprime to 2, 3 and 5 if and only if  $d$  is congruent to 1, 7, 11,

13, 17, 19, 23 or 29 (mod 30). So we can trial divide  $m$  only by numbers satisfying one of those eight congruences modulo 30. We'll call this "mod 30 trial division".

If we are trying to factor  $m$ , and  $r$  is the smallest prime divisor of  $m$ , it would take approximately  $8/30r$  mod 30 trial divisions before we find the divisor  $r$  of  $m$ .

For example, to factor 20081 (which is easily seen to be not divisible by 2, 3 or 5), we could trial divide by 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 and 43, at which point we discover that  $20081 = 43 \cdot 467$ .

Trial division works fairly quickly on a number  $m$  that has a small prime factor, and slowly on a number  $m$  that factors into a product of two primes close to  $\sqrt{m}$ .

Can we find a faster factoring method? The next three sections of this chapter are devoted to that question.

## 17.2 The Basic Idea Behind the Quadratic Sieve Method

In Section 3.5 we proved the Coprime Divisibility Lemma: if a number  $m$  divides a product  $cd$  of numbers, and  $m$  and  $c$  are coprime, then  $m$  divides  $d$ .

A consequence of that result is

**Proposition 17.1** *Suppose  $m, c, d$  are numbers and  $m$  divides  $cd$ . If  $m$  does not divide  $c$  and  $m$  does not divide  $d$ , then the greatest common divisor  $(m, c)$  is a non-trivial factor of  $m$ .*

*Proof* Suppose  $m$  divides  $cd$  and  $m$  does not divide  $c$  or  $d$ . We know that  $1 \leq (m, c) \leq m$ , and, of course,  $(m, c)$  divides  $m$ .

If  $(m, c) = m$ , then  $m$  divides  $c$ .

If  $(m, c) = 1$ , then  $m$  divides  $d$  by the Coprime Divisibility Lemma.

So if  $m$  does not divide  $c$  or  $d$ , then  $1 < (m, c) < m$ , and hence  $(m, c)$  is a non-trivial divisor of  $m$ . (The same argument shows that  $(m, d)$  is also a non-trivial factor of  $m$ ).  $\square$

*Example 17.2* Suppose we want to factor 703. Now  $703 \cdot 25 = 17575$ . Suppose we somehow observe that  $17575 = 95 \cdot 185$ . Since 703 divides 17575 but doesn't divide 95 or 185, we find that  $(95, 703) = 19$  and  $(185, 703) = 37$  are non-trivial divisors of 703. In fact,  $703 = 19 \cdot 37$ .

To turn this idea into a method of factoring a number  $m$ , we seek ways to find numbers  $c$  and  $d$  so that  $m$  divides  $cd$  but not  $c$  or  $d$ .

We've seen a possible approach: find numbers  $a$  and  $b$  so that  $m$  divides  $a^2 - b^2 = (a+b)(a-b)$ , but doesn't divide either  $a+b$  or  $a-b$ .

This idea showed up in three places in earlier chapters.

**(i). Carmichael numbers.** In Section 9.8 we showed that odd Carmichael numbers are easy to factor, because if  $m$  is an odd Carmichael number, then for every number  $a$  coprime to  $m$ ,  $a^{m-1} \equiv 1 \pmod{m}$ . Write  $m-1 = 2^e q$  with  $q$  odd and consider the strong  $a$ -pseudoprime sequence modulo  $m$ :

$$a^q, a^{2q}, a^{2^2q}, a^{2^3q}, \dots, a^{2^{e-1}q}, a^{2^eq}.$$

The rightmost number in the sequence is 1 since  $m$  is Carmichael. Rabin's Theorem showed that for at least 3/4 of all  $a$  coprime to  $m$ , the sequence for  $a$  contains a number  $b$  not congruent to 1 or  $-1$  modulo  $m$  so that  $b^2 \equiv 1 \pmod{m}$ . In that case we say that  $m$  fails the strong  $a$ -pseudoprime test. For this number  $b$ ,  $m$  divides  $b^2 - 1 = (b+1)(b-1)$  but not  $b+1$  or  $b-1$ . So  $(m, b-1)$  and  $(m, b+1)$  are non-trivial factors of  $m$ .

*Example 17.3* Let  $m = 8911$ , the seventh Carmichael number. Then  $8910 = 2 \cdot 4455$ . We find that modulo 8911,

$$\begin{aligned} 2^{4455} &\equiv 6364 \\ 6364^2 &\equiv 1 \pmod{8911}. \end{aligned}$$

So 8911 fails the strong 2-pseudoprime test. Moreover, the greatest common divisor of 8911 and  $6364 - 1 = 6363$  is a proper factor of 8911. In fact,  $(6363, 8911) = 7$ .

**(ii). Blum-Goldwasser cryptography.** In Section 16.6, on the security of Blum-Goldwasser cryptography, we let  $m = pq$  where  $p$  and  $q$  are primes both congruent to 3 modulo 4, and examined the subgroup  $S_m$  of the group  $U_m$  of units modulo  $m$  that consists of the squares of units modulo  $m$ . (For example, for  $m = 21$ , there are 12 units: 1, 2, 4, 5, 8, 10 and their negatives, and three of them are squares: 1, 4 and 16. So  $S_{21} = \{1, 4, 16\}$ ).

We showed in Proposition 16.11 that for  $p$  and  $q$  both  $\equiv 3 \pmod{4}$ , the squaring map  $\theta : S_m \rightarrow S_m$  is a bijection (in fact, an isomorphism of groups). In other words, every number  $w$  which is the square of some unit modulo  $m$  has a unique square root  $z$  which is itself the square of some unit modulo  $m$ . We called  $z$  the *square square root* of  $w$ . For  $a$  in  $S_m$ , the unique square square root of  $a$  is denoted by  $z = \omega(a)$ .

We showed in Proposition 16.14 that if Eve, a malicious eavesdropper, is able to find some way to obtain the unique square square root of each element of  $S_m$ , then she can factor  $m$ . The idea is to pick a random unit  $y$  from  $U_m$ , find its square  $w = y^2$ , and then find the square square root  $\omega(w)$  of  $w$  in  $S_m$ . If  $y \neq \omega(w)$  and  $y \neq -\omega(w)$ , then

$$m \text{ divides } y^2 - \omega(w)^2 = (y + \omega(w))(y - \omega(w))$$

but

$$m \text{ does not divide } y - \omega(w) \text{ or } y + \omega(w).$$

(This case will occur for half of the units  $y$  of  $U_m$ .) Then the greatest common divisor of  $m$  and  $y - \omega(w)$  is a non-trivial proper divisor of  $m$ . So we have factored  $m$ .

*Example 17.4* Let  $m = 21$ . We have  $11^2 = 121 \equiv 16 \pmod{21}$  and  $\omega(16) = 4$  is the unique square square root of 16. So  $11^2 \equiv 16 \equiv 4^2 \pmod{21}$ . So

$$21 \text{ divides } 11^2 - 4^2 = (11 + 4)(11 - 4) = 15 \cdot 7.$$

But 21 doesn't divide 15 or 7 because 11 is not congruent to 4 or  $-4 \pmod{21}$ . So the greatest common divisors  $3 = (21, 15)$  and  $7 = (21, 7)$  are non-trivial divisors of 21.

*Example 17.5* Let  $m = 25573$ . Suppose Eve learns that 5024 is the unique square square root of 25 modulo 25573, so that  $5024^2 \equiv 25 \pmod{25573}$ . Then 25573 divides  $(5024 - 5)(5024 + 5)$ . Euclid's Algorithm yields that

$$(5019, 25573) = 239 \text{ and } (5029, 25573) = 107,$$

the two prime factors of  $m = 25573$ .

**(iii). Boneh's Theorem.** The idea also showed up in the proof of Boneh's Theorem (Section 14.6), which says that if Eve is able to find a decrypting exponent for an RSA cryptosystem, then she can with high probability factor the modulus.

### 17.3 Fermat's Method of Factoring

Fermat's method of factoring a number  $m$  is a way of systematically looking for numbers  $a$  and  $b$  so that  $m$  divides  $a^2 - b^2$ .

Let  $c$  be the integer so that  $c - 1 < \sqrt{m} < c$ . In Fermat's method, we compute the numbers  $s = b^2 - m$  for  $b = c, c + 1, c + 2, \dots$ , trying to find some  $b$  so that  $s = b^2 - m$  is a square. If  $s = t^2$  for some integer  $t$ , then

$$m = b^2 - t^2 = (b + t)(b - t)$$

is a factorization of  $m$ .

*Example 17.6* Let  $m = 3569$ . The smallest integer  $> \sqrt{m}$  is  $c = 60$ . We check some numbers  $\geq 60$ :

$b$	$b^2$	$s = b^2 - m$
60	3600	31
61	3721	152
62	3844	275
63	3969	400

For  $b = 63$ , the number  $s = 400 = 20^2$ , a square. So

$$3569 = 63^2 - 20^2 = (63 + 20)(63 - 20) = 83 \cdot 43.$$

We found the factorization quickly.

But Fermat's method can be very slow. Here is an example.

*Example 17.7* Let  $m = 18989$ . We start Fermat's method starting with  $c = 138$ , the first number whose square is  $> m$ : recall  $s = b^2 - m$ .

$b$	$b^2$	$s$
138	19044	55
139	19321	332
140	19600	611
141	20164	852
		:

To decide whether or not  $s$  is a square, we could compute  $\sqrt{s}$  and see if it is an integer, or just create a table of squares to check  $s$  against.

For our example,  $m = 18989$ , it takes 430 trials until we reach  $b = 567$  and we find a square,  $s = 302500 = 550^2$ . Then  $t = 550$ , and

$$18989 = 567^2 - 550^2 = (567 + 550)(567 - 550) = 1117 \cdot 17.$$

Trial division by primes 2, 3, 5, 7, 11, ... would have been far faster!

Looking at these two examples suggests that Fermat's method and trial division are complementary factoring methods. If the smallest factor of  $m$  is much smaller than  $\sqrt{m}$ , then trial division is fast and Fermat's method is slow. On the other hand, if the smallest factor of  $m$  is close to  $\sqrt{m}$ , then trial division is slow and Fermat's method is fast.

In the appendix to this chapter we suppose  $m = pq$  where  $p > q$  are primes, and we'll determine whether trial division or Fermat's method is faster, based on the relative size of  $q$  and  $\sqrt{m}$ .

## 17.4 The Quadratic Sieve Method

Fermat's method is not reliably faster than trial division. But a sophisticated and fast generalization of Fermat's method, called the quadratic sieve method, was proposed by Carl Pomerance in 1982 and soon became the most effective factoring method available. It remains a popular method for factoring numbers of under 100 digits. ([CP05] is a reliable resource for the quadratic sieve method.) A more recent analogue, the Number Field Sieve, is the algorithm of choice for numbers of over 100 digits.

The quadratic sieve method is like Fermat's method, in that it seeks to factor a number  $m$  by finding numbers  $b$  and  $t$  so that  $b^2 \equiv t^2 \pmod{m}$ . But instead of seeking a single number  $s = b^2 - m$  that is a square, this method searches for a collection of numbers

$$b_1^2 - m = s_1,$$

$$b_2^2 - m = s_2,$$

...,

$$b_r^2 - m = s_r$$

whose product  $s_1 \cdot \dots \cdot s_r$  is a square. It does this by computing  $b^2 - m = s$  for many numbers  $b$  near  $\sqrt{m}$ , and retaining a collection of numbers  $b$  whose corresponding numbers  $s$  are products of small primes. Looking at the retained set of numbers  $s$ , we try to find a square by multiplying some of them together. With some luck, this will lead to a factorization of  $m$ .

We illustrate the method with an example.

*Example 17.8* Let  $m = 68137$ . Then  $261 < \sqrt{m} < 262$ . We try some numbers  $b$  near 261. We can allow  $b^2 - m$  to be negative provided that when we combine numbers, we have an even number of negatives. The factorization of  $b^2 - m$  is given in the following table only when the factorization involves only primes  $< 18$ :

$b$	$b^2 - m$	factorization of $b^2 - m$
255	-3112	
256	-2601	$-3 \cdot 3 \cdot 17 \cdot 17$
257	-2088	
258	-1573	$-11 \cdot 11 \cdot 13$
259	-1056	$-2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 11$
260	-537	
261	-16	$-2 \cdot 2 \cdot 2 \cdot 2$
262	507	$3 \cdot 13 \cdot 13$
263	1032	
264	1559	
265	2088	
266	2619	
267	3152	
268	3687	
269	4224	$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 11$
270	4763	
271	5304	$2 \cdot 2 \cdot 2 \cdot 3 \cdot 13 \cdot 17$

In each row, the number in the second column is congruent modulo  $m$  to the square of the number in the first column. Staring at the table, we notice that

$$\begin{aligned}(256 \cdot 261)^2 &= (-2601)(-16) \equiv (-3 \cdot 3 \cdot 17 \cdot 17) \cdot (-2 \cdot 2 \cdot 2 \cdot 2) \\ &= 2^4 \cdot 3^2 \cdot 17^2 \\ &= (2^2 \cdot 3 \cdot 17)^2 \pmod{68137}.\end{aligned}$$

So  $m = 68137$  divides

$$(256 \cdot 261)^2 - (2^2 \cdot 3 \cdot 17)^2 = 66816^2 - 204^2.$$

Thus  $m$  divides

$$\begin{aligned}66816^2 - 204^2 &= (66816 + 204)(66816 - 204) \\ &= 67020 \cdot 66612.\end{aligned}$$

Clearly 68137 doesn't divide either factor. Computing greatest common divisors, we find that

$$(68137, 66612) = 61 \text{ and } (68137, 67020) = 1117,$$

the two factors of  $m = 68137$ .

We note that there are other ways to multiply numbers  $b$  together to get a square.

If we try

$$\begin{aligned}(259 \cdot 261 \cdot 269)^2 &\equiv ((-1) \cdot 2^5 \cdot 3 \cdot 11) \cdot ((-1) \cdot 2^4) \cdot (2^7 \cdot 3 \cdot 11) \\ &\equiv 2^{16} \cdot 3^2 \cdot 11^2 \\ &= (2^8 \cdot 3 \cdot 11)^2 \pmod{68137},\end{aligned}$$

we obtain

$$18184131^2 \equiv 8448^2 \pmod{68137}.$$

So 68137 divides  $(18184131 + 8448)(18184131 - 8448)$ .

But we find that 68137 divides  $18184131 - 8448$ . So that combination fails to yield a factorization of  $m$ .

Another product of numbers  $b^2$  that gives a square modulo  $m$ , and hence might give a factorization, is left as an exercise.

To implement the quadratic sieve to factor a number  $m$  involves several steps:

I. In the examples we did not factor every number of the form  $b^2 - m$ , but only looked at those that were a product of small primes. Call the set of primes we use to factor numbers of the form  $b^2 - m$  the *factor base* for  $m$ . The factor base will consist only of primes  $< B$  for some bound  $B$ . In the last example we looked only at primes  $< B = 18$ . In general, how do we choose  $B$ ?

II. We should determine which primes will be involved in the factor base. We don't want to include primes that can never appear in a factorization of a number  $b^2 - m$ . In the last example, we saw that the primes 5 and 7 never appeared for  $m = 68137$ .

III. Once we decide on the primes in the factor base, we want to efficiently find numbers that factor only into primes in our factor base.

IV. Having found the factorizations involving the factor base of a sufficiently large set of numbers  $b^2 - m$ , we want to find products of those numbers that are squares. We found two such products in the last example.

V. Having found squares, we check to see if the squares actually yield a factorization of  $m$ . In the last example, we saw that it can go either way—some squares yield factors of  $m$ , some don't.

We consider each issue in turn.

**I. How many primes?** To factor the number  $m$  efficiently, we want to limit the factor base to primes  $p < B$  for some  $B$ . But choosing  $B$  is delicate.

There is some terminology related to this issue.

A number  $c$  is called *B-smooth* if every prime divisor of  $c$  is  $< B$ .

*Example 17.9* To get a feeling for this terminology, consider the factorization into primes of numbers between 1000 and 1015. The first column orders the numbers by size, the second by the size of their largest prime factor:

$1000 = 2^3 \cdot 5^3$	$1000 = 2^3 \cdot 5^3$
$1001 = 7 \cdot 11 \cdot 13$	$1008 = 2^4 \cdot 3^2 \cdot 7$
$1002 = 2 \cdot 3 \cdot 167$	$1001 = 7 \cdot 11 \cdot 13$
$1003 = 17 \cdot 59$	$1014 = 2 \cdot 3 \cdot 13^2$
$1004 = 2 \cdot 2 \cdot 251$	$1012 = 2^2 \cdot 11 \cdot 23$
$1005 = 3 \cdot 5 \cdot 67$	$1015 = 5 \cdot 7 \cdot 29$
$1006 = 2 \cdot 503$	$1007 = 19 \cdot 53$
$1007 = 19 \cdot 53$	$1003 = 17 \cdot 59$
$1008 = 2^4 \cdot 3^2 \cdot 7$	$1005 = 3 \cdot 5 \cdot 67$
$1009 = 1009$	$1010 = 2 \cdot 5 \cdot 101$
$1010 = 2 \cdot 5 \cdot 101$	$1002 = 2 \cdot 3 \cdot 167$
$1011 = 3 \cdot 337$	$1004 = 2 \cdot 2 \cdot 251$
$1012 = 2^2 \cdot 11 \cdot 23$	$1011 = 3 \cdot 337$
$1013 = 1013$	$1006 = 2 \cdot 503$
$1014 = 2 \cdot 3 \cdot 13^2$	$1009 = 1009$
$1015 = 5 \cdot 7 \cdot 29$	$1013 = 1013$

As can be seen by the second column, among these numbers:

the 10-smooth numbers are 1000 and 1008 (every prime dividing 1000 or 1008 is  $< 10$ );

the 25-smooth numbers are the 10-smooth numbers, and also 1001, 1014 and 1012;

the 100-smooth numbers are the 25-smooth numbers and also 1015, 1007, 1003 and 1005;

All sixteen numbers are 1015-smooth.

Choosing the smoothness bound  $B$  involves balancing two problems. If we choose too small a value of  $B$ , then  $B$ -smooth numbers of the form  $b^2 - m$  will be relatively scarce, and we will have to look through a larger collection of numbers of the form  $b^2 - m$  to find sufficiently many that are  $B$ -smooth. On the other hand, if we choose too large a value, we will end up with a large factor base of primes, and it will be more difficult to find products of numbers of the form  $b^2 - m$  that are squares.

In the example with  $m = 68137$  above, we chose  $B = 18$  and found nine numbers among the 30 we examined that were 18-smooth.

Crandall and Pomerance [CP05] suggest that to minimize running time, for a large number  $m$ , one should choose  $B$  to be about

$$B \sim e^{\frac{1}{2}\sqrt{\ln m \ln \ln m}}.$$

where  $\ln$  is the natural logarithm. In our example,  $m = 68137$  is a number that is very small relative to the size of numbers on which the quadratic sieve is typically used. For  $m = 68137$ , we find  $\ln m = 11$  and  $\ln \ln m = \ln 11 = 2.4$ . So we should choose  $B$  somewhere near

$$e^{\frac{1}{2}\sqrt{11 \cdot 2.4}} = e^{\frac{1}{2}\sqrt{26.4}} = e^{2.57} \sim 13.$$

In our example we found it convenient to choose a somewhat larger  $B$  since  $m$  was so small, and in fact to obtain the factorization, we needed to use the prime 17.

Crandall and Pomerance [CP05] also offers the comment: “or tune  $B$  to taste”.

Obtaining a precise estimate of the number of  $B$ -smooth numbers less than a given real number  $x$  is a non-trivial problem. See [CP05] and [Gra04].

**II. Which primes are relevant?** Once a bound  $B$  is chosen, our factor base will consist of primes  $< B$ . But not all of those primes can appear in a factorization of a number of the form  $b^2 - m$ , so we can omit them in the factor base.

The primes that can appear are easily described: they are prime numbers  $p$  so that  $m$  is a square modulo  $p$ . For if  $s = b^2 - m$  and  $p$  is a prime factor of  $s$ , then  $m \equiv b^2 \pmod{p}$ .

To decide whether or not  $m$  is a square modulo  $p$  involves some classical number theory, involving quadratic residues, the Legendre symbol and its generalization, the Jacobi symbol, and the famous Law of Quadratic Reciprocity. Suffice it to say that to decide whether or not  $m$  is a square modulo  $p$  takes approximately the same amount of time as it takes to compute Euclid's Algorithm for  $m$  and  $p$ . There are many sources to read about this topic, including most textbooks on elementary number theory, so we will omit this aspect of the quadratic sieve method here.

We also add to our factor base the number  $(-1)$ . Since no negative number is a square, if we want to use numbers of the form  $b^2 - m$  where  $b < \sqrt{m}$ , then we need an even number of them in order to form a square. We did that in Example 17.8 above, with  $m = 68137$ .

**III. Sieve out numbers that are  $B$ -smooth.** The next step is to find a collection of numbers of the form  $b^2 - m$  whose factorization includes only the primes in our prime factor base. To illustrate this, we look at an extended example.

*Example 17.10* Let  $m = 126811$ . Then the square root of  $m$  is near 356, so we try to find numbers  $b$  near 356 so that  $b^2 - m$  is only divisible by small primes. By “small” we decide: primes  $< B = 42$ .

$b$	$b^2 - m$	largest prime factor or factorization
324	-21835	397
325	-21186	107
326	-20535	$-3 \cdot 5 \cdot 37 \cdot 37$
327	-19882	9941
328	-19570	$-3 \cdot 13 \cdot 17 \cdot 29$
329	-18570	619
330	-17911	17911
331	-17250	$-2 \cdot 3 \cdot 5 \cdot 5 \cdot 23$
332	-16587	97
333	-15922	419
334	-15255	1017
335	-14583	$-2 \cdot 3 \cdot 11 \cdot 13 \cdot 17$
336	-13915	$-5 \cdot 11 \cdot 11 \cdot 23$
337	-13242	2207
338	-12567	71
339	-11890	41
340	-11211	101
341	-10530	$-2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 13$
:	:	
351	-3610	$-2 \cdot 5 \cdot 19 \cdot 19$
352	-2907	$-3 \cdot 3 \cdot 17 \cdot 19$
353	-2202	367
354	-1495	$-5 \cdot 13 \cdot 23$
355	-786	131
356	-75	$-3 \cdot 5 \cdot 5$
:	:	

We omitted the numbers 342 to 350 in the table because all are divisible by a prime  $\geq 43$ . Our table continues for another 63 numbers.

To find the numbers  $b$  between 324 and 419 so that  $b^2 - m$  is a product of only primes  $< 42$ , a simple idea is to take that set of numbers  $b^2 - m$ , view them as real numbers and divide them all by 2, by 3, by 5, by 11, by 13, by 17, by 19, ..., by 41. (I used Excel.). If the result of dividing  $b^2 - m$  by, say 13, is an integer, then 13 divides  $b^2 - m$ . Otherwise not. If  $b^2 - m$  is divisible by enough of the primes 2, ..., 41, then we look at  $b^2 - m$  more closely—perhaps all of the prime factors of  $b^2 - m$  are  $\leq 41$ .

Someone with decent programming skills could likely do this fairly efficiently.

I did this for the 96 numbers  $b$  with  $324 \leq b \leq 419$ , and ended up with the following set of eleven numbers (where, recall,  $m = 126811$ ).

$b$	$b^2 - m$	factorization of $b^2 - m$
326	-20535	$-3 \cdot 5 \cdot 37^2$
335	-14586	$-2 \cdot 3 \cdot 11 \cdot 13 \cdot 17$
341	-10530	$-2 \cdot 3^4 \cdot 5 \cdot 13$
351	-3610	$-2 \cdot 5 \cdot 19^2$
356	-75	$-3 \cdot 5^2$
361	3510	$2 \cdot 3^3 \cdot 5 \cdot 13$
369	9350	$2 \cdot 5^2 \cdot 11 \cdot 17$
371	10830	$2 \cdot 3 \cdot 5 \cdot 19^2$
379	16380	$2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 17$
413	43758	$2 \cdot 3^2 \cdot 11 \cdot 13 \cdot 17$
419	48750	$2 \cdot 3 \cdot 5^4 \cdot 13$

This is a list of eleven factorizations involving  $(-1)$ , 2, 3, 5, 11, 13 and 17 (together with  $19^2$  and  $37^2$ ). Thinking of  $(-1)$  as an additional factor that needs to be raised to an even power, this is a set of seven “primes”. We want to find products of the 11 numbers in the right-hand column that are squares.

**IV. Linear algebra modulo 2.** Look at the exponents of the primes in the rightmost column of the table above, and reduce them modulo 2. We can put the resulting mod 2 exponents into the following table:

	326	335	341	351	356	361	369	371	379	413	419
$(-1)$	1	1	1	1	1	0	0	0	0	0	0
2	0	1	1	1	0	1	1	1	1	1	1
3	1	1	0	0	1	1	0	1	0	0	1
5	1	0	1	0	0	1	0	1	1	0	0
11	0	1	0	0	0	0	1	0	1	1	0
13	0	1	1	0	0	1	0	0	0	1	1
17	0	1	0	0	0	0	1	0	1	1	0

We omitted the primes 19 and 37 because the exponents of 19 and 37 in the earlier table are even.

View the columns of this table (omitting the first column) as column vectors in the vector space  $\mathbb{F}_2^7$ . We look for a sum of some of those columns that yield the zero vector. For example, notice that

$$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

the zero vector. Obtaining the zero vector as a sum of column vectors means that the product of the squares of the corresponding numbers  $b$  is congruent to a positive number whose prime factors all have even exponents, and hence is a square:

$$341^2 \cdot 356^2 \cdot 361^2 \equiv (-1)^2 \cdot 2^2 \cdot 3^8 \cdot 5^4 \cdot 13^2 \pmod{m}.$$

So we turn the entries of the table into an  $7 \times 11$  matrix with entries in  $\mathbb{F}_2$ :

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

We want to find  $\mathbb{F}_2$ -linear combinations of the columns of  $\mathbf{A}$  that equal 0. By Corollary 7.7, this problem is equivalent to finding vectors in the null space of  $\mathbf{A}$ . If, for example, we find that the vector

$$(0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0)^T$$

is in the null space, that is,

$$\mathbf{A} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

then the sum of the third, fifth and sixth columns of  $A$  is the zero vector: that is,

$$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Since  $\mathbf{A}$  has 11 columns and 7 rows, the null space of  $\mathbf{A}$ , that is, the set of column vectors  $\bar{x}$  in  $\mathbb{F}_2^{11}$  so that  $\mathbf{A}\bar{x} = 0$ , has dimension at least 4. So there should be at least four linearly independent products of the 11 numbers  $b^2$  that are congruent modulo  $m$  to a square.

The classical way to find the null space of  $\mathbf{A}$  is to reduce  $\mathbf{A}$  to reduced row echelon form.

We find that the reduced row echelon form of  $\mathbf{A}$  is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let  $\mathbf{x} = (x_1, x_2, \dots, x_{11})^T$ . The solutions of  $\mathbf{Ax} = 0$  depend on six parameters, namely  $x_6, \dots, x_{11}$ , so the null space of  $\mathbf{A}$  has dimension 6.

A basis of the null space of  $\mathbf{A}$  is the set of vectors corresponding to setting one parameter = 1 and all others = 0. Here is the basis:

$$\mathbf{v}_6 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v}_7 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v}_8 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v}_9 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v}_{10} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v}_{11} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

We saw that  $\mathbf{v}_6$  corresponded to the congruence

$$(341 \cdot 356 \cdot 361)^2 \equiv (2 \cdot 3^4 \cdot 5^2 \cdot 13)^2 \pmod{m}.$$

Corresponding to the other five vectors  $\mathbf{v}_7, \dots, \mathbf{v}_{11}$  in the basis of the null space of  $A$  are the following congruences:

$$\begin{aligned} \mathbf{v}_7 : \quad & (335 \cdot 341 \cdot 351 \cdot 356 \cdot 369)^2 \equiv (2^2 \cdot 3^3 \cdot 5^3 \cdot 11 \cdot 13 \cdot 17 \cdot 19)^2 \pmod{m} \\ \mathbf{v}_8 : \quad & (351 \cdot 356 \cdot 371)^2 \equiv (2 \cdot 3 \cdot 5^2 \cdot 19^2) \pmod{m} \\ \mathbf{v}_9 : \quad & (326 \cdot 335 \cdot 341 \cdot 351 \cdot 379)^2 \equiv (2^2 \cdot 3^4 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 37)^2 \pmod{m} \\ \mathbf{v}_{10} : \quad & (335 \cdot 356 \cdot 413)^2 \equiv (2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 13 \cdot 17)^2 \pmod{m} \\ \mathbf{v}_{11} : \quad & (326 \cdot 341 \cdot 419)^2 \equiv (2 \cdot 3^3 \cdot 5^3 \cdot 13 \cdot 37)^2 \pmod{m} \end{aligned}$$

There has been considerable research on methods to speed up this linear algebra step. Since the matrices are “sparse”, that is, have few non-zero entries, there are some specialized methods for handling those matrices. See, for example, [LO91].

**V. Testing each combination.** Finally, to look for a factorization of  $m = 126811$ , we check each congruence in turn:

$\mathbf{v}_6$ : We have

$$(341 \cdot 356 \cdot 361)^2 \equiv (2 \cdot 3^4 \cdot 5^2 \cdot 13)^2 \pmod{m},$$

and we have

$$\begin{aligned} 341 \cdot 356 \cdot 361 &= 43823956; \\ 2 \cdot 3^4 \cdot 5^2 \cdot 13 &= 52650. \end{aligned}$$

So  $m = 126811$  divides

$$\begin{aligned} (43823956)^2 - (52650)^2 &= (43823956 + 52650)(43823956 - 52650) \\ &= 43879906 \cdot 43771306. \end{aligned}$$

But we find that the first factor 43879906 is a multiple of 126811. This combination fails.

**v7:**

$$\begin{aligned} 335 \cdot 341 \cdot 351 \cdot 356 \cdot 369 &= 5267234655540; \\ 2^2 \cdot 3^3 \cdot 5^3 \cdot 11 \cdot 13 \cdot 17 \cdot 19 &= 623551500. \end{aligned}$$

So  $m = 126811$  divides  $(5267234655540)^2 - (623551500)^2$

$$= (5267234655540 + 623551500)(5267234655540 - 623551500).$$

Applying Euclid's algorithm to  $m$  and each of the two factors, we find that for the sum, the greatest common divisor is

$$(5267234655540 + 623551500, 126811) = 211,$$

and for the difference, the greatest common divisor is

$$(5267234655540 - 623551500, 126811) = 601.$$

So  $126811 = 211 \cdot 601$ . Success!

**v8:**

$$\begin{aligned} 351 \cdot 356 \cdot 371 &= 46358676 \\ 2 \cdot 3 \cdot 5^2 \cdot 19^2 &= 54150. \end{aligned}$$

The sum of these two numbers is divisible by  $m$ . Failure.

**v9:**

$$\begin{aligned} 326 \cdot 335 \cdot 341 \cdot 351 \cdot 379 &= 4954081107690; \\ 2^2 \cdot 3^4 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 37 &= 13842843300. \end{aligned}$$

The difference of these two numbers is divisible by  $m$ . Failure.

**v10:**

$$\begin{aligned} 335 \cdot 356 \cdot 413 &= 49254380; \\ 2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 13 \cdot 17 &= 218790. \end{aligned}$$

The greatest common divisor of the sum of these two numbers and  $m = 126811$  is equal to 211; the greatest common divisor of the difference and  $m$  is = 601. Success!

**v<sub>11</sub>:**

$$326 \cdot 341 \cdot 419 = 46578554;$$

$$2 \cdot 3^3 \cdot 5^3 \cdot 13 \cdot 37 = 3246750.$$

The greatest common divisor of the sum of these two numbers and  $m = 126811$  is equal to 601; the greatest common divisor of the difference and  $m$  is = 211. Success!

**Fermat factoring again.** Among the numbers  $b$  tested for  $m = 126811$ , I inadvertently omitted

$$406^2 - 126811 = 38025 = 3^2 \cdot 5^2 \cdot 13^2 = (195)^2.$$

So

$$406 - 195 = 211; \quad 406 + 195 = 601.$$

Fermat's method would have worked on  $m = 126811$ .

This concludes Example 17.10.

**Application to factoring large numbers.** What we have presented here is a “bare bones” version of the quadratic sieve.

The factorization of RSA-129 in April, 1994 was announced on the internet at [AGL94] and widely publicized, e.g., [Ko94]. The method used was a refined version of the quadratic sieve. The factorization of RSA-129 took 8 months and involved about 600 volunteers from more than 20 countries.

The quadratic sieve method involves the five steps: 1. choose a bound  $B$  (which takes no time), 2. decide which primes  $< B$  should be in the factor base, 3. find enough numbers of the form  $b^2 - m$  where each is a square times a product of primes in the factor base, 4. the linear algebra step, to get a set of pairs  $(b, c)$  of numbers  $b$  and  $c$  so that  $m$  divides  $b^2 - c^2$ , and 5. check to see if  $(b, c)$  yields a factorization of  $m$ .

Steps 2, 3 and 5 can be distributed over many computers. The main computational roadblock in the quadratic sieve method is the linear algebra step.

Given the size of RSA-129, the proposed guideline for the bound  $B$  would be around  $B = 850,000,000$ . There are approximately 41,300,000 primes  $\leq 850,000,000$ , and  $m$  is a square modulo  $p$  for approximately half of those primes. So the linear algebra step would involve finding column dependencies in an  $m \times n$  matrix with entries in  $\mathbb{F}_2$  where  $20,000,000 < m < n$ .

According to the announcement of the factoring of RSA-129, rather than having a factor base of some 20 million primes, the factorization of RSA-129 had a factor base of 524,338 primes.

To get around the problem of finding enough  $B$ -smooth numbers with such a small factor base, the researchers used a modification of the quadratic sieve method. Instead of evaluating the polynomial  $x^2 - m$  at numbers  $b$  near  $\sqrt{m}$ , the solvers used a multiple polynomial variation of the quadratic sieve method, where  $x^2 - m$  was replaced by a collection of quadratic polynomials. For details, see Subsection 6.1.5 of [CP05]. Each  $b$  involved a separate computation involving the factor base, so the task of finding a suitable set of more than 524,338 numbers  $b$  could be distributed among many computers. (Hence the 600 volunteers from 20 countries.)

According to the announcement, the computations yielded a set of 569,466 numbers  $b$ , so the matrix examined for column dependences had 524,338 rows and 569,466 columns. The matrix was reduced to a dense matrix of 188,160 rows and 188,614 columns using a technique they called structured Gaussian elimination. That matrix was then reduced to echelon form after 45 hours on a massively parallel computer. (The difficulties of the matrix step are beyond the scope of this book. See Section 6.1.3 of [CP05] for some discussion and references.)

The null space of the matrix had dimension at least  $(188614 - 188160) = 454$ , so there were at least that many independent column dependencies.

The first three dependencies tested all turned out to yield only the trivial factor RSA-129. The fourth dependency produced the desired factorization.

## 17.5 The Index Calculus Method for Discrete Logarithms

Section 13.10 presented the Baby Step-Giant Step algorithm for finding the discrete logarithm of an element  $a$  in a finite group  $\langle g \rangle$  of order  $n$ . Let  $m$  be the smallest integer  $> \sqrt{n}$ . The idea is to write down  $g^r$  for  $r = 1, 2, \dots, m-1$ , then begin writing down  $ag^{-mq}$  for  $q = 1, \dots, m$  and look for a match: find  $q, r$  so that  $ag^{-mq} = g^r$  for some  $r < m$ . When we find one, then

$$a = g^{mq+r}$$

and we've found  $\log_g(a) = mq + r$ . The algorithm is similar to Fermat's method of factoring a number  $m$ : we write down elements  $b^2 - m$  for many  $b > \sqrt{m}$  near  $\sqrt{m}$  and see if any one is congruent modulo  $m$  to a square. The list of small powers of  $g, g^2, g^3, \dots$  in the Baby Step-Giant Step method is analogous to a list of squares to compare each  $b^2 - m$  to in the Fermat method.

Let  $g$  be a primitive root modulo  $p$ , a prime number. The Index Calculus method for finding the discrete logarithm of an element  $a$  of  $U_p = \langle g \rangle$  relates to the Baby Step-Giant Step algorithm as the Quadratic Sieve factoring method relates to Fermat's method of factoring. Instead of trying to find  $\log_g(a)$  by looking for a direct hit of the form  $ag^e = g^f$  for some  $e, f$ , the idea is to look for a number  $q$  so that  $ag^q = p_1^{e_1} \cdots p_r^{e_r}$  where we have previously found the discrete logarithms of the primes  $p_1, \dots, p_r$ . Then, just as with the Baby Step-Giant Step algorithm, we can write down the discrete logarithm of  $a$  immediately.

More precisely, the Index Calculus method to find  $\log_g(a)$  involves three steps, two preparatory steps followed by one step involving  $a$ .

**Step I.** Pick a smoothness bound  $B$  and find a collection of powers of the primitive root  $g$  that modulo  $p$  are divisible only by the primes  $p_1, \dots, p_r < B$ :

$$\begin{aligned} g^{q_1} &\equiv p_1^{c_{1,1}} p_2^{c_{1,2}} \cdots p_r^{c_{1,r}} \\ g^{q_2} &\equiv p_1^{c_{2,1}} p_2^{c_{2,2}} \cdots p_r^{c_{2,r}} \\ &\vdots \\ g^{q_k} &\equiv p_1^{c_{k,1}} p_2^{c_{k,2}} \cdots p_r^{c_{k,r}} \end{aligned}$$

where  $k$  is sufficiently larger than  $r$ .

**Step II.** To find  $\log_g(p_1), \dots, \log_g(p_r)$ : take  $\log_p$  of the equations in Step I to get

$$\begin{aligned} \log_g(g^{q_1}) &= q_1 \equiv c_{1,1} \log_g(p_1) + c_{1,2} \log_g(p_2) + \dots + c_{1,r} \log_g(p_r) \\ \log_g(g^{q_2}) &= q_2 \equiv c_{2,1} \log_g(p_1) + c_{2,2} \log_g(p_2) + \dots + c_{2,r} \log_g(p_r) \\ &\vdots \\ \log_g(g^{q_k}) &= q_k \equiv c_{k,1} \log_g(p_1) + c_{k,2} \log_g(p_2) + \dots + c_{k,r} \log_g(p_r). \end{aligned}$$

This is a system of linear equations modulo  $p-1$  where the unknowns are  $\log_g(p_i)$  for  $i = 1, \dots, r$  and the coefficients  $c_{i,j}$  come from Step 1. Since there are more equations than unknowns, there should be a unique solution of the equations (the first  $r$  rows of the reduced row echelon form of the matrix of coefficients should be the  $r \times r$  identity matrix).

Solve these equations modulo  $p-1$  to find  $\log_g(p_1), \log_g(p_2) \dots \log_g(p_r)$ .

**Step III.** Now, to find  $x = \log_g(a)$ , that is, to find  $x$  so that  $g^x \equiv a \pmod{p}$ , look at  $ag^n$  modulo  $p$  for various exponents  $n$  until you find some exponent  $n$  so that  $ag^n$  is  $B$ -smooth, that is,

$$ag^n \equiv p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \pmod{p}$$

for some  $e_1, \dots, e_r$ . Having done so, to find  $x = \log_g(a)$ , just take  $\log_g$  of both sides of this last equation, to get, modulo  $p - 1$ ,

$$x + n \equiv e_1 \log_g(p_1) + e_2 \log_g(p_2) + \dots + e_r \log_g(p_r).$$

Since  $\log_g(p_1), \dots, \log_g(p_r)$  are known from Step II and  $n, e_1, \dots, e_r$  are known, we can find  $x = \log_g(a)$  immediately.

We illustrate the method with an example.

*Example 17.11* Let  $p = 503$ , a prime. Then  $g = 17$  is a primitive root, so has order 502 modulo 503.

Suppose we want to find  $\log_{17}(323)$ : that is, find  $x$  so that  $17^x \equiv 323 \pmod{503}$ .

Before even considering 323, we need to do Steps I and II: that is, generate a database of powers of 17 modulo 503 that are “smooth”: that is, are divisible only by small primes.

For illustration, we restrict ourselves to the primes 2, 3, 5 and 7 (so the smoothness bound is  $B = 8$ ). We want to find powers of 17 that yield numbers modulo 503 that are only divisible by 2, 3, 5 and 7.

For Step I, I computed the first 40 powers of the primitive root  $g = 17$  modulo 503 (I used Excel) and found that modulo 503,

$$\begin{aligned} 17^6 &\equiv 2^2 \cdot 3^3 \\ 17^{18} &\equiv 2^3 \cdot 5^2 \\ 17^{25} &\equiv 2 \cdot 5 \\ 17^{27} &\equiv 3 \cdot 5^3 \\ 17^{32} &\equiv 2^2 \cdot 3^2 \cdot 7 \\ 17^{38} &\equiv 2 \cdot 3^3. \end{aligned}$$

These equations translate into equations involving the unknown quantities  $\log_{17}(2)$ ,  $\log_{17}(3)$ ,  $\log_{17}(5)$  and  $\log_{17}(7)$ :

$$\begin{aligned} 6 &\equiv 2 \log_{17} 2 + 3 \log_{17} 3 \pmod{502} \\ 18 &\equiv 3 \log_{17} 2 + 2 \log_{17} 5 \pmod{502} \\ 25 &\equiv \log_{17} 2 + \log_{17} 5 \pmod{502} \\ 27 &\equiv \log_{17} 3 + 3 \log_{17} 5 \pmod{502} \\ 32 &\equiv 2 \log_{17} 2 + 2 \log_{17} 3 + \log_{17} 7 \pmod{502} \\ 38 &\equiv \log_{17} 2 + 3 \log_{17} 3 \pmod{502}. \end{aligned}$$

From these congruences modulo 502 we proceed to Step II, to find  $\log_{17}(p)$  for  $p = 2, 3, 5$  and 7. The augmented matrix of that set of equations is

$$\left( \begin{array}{ccccc} 2 & 3 & 0 & 0 & 6 \\ 3 & 0 & 2 & 0 & 18 \\ 1 & 0 & 1 & 0 & 25 \\ 0 & 1 & 3 & 0 & 27 \\ 2 & 2 & 0 & 1 & 32 \\ 1 & 3 & 0 & 0 & 38 \end{array} \right),$$

where the unknowns corresponding to the four left columns are, from left to right,

$$\log_{17}(2), \log_{17}(3), \log_{17}(5), \log_{17}(7).$$

We do row operations on the matrix. If we subtract 2 times the third row from the second row, modulo 502, we obtain

$$(3, 0, 2, 0, 18) - (2, 0, 2, 0, 50) = (1, 0, 0, 0, 470),$$

so  $\log_{17} 2 = 470$ . Then

$$(1, 0, 1, 0, 25) - (1, 0, 0, 0, 470) = (0, 0, 1, 0, 57),$$

so  $\log_{17} 5 = 57$ . Then

$$(0, 1, 3, 0, 27) - (0, 0, 3, 0, 171) = (0, 1, 0, 0, 358),$$

so  $\log_{17} 3 = 358$ . Finally,

$$(2, 2, 0, 1, 32) - (2, 0, 0, 0, 940) - (0, 2, 0, 0, 716) = (0, 0, 0, 1, 384),$$

so  $\log_{17} 7 = 384$ .

Now suppose we want to find  $\log_{17}(323)$ . For Step III, we compute  $323 \cdot 17^e$  for  $e = 1, 2, 3, \dots$  to find some  $e$  so that the result modulo 503 is divisible only by 2, 3, 5 and 7. We find quickly that modulo 503,

$$\begin{aligned} 323 \cdot 17^5 &\equiv 40 \\ &= 2^3 \cdot 5. \end{aligned}$$

So taking  $\log_{17}()$  of both sides we have, modulo 502,

$$\log_{17}(323) + 5 = 3 \log_{17} 2 + \log_{17} 5,$$

so

$$\log_{17}(323) = 3 \log_{17} 2 + \log_{17} 5 - 5 = 3 \cdot 470 + 57 - 5 = 458.$$

Notice that in the computation, the discrete logarithms are only defined modulo  $p - 1 = 502$ . Since  $502 = 2 \cdot 251$  (where 251 is prime), a row operation involving dividing a row by 2 (or 251) could make the solution invalid.

*Remark 17.12* Steps I and II of the Index Calculus method pick a bound  $B$  and solve the discrete logarithm problem for primes  $< B$  in the group  $\langle g \rangle = U_p$ . Thus the method creates a database, a log table, of discrete logarithms of the primes  $< B$ . These computations are independent of any particular discrete logarithm problem. (In our example,  $B = 8$ : the primes were 2, 3, 5 and 7.)

Having done so for  $B$  sufficiently large, then Step III, the step of trying to find some  $e$  so that  $g^e a$  is a product of powers of primes  $< B$ , thereby yielding  $\log_g(a)$ , can be done comparatively rapidly.

The issue in applying the Index Calculus method is choosing  $B$  small enough to make the database practical, while large enough so that finding some  $e$  so that  $g^e a$  is divisible only by the primes  $< B$  can be done efficiently.

But, as observed in Section 13.5, if the same underlying group  $U_p = \langle g \rangle$  is used widely, it could be worthwhile for an eavesdropper with sufficient resources to choose a very large smoothness bound  $B$  and develop a large database of discrete logarithms of primes. A sufficiently large database would make the final step (Step III), to find a particular discrete logarithm, very quick. Such an eavesdropper would then have access to every use of Diffie-Hellman with that particular group  $\langle g \rangle = U_p$ .

Thus the recent (pre-2015) practice of using a very small set of Diffie-Hellman groups for key exchanges all over the internet would make the internet transparent for a sufficiently dedicated eavesdropper, such as a nation-state having access to supercomputers. (See [www.top500.org](http://www.top500.org) for a list of the 500 fastest publicly known supercomputers in the world. As of November, 2018, the U. S. had five of the top ten, China two, and there was one each in Japan, Switzerland and Germany.)

See [CP05] for further information on the index calculus method.

## Exercises

- 17.1.  $m = 46657$  is a Carmichael number. Find some number  $a$  so that  $m$  fails the strong  $a$ -pseudoprime test. Use that failure to factor  $m$ .
- 17.2.  $m = 162401$  is a Carmichael number. Find some number  $a$  so that  $m$  fails the strong  $a$ -pseudoprime test. Use that failure to factor  $m$ .
- 17.3. Let  $m = 77$ . It turns out that  $20^2 \equiv 15 \pmod{77}$ , and the unique square square root of 15 is 64. Use this information to find the two prime factors of 77 as greatest common divisors.
- 17.4. Factor  $m = 9167$  by Fermat's method.
- 17.5. Factor  $m = 26329$  by Fermat's method.
- 17.6. Factor  $m = 18281$  by Fermat's method.
- 17.7. The number 20911 factors as  $11 \cdot 1901$ , both prime factors, and  $145 > \sqrt{20911} > 144$ . If you tried to factor 20911 by Fermat's method by looking for squares among

$$145^2 - 20911, 146^2 - 20911, \dots,$$

how many numbers would you need to check before you found some  $b \geq 145$  with  $b^2 - 20911 = s^2$  for some number  $s$ ?

- 17.8. In Example 17.8, the factorization of  $m = 68137$ , notice from the table that  $256^2 \cdot 259^2 \cdot 269^2$  is congruent to a square modulo  $m$ . Decide whether or not that choice of numbers  $b$  gives a non-trivial factorization of  $m$ , and justify your answer.
- 17.9. Let  $n = 2441921$ . I found that

$$\begin{aligned} 1519^2 - n &= -134560 = -2^5 \cdot 5 \cdot 29^2 \\ 1541^2 - n &= -67240 = -2^3 \cdot 5 \cdot 41^2. \end{aligned}$$

Using those facts, factor  $n$  into a product of primes.

- 17.10. With  $n = 2441921$  as in the last problem, I found that

$$\begin{aligned} 1562^2 - n &= -31 \cdot 67 \\ 1587^2 - n &= 2^3 \cdot 11 \cdot 13 \cdot 67 \\ 1569^2 - n &= 2^7 \cdot 5 \cdot 31 \\ 1559^2 - n &= -2^4 \cdot 5 \cdot 11 \cdot 13. \end{aligned}$$

Do these facts yield a factorization of  $n$  into a product of primes?

- 17.11. As in Example 17.11, let  $p = 503$ , a prime. Then  $g = 5$  is a primitive root, so has order 502 modulo 503.

Suppose we want to find  $\log_5(323)$  in  $U_{503}$ : that is, find  $x$  so that  $5^x \equiv 323 \pmod{503}$ .

To do so, we need to do Steps I and II: that is, generate a database of powers of 5 modulo 503 that are “smooth”: that is, are divisible only by small primes.

As in the example, we restrict ourselves to the primes 2, 3, 5 and 7 (so the smoothness bound is  $B = 8$ ). We want to find powers of 5 that yield numbers modulo 503 that are only divisible by 2, 3, 5 and 7.

For Step I, I computed the first 100 powers of  $g = 5$  modulo 503 and found that

$$\begin{aligned} 5^1 &= 5 \\ 5^6 &\equiv 2^5 \\ 5^{12} &\equiv 2 \cdot 3^2 \\ 5^{58} &\equiv 2^2 \cdot 3 \\ 5^{86} &\equiv 7. \end{aligned}$$

- (i) Use this information to find  $\log_5(x)$  for  $x = 2, 3, 5$  and 7.

Now I computed  $5^e \cdot 323$  for various  $e$ , to find some  $e$  so that the result modulo 503 is divisible only by 2, 3, 5 and 7. I found that  $e = 24$  yields

$$5^{24} \cdot 323 \equiv 4 \cdot 7.$$

- (ii) Use this information and the results of part (i) to find  $\log_5(323)$ .

- 17.12. (i) I know that  $\log_{17} 5 = 57$ , so  $17^{57} \equiv 5 \pmod{503}$ . Solve  $5^x \equiv 17 \pmod{503}$ . What, then, is  $\log_5 17$ ?  
(ii) Suppose I know that  $\log_{17} 323 = 458$  in  $U_{503}$ . If I know  $\log_5 17$ , can I then determine  $\log_5 323$ ?  
17.13. Suppose Eve worked with the cyclic group  $U_p$  with generator  $g$  (a fixed primitive root modulo  $p$ ) and generated a database of  $\log_g(q)$  for a large collection of primes  $q$ . Suppose Alice and Bob used the same cyclic group  $U_p$  but chose a different generator (primitive root)  $h$  for the group. Would Eve’s database be of use for finding  $\log_h(x)$  for any  $x$  in  $U_p$ ? How would Eve proceed? (See Exercise 17.12.)

## Appendix: Fermat’s Method Versus Trial Division

Let  $m = pq$ , a product of two odd primes  $p > q$ . Then  $q$  is the smallest non-trivial factor of  $m$ , and mod 30 trial division would reach  $q$  after  $\frac{8}{30}q$  trial divisions (give or take a few divisions, such as those by 2, 3 and 5).

Let  $p = b + c$  and  $q = b - c$ , then  $b = (p + q)/2$ ,  $c = (p - q)/2$ , and  $m = (b + c)(b - c) = b^2 - c^2$ . The number of trials of Fermat’s method is then the largest integer  $< b - \sqrt{m}$ .

To compare the number of mod 30 trial divisions needed to factor  $m$  with the number of Fermat trials needed to factor  $m$ , we compare the size of  $b - \sqrt{m}$  and  $\frac{8}{30}q$ .

**Proposition 17.13** *Fermat's method factors  $m$  in fewer steps than mod 30 trial division if and only if  $q > \frac{4.05}{7}\sqrt{m}$ .*

*Proof* We have  $b = \frac{1}{2}(q + p) = \frac{1}{2}(q + \frac{m}{q})$ , and so the number of Fermat trials is

$$b - \sqrt{m} = \frac{1}{2}(q + \frac{m}{q}) - \sqrt{m}.$$

So the number of Fermat divisions is less than the number of mod 30 trial divisions when

$$\begin{aligned} \frac{8}{30}q &> \frac{1}{2}(q + \frac{m}{q}) - \sqrt{m} \\ \sqrt{m} &> \frac{7}{30}q + \frac{m}{2q}. \end{aligned}$$

Multiplying by  $30q/7$  gives

$$\frac{30}{7}q\sqrt{m} > q^2 + \frac{15}{7}m$$

or

$$-\frac{15}{7}m > q^2 - \frac{30}{7}q\sqrt{m}.$$

Completing the square on the right side gives

$$\frac{120}{49}m > (q - \frac{15}{7}\sqrt{m})^2.$$

Since  $q < \sqrt{m}$ , taking the positive square root of both sides gives

$$\frac{\sqrt{120}}{7}\sqrt{m} > \frac{15}{7}\sqrt{m} - q.$$

Hence Fermat's method is faster when

$$q > \frac{(15 - \sqrt{120})}{7}\sqrt{m}.$$

Since  $\sqrt{120} = 10.95$ , we conclude that Fermat's method is faster when the smaller prime factor  $q$  of  $m$  satisfies

$$q > \frac{4.05}{7}\sqrt{m}.$$

□

To illustrate the bound, here is a table of examples of numbers  $m$  near 20,745,000 that are the product of two primes, comparing the number of mod 30 trial divisions needed to factor  $m$  and the number of Fermat trials. As we move down the table, the Fermat trials method gets better and mod 30 trial division gets worse. For the fifth example, the square root of  $2633 * 7879 = 20745407$  is 4554.7, and  $\frac{15 - \sqrt{120}}{7}(4555) = 2632$ . So the inequality of the proposition is almost an equality, corresponding to the fact that Fermat's method and mod 30 trial division take almost exactly the same number of steps.

$q$	$p$	$m$	Fermat trials	mod 30 trials
359	57781	20743379	24516	96
773	26839	20746547	9251	206
1409	14723	20744707	3511	376
2203	9419	20750057	1256	587
2633	7879	20745407	701	702
3001	6911	20739911	402	800
3163	6563	20758769	307	843
3559	5827	20738293	139	949
4007	5179	20752253	38	1069
4363	4751	20728613	4	1163
4507	4603	20745721	1	1202

The last line of the table shows that when we try Fermat's method on the last example,  $m = 20745721$ , the square root  $\sqrt{20745721} = 4554.7$ , and so the first step is

$$4555^2 - 20745721 = 2304 = 48^2.$$

It takes just one trial of Fermat's method to find the two factors of  $m$ ,  $4555 - 48 = 4507$  and  $4555 + 48 = 4603$ .

# Chapter 18

## Polynomials and Finite Fields



In this chapter we show how to construct all fields with a finite number of elements, “finite fields”. We already know an infinite set of finite fields, namely the fields  $\mathbb{Z}_p$  of integers modulo  $p$  for  $p$  a prime number. Those fields are often called *prime fields*. But starting from the ring of polynomials over a finite field and using the same ideas we used to construct  $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ , we can construct all finite fields. We’ll show how that is done in this chapter.

One reason we do this is that some applications routinely use finite fields other than prime fields. We’ll do an example of a Reed-Solomon code using a field of 8 elements in Chapter 19. Many applications use Reed-Solomon codes constructed with a field of  $2^8 = 256$  elements. The widely used symmetric cryptosystem AES uses a field of 256 elements, as we’ll note in the last section of this chapter.

The construction of finite but non-prime fields involves manipulations with polynomials. In order to work with  $\mathbb{Z}_m$  for  $m$  an integer, we needed to know some facts and algorithms involving integers. For example, to find the inverse of a number  $a$  modulo  $m$ , we needed first to know that the inverse of  $a$  exists, which is equivalent to knowing that the greatest common divisor of  $a$  and  $m$  is 1. Then, to find the inverse of  $a$  modulo  $m$ , we needed to find Bezout’s identity, that is, to find integers  $r$  and  $s$  so that  $ar + ms = 1$ : then  $r$  is the inverse of  $a$  modulo  $m$ .

We begin this chapter by showing that in the ring  $F[x]$  of polynomials with coefficients in a field  $F$ , a similar theory is true.

### 18.1 Greatest Common Divisors

In the first two sections of this chapter, we follow the development in Chapters 3 and 4 very closely. In those chapters we defined the greatest common divisor of two numbers, showed that the greatest common divisor can be found by Euclid’s Algorithm, and obtained Bezout’s Identity. Using Bezout’s Identity, we showed that every number factors uniquely into a product of prime numbers.

The same theory works for polynomials with coefficients in a field, and we’ll elaborate on that fact before we begin constructing new fields.

We work in the ring  $F[x]$  of polynomials, where  $F$  is a field. We’ll often write  $f, g, m$ , etc. for  $f(x), g(x), m(x)$ , etc. We begin with the greatest common divisor.

Let  $f, g$  be in  $F[x]$ . A polynomial  $p$  in  $F[x]$  is a *greatest common divisor* (g.c.d.) of  $f$  and  $g$  if  $p$  divides  $f$  and  $p$  divides  $g$ , and if  $q$  in  $F[x]$  divides  $f$  and  $g$ , then  $\deg(q) \leq \deg(p)$ . That is,  $p$  is a common divisor of  $f$  and  $g$  of largest degree.

*Example 18.1* Let  $F = \mathbb{Q}$ . The polynomials  $f(x) = 12x^2 + 7x + 1$  and  $g(x) = 3x^3 + 4x^2 + 4x + 1$  have a common divisor  $3x + 1$ , because

$$\begin{aligned}f(x) &= (3x + 1)(4x + 1) \\g(x) &= (3x + 1)(x^2 + x + 1).\end{aligned}$$

Since  $f(x)$  doesn't divide  $g(x)$ , no polynomial of degree 2 can be a common divisor of  $f$  and  $g$ .

But also, we see that  $f(-\frac{1}{3}) = 0$  and  $g(-\frac{1}{3}) = 0$ , so by the Root Theorem,  $x + \frac{1}{3}$  is a common divisor of  $f$  and  $g$ .

So  $f$  and  $g$  have two greatest common divisors,  $3x + 1$  and  $x + \frac{1}{3}$ . But  $3x + 1 = 3(x + \frac{1}{3})$ . This reflects the fact, which we'll prove shortly, that given any two greatest common divisors of  $f$  and  $g$ , each is a scalar multiple of the other.

**Euclid's Algorithm.** Just as for numbers, we can find a greatest common divisor of two polynomials by using the Division Theorem repeatedly. The process is called Euclid's Algorithm for polynomials. Here it is for the two polynomials above.

*Example 18.2* Let  $f(x) = 12x^2 + 7x + 1$  and  $g(x) = 3x^3 + 4x^2 + 4x + 1$ . We take the polynomial of lower degree,  $f(x)$  and divide it into  $g(x)$ :

$$3x^3 + 4x^2 + 4x + 1 = (12x^2 + 7x + 1)\left(\frac{1}{4}x + \frac{3}{16}\right) + \left(\frac{39}{16}x + \frac{13}{16}\right),$$

then divide the remainder into the divisor:

$$12x^2 + 7x + 1 = \left(\frac{39}{16}x + \frac{13}{16}\right)\left(\frac{64}{13}x + \frac{16}{13}\right) + 0.$$

The last non-zero remainder is

$$r = \frac{39}{16}x + \frac{13}{16},$$

so  $r$  is a greatest common divisor of  $f$  and  $g$ .

Notice that

$$r = \frac{39}{16}x + \frac{13}{16} = \frac{13}{16}(3x + 1),$$

a constant (or scalar) multiple of the greatest common divisor we found earlier.

In general Euclid's Algorithm for two non-zero polynomials  $f$  and  $g$  works just as with numbers.

Divide  $f$  into  $g$ :

$$g = fq_1 + r_1.$$

Then divide the remainder into the divisor:

$$f = r_1q_2 + r_2.$$

Then repeat:

$$\begin{aligned} r_1 &= r_2 q_3 + r_3 \\ r_2 &= r_3 q_4 + r_4 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} + r_{n+1}. \end{aligned}$$

The process stops when  $r_{n+1} = 0$ , the zero polynomial.

Since by the Division Theorem,  $\deg r_1 < \deg f$ ,  $\deg r_2 < \deg r_1$ , etc., the sequence of divisions ends after at most  $\deg f$  steps.

**Theorem 18.3** (Euclid's Algorithm) *Given two non-zero polynomials  $f, g$  in  $F[x]$  with  $f \neq 0$ , the last non-zero remainder in Euclid's Algorithm is a greatest common divisor of  $f$  and  $g$ .*

The proof that the last non-zero remainder is a greatest common divisor of  $f$  and  $g$  is proved in the same way as for numbers. The key idea is

**Proposition 18.4** *If  $g = fq + r$ , then every common divisor of  $f$  and  $g$  is also a common divisor of  $f$  and  $r$ , and conversely.*

Thus in Euclid's Algorithm, every greatest common divisor of  $f$  and  $g$  is a greatest common divisor of  $g$  and  $r_1$ , which in turn is a greatest common divisor of  $r_1$  and  $r_2, \dots$ , which in turn is a greatest common divisor of  $r_{n-1}$  and  $r_n$ . But since  $r_n$  divides  $r_{n-1}$ , the greatest common divisors of  $r_n$  and  $r_{n-1}$  are the non-zero scalar multiples  $cr_n$  of  $r_n$ . So  $r_n$  is a greatest common divisor of  $f$  and  $g$ , and every greatest common divisor of  $f$  and  $g$  divides  $r_n$ .

Two polynomials that are scalar multiples of each other are called *associates*. Euclid's Algorithm implies that every greatest common divisor of  $f$  and  $g$  is an associate of the last non-zero remainder in Euclid's Algorithm for  $f$  and  $g$ . In our example with  $f(x) = 12x^2 + 7x + 1$  and  $g(x) = 3x^3 + 4x^2 + 4x + 1$ , the two greatest common divisors we identified for  $f$  and  $g$ , namely  $3x + 1$  and  $x + \frac{1}{3}$ , are both associates of the last non-zero remainder in Euclid's algorithm, namely  $\frac{39}{16}x + \frac{13}{16}$ .

**Bezout's Identity.** Just as for numbers, we have Bezout's Identity for polynomials:

**Proposition 18.5** *If  $d$  is a greatest common divisor of two non-zero polynomials  $f$  and  $g$ , then  $d = af + bg$  for some polynomials  $a$  and  $b$ .*

To find  $a$  and  $b$ , we adapt the extended Euclidean algorithm row vector scheme that we used for numbers.

**Example 18.6** Let  $F = \mathbb{F}_3 = \mathbb{Z}_3$ , and represent the elements of  $F$  by 0, 1, and 2 = -1. Let  $f = x^3 + 2x + 2$ ,  $g = x^3 + x^2 + 2x$ . Then Euclid's algorithm is

$$\begin{aligned} g &= f + (x^2 + 1) \\ f &= (x^2 + 1)x + (x + 2) \\ (x^2 + 1) &= (x + 2)(x + 1) + 2. \end{aligned}$$

Set  $r_1 = x^2 + 1$ ,  $r_2 = x + 2$ ,  $r_3 = 2$ . Then solving for  $r_1, r_2, r_3$ , we have

$$\begin{aligned} g - f &= r_1 \\ f - r_1x &= r_2 \\ r_1 - r_2(x + 1) &= r_3. \end{aligned}$$

The EEA yields a sequence of row vectors, starting with

$$(g, 1, 0),$$

which means  $g = 1 \cdot g + 0 \cdot f$ , and

$$(f, 0, 1),$$

which means  $g = 0 \cdot g + 1 \cdot f$ . Then from Euclid's Algorithm, we find

$$(g, 1, 0) - (f, 0, 1) = (g - f, 1, -1) = (r_1, 1, -1)$$

which means  $r_1 = 1 \cdot g + 2 \cdot f$  (since  $-1 = 2$ );

$$(f, 0, 1) - x(r_1, 1, -1) = (f - xr_1, -x, x + 1) = (r_2, -x, x + 1),$$

which means  $r_2 = -x \cdot g + (x + 1) \cdot f$ ; and

$$\begin{aligned} (r_1, 1, -1) - (x + 1)(r_2, -x, x + 1) \\ &= (r_1 - (x + 1)r_2, x^2 + x + 1, 2x^2 + x + 1) \\ &= (r_3, x^2 + x + 1, 2x^2 + x + 1). \end{aligned}$$

The last line yields Bezout's Identity:

$$r_3 = 2 = (x^2 + x + 1)(x^3 + x^2 + 2x) + (2x^2 + x + 1)(x^3 + 2x + 2).$$

To prove that Bezout's identity exists, we use Well-Ordering.

*Proof* Let

$$J = \{h \in F[x] : h = af + bg \text{ for some } a, b \text{ in } F[x]\}.$$

Since at least one of  $f$  and  $g$  is not zero, then  $J$  contains a non-zero polynomial (if  $f \neq 0$ , then  $J$  contains  $f \cdot 1 + g \cdot 0 = f$ .) So the set  $\mathcal{E}$  of degrees of polynomials in  $J$  is a non-empty set of integers  $\geq 0$ . By Well-Ordering, there is a polynomial  $d$  in  $J$  whose degree  $e$  is minimal.

Let  $d = af + bg$  for some polynomials  $a, b$  in  $F[x]$ . We claim:  $d$  divides  $f$  and  $d$  divides  $g$ . For example, to show that  $d$  divides  $f$ , we apply the Division Theorem:

$$f = dq + r$$

with  $\deg(r) < \deg(d)$ . Then

$$r = f - dq = f - q(af + bg) = (1 - qa)f + (qb)g$$

so  $r$  is in  $J$ . If  $r \neq 0$ , then  $r$  is a non-zero polynomial in  $J$  of smaller degree than  $d$ , which is a contradiction to the assumption that  $\deg(d)$  is the minimal number in the set  $\mathcal{E}$  of degrees of non-zero polynomials in  $J$ . So  $r$  must = 0, and so  $d$  divides  $f$ .

In the same way,  $d$  divides  $g$ . So  $d$  is a common divisor of  $f$  and  $g$ .

To show that  $d$  is a greatest common divisor of  $f$  and  $g$ , we show that every common divisor of  $f$  and  $g$  divides  $d$ . But clearly if  $h$  is a common divisor of  $f$  and  $g$ , then  $h$  divides  $rf + sg$  for all polynomials  $r$  and  $s$  in  $F[x]$ —just write  $f = hm$ ,  $g = hn$  for some polynomials  $m$  and  $n$ . So in particular, any common divisor  $h$  of  $f$  and  $g$  divides  $d = ar + bf$ . Hence  $d$  is a greatest common divisor of  $f$  and  $g$ .  $\square$

Every non-zero polynomial in  $F[x]$ ,  $F$  a field, is an associate of a monic polynomial (for if the leading coefficient of  $f(x)$  is  $a_n \neq 0$ , then the leading coefficient of  $a_n^{-1}f(x)$  is = 1.) So we can always choose a greatest common divisor of  $f$  and  $g$  to be monic. Hereafter, when we call a polynomial  $d$  the greatest common divisor of  $f$  and  $g$ , we will mean that  $d$  is the unique monic polynomial of smallest degree that divides both  $f$  and  $g$ .

*Example 18.7* Using Euclid's Algorithm, we found that  $f(x) = 12x^2 + 7x + 1$  and  $g(x) = 3x^3 + 4x^2 + 4x + 1$  have a greatest common divisor  $\frac{39}{16}x + \frac{13}{16}$ . We also observed that  $3x + 1$  is a greatest common divisor, because

$$\begin{aligned} f(x) &= (3x + 1)(4x + 1) \\ g(x) &= (3x + 1)(x^2 + x + 1). \end{aligned}$$

Also  $x + \frac{1}{3}$  is a greatest common divisor, and is monic. So if we refer to the greatest common divisor of  $f$  and  $g$  here, we'll mean  $x + \frac{1}{3}$ .

Using the EEA, we can write the last non-zero remainder  $r_n$  in Euclid's Algorithm as  $r_n = af + bg$  for some polynomials  $a$  and  $b$ . If  $d$  is the unique monic greatest common divisor of  $f$  and  $g$ , then  $sr_n = d$  for some non-zero constant  $s$  in  $F$ . Then

$$d = (sa)f + (sb)g,$$

so we can also obtain the (monic) greatest common divisor of  $f$  and  $g$  as in Bezout's identity.

Adapting the notation for the greatest common divisor of two numbers, let  $(f, g)$  be the unique monic greatest common divisor of  $f$  and  $g$ .

Say that  $f$  and  $g$  are *coprime*, or *relatively prime*, if every greatest common divisor of  $f$  and  $g$  has degree 0. In that case, 1 is the greatest common divisor (since 1 is the only monic polynomial of degree 0 and is an associate of any non-zero constant polynomial), and we can write  $1 = rf + sg$  for some polynomials  $r$  and  $s$ .

The analogous fact for numbers is the key fact we used for showing that factorization of numbers into products of prime numbers is unique. And so it is for polynomials, as we now see.

## 18.2 Factorization into Irreducible Polynomials

We recall the units of  $F[x]$ , from Corollary 6.2:

**Proposition 18.8** *If  $F$  is a field, then the units of  $F[x]$  are the units of  $F$ , where  $F$  is identified as the set of polynomials of degree  $\leq 0$  in  $F[x]$ .*

This is a consequence of the *degree property*: for  $f, g$  in  $F[x]$ ,  $F$  a field,

$$\deg(f) + \deg(g) = \deg(fg).$$

**Definition** A non-zero polynomial  $p$  in  $F[x]$  is *irreducible* if  $p$  has degree  $\geq 1$ , and if  $p$  factors in any way as  $p = fg$ , then  $f$  or  $g$  must have degree  $= 0$ , that is, be a constant polynomial.

Here are some examples of irreducible polynomials:

For every  $a$  in the field  $F$ , the polynomial  $x - a$  is irreducible, because of the degree property.

$x^2 + 1$  is irreducible in  $\mathbb{R}[x]$ , but  $x^2 + 1$  is not irreducible in  $\mathbb{C}[x]$ : it factors as  $(x - i)(x + i)$  where  $i = \sqrt{-1}$  in  $\mathbb{C}$ .

$x^3 - 3$  is irreducible in  $\mathbb{Q}[x]$ , but not in  $\mathbb{R}[x]$ .

We'll see how to find more examples in the next section.

Irreducible polynomials are like prime numbers. In particular:

**Proposition 18.9** *If  $p$  is an irreducible polynomial in  $F[x]$ , and  $f$  is a polynomial which is not divisible by  $p$ , then the greatest common divisor of  $p$  and  $f$  is 1.*

*Proof* Suppose  $d = (f, p)$  (so  $d$  is monic). Then  $dh = p$  for some polynomial  $h$ . Since  $p$  is irreducible, either  $h$  or  $d$  has degree 0. If  $h$  has degree 0, then  $p$  and  $d$  are associates, so  $p$  divides  $f$ . So if  $p$  does not divide  $f$ , then  $d$  has degree 0, hence  $d = 1$ .  $\square$

Irreducible polynomials in  $F[x]$ ,  $F$  a field, are the multiplicative building blocks of nonconstant polynomials, just as primes are the building blocks of natural numbers  $> 1$ :

**Theorem 18.10** *Every polynomial of degree  $\geq 1$  in  $F[x]$ ,  $F$  a field, is irreducible or factors into a product of irreducible polynomials.*

The proof is virtually identical to that for numbers, an induction argument on the degree of the polynomial, and is left as Exercise 18.5, below.

The proof that factorization of a polynomial into a product of irreducible polynomials is unique is almost identical to the proof of unique factorization of numbers into products of primes. The key lemma in the proof, as with numbers, is the Coprime Divisibility Lemma:

**Proposition 18.11** *For  $f, g, h$  in  $F[x]$ ,  $F$  a field, if  $f$  divides  $gh$  and  $f$  and  $g$  are coprime, then  $f$  divides  $h$ .*

*Proof (The same as for numbers)* Apply Bezout's identity to  $f$  and  $g$ : if  $f$  and  $g$  are coprime, there are polynomials  $a$  and  $b$  so that

$$fa + gb = 1.$$

Multiply both sides by  $h$  to get  $fah + ghb = h$ . Then  $f$  divides  $fah$  and  $ghb$ , so  $f$  divides  $h$ .  $\square$

Then, just as with numbers, we have

**Corollary 18.12** *Let  $p$  be an irreducible polynomial in  $F[x]$ ,  $F$  a field. For every polynomials  $f, g$  in  $F[x]$ , if  $p$  divides  $fg$ , then  $p$  divides  $f$  or  $p$  divides  $g$ .*

This follows by Propositions 18.9 and 18.11.

Here is the theorem on uniqueness of factorization:

**Theorem 18.13** *In  $F[x]$ ,  $F$  a field, if*

$$f = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

*are two factorizations of the polynomial  $f$  into a product of irreducible polynomials in  $F[x]$ , then  $s = t$  and there is a one-to-one correspondence between the factors  $p_1, p_2, \dots, p_s$  and  $q_1, q_2, \dots, q_t$ , where if  $p_i$  corresponds with  $q_j$ , then  $p_i$  and  $q_j$  are associates.*

Every factorization of an associate of  $f$  will have factors that are associates of a factorization of  $f$ . For example, in  $\mathbb{Q}[x]$ ,

$$f(x) = 12x^2 + 7x + 1 = (3x + 1)(4x + 1).$$

The monic polynomial which is an associate of  $f(x)$  factors as

$$x^2 + \frac{7}{12}x + \frac{1}{12} = \left(x + \frac{1}{3}\right)\left(x + \frac{1}{4}\right).$$

The two polynomials are associates of each other, and the factors  $3x + 1$  and  $4x + 1$  are associates of  $x + \frac{1}{3}$  and  $x + \frac{1}{4}$ , respectively.

Since every polynomial is an associate of a unique monic polynomial (that is, a polynomial with leading coefficient = 1), and the product of monic polynomials is monic, we can rephrase the theorem on unique factorization to require that  $f$  and all  $p_i$  and  $q_j$  be monic polynomials. In this case, the theorem resembles the corresponding theorem for numbers very closely, with “monic polynomial” corresponding to “positive integer”:

**Theorem 18.14** *In  $F[x]$ ,  $F$  a field, if*

$$f = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

*are two factorizations of the monic polynomial  $f$  into a product of monic irreducible polynomials in  $F[x]$ , then  $s = t$  and after a suitable renumbering of  $q_1, \dots, q_s$ , we have  $p_1 = q_1, p_2 = q_2, \dots, p_s = q_s$ .*

We have left several of the proofs in this section, including the proof of Theorem 18.14, as exercises, because the theorems and the proofs are so similar to those for natural numbers.

**Exponential notation.** Just as with integers, we can write the factorization of a polynomial  $f$  in  $F[x]$  in exponential notation, as

$$f = p_1^{e_1} p_2^{e_2} \cdots p_g^{e_g}$$

where  $p_1, p_2, \dots, p_g$  are distinct irreducible polynomials. If any  $e_i$  is bigger than 1, we shall say that  $f$  has a *multiple factor*: thus  $f(x) = (x^3 + 5)^3(x + 1)$  in  $\mathbb{R}[x]$  has a multiple factor, while  $f(x) = (x^2 + 2)(x - 5)$  does not. If  $f(x)$  has a multiple linear factor, then  $f(x)$  is said to have a *multiple root* in  $F$ . An example is  $f(x) = (x + 2)^3(x^2 + 1)$ , which has the multiple root  $-2$ .

Exponential notation for polynomials satisfies the same properties as exponential notation does for numbers. Let  $p$  be an irreducible polynomial. For a non-zero polynomial  $f$ , the notation  $p^e \parallel f$  means that  $p^e$  divides  $f$  but  $p^{e+1}$  does not. Then  $f$  divides  $g$  if and only if for each irreducible polynomial  $p$  that divides  $f$  or  $g$ , if  $p^d \parallel f$  and  $p^e \parallel g$ , then  $d \leq e$ .

We can then write down the greatest common divisor of  $f$  and  $g$ , and the least common multiple of  $f$  and  $g$  in terms of the factorizations of  $f$  and  $g$ .

For example, in  $\mathbb{Q}[x]$  if  $f = (x^2 + 2)^4(x - 5)$  and  $g = (x^2 + 2)^2(x - 5)^3(x - 7)$ , then

$$(f, g) = (x^2 + 2)^2(x + 5), \quad [f, g] = (x^2 + 2)^4(x - 5)^3(x - 7).$$

### 18.3 Ideals of $F[x]$

We observed in Chapter 6 that if  $F$  is a field (or more generally, if  $F$  is a commutative ring), then the set  $F[x]$  is a commutative ring. The field  $F$  is contained in  $F[x]$  as the set of polynomials of degree  $\leq 0$ . The units of  $F[x]$  are exactly the polynomials of degree 0, that is, the non-zero elements of  $F$  viewed as polynomials.

Recall from Section 5.4 that an ideal of a commutative ring  $R$  is a subset  $J$  of  $R$  that is closed under addition and scalar multiplication.

We can describe all of the ideals of  $F[x]$  when  $F$  is a field. The result is very similar to that for the commutative ring  $\mathbb{Z}$ . For  $\mathbb{Z}$  we showed that there was a one-to-one correspondence between the natural numbers and the non-zero ideals of  $\mathbb{Z}$  by the map sending  $m$  in  $\mathbb{N}$  to  $m\mathbb{Z}$ , the principal ideal of  $\mathbb{Z}$  consisting of all multiples of  $m$ .

For  $m = m(x)$  in  $F[x]$ , let  $\langle m \rangle$  denote the ideal of  $F[x]$  generated by  $m$ :

$$\langle m \rangle = \{fm \mid f \text{ in } F[x]\},$$

the set of all polynomial multiples of  $m$ . Then  $\langle m \rangle$  is the principal ideal of  $F[x]$  generated by  $m$ .

*Example 18.15*

$$\langle x \rangle = \{xf(x) \mid f(x) \text{ in } F[x]\}.$$

This is the set of all polynomials with coefficients in  $F$  that have no term of degree 0.

Here is the analogue for  $F[x]$  of Proposition 5.14:

**Theorem 18.16** *Let  $F$  be a field. Every non-zero ideal of  $F[x]$  is a principal ideal, generated by a monic polynomial. The function from monic polynomials in  $F[x]$  to ideals of  $F[x]$  given by  $m \mapsto \langle m \rangle$  is a bijection.*

*Proof* To show the first statement, let  $J$  be a non-zero ideal. Then  $J$  contains a polynomial of degree  $\geq 0$ . Let  $S$  be the set of degrees of non-zero polynomials in  $J$ . Then  $S$  is non-zero. Let  $d$  be the smallest element of  $S$  and let  $m$  be a monic polynomial in  $J$  of degree  $d$ . We claim that  $J = \langle m \rangle$ : that is, every polynomial  $g$  in  $J$  is a multiple of  $m$ .

To see this, let  $g$  be in  $J$ . Divide  $g$  by  $m$  as in the Division Theorem:  $g = mq + r$ . Then  $r$  is in  $J$  because  $J$  is closed under scalar multiplication (so  $mq$  is in  $J$ ) and addition (so that  $g - mq = r$  is in  $J$ ). But since  $r$  is the remainder, we have  $\deg(r) < \deg(m)$ . If  $r \neq 0$ , then  $\deg(r)$  is in  $S$  and is less than  $\deg(m) = d$ , in violation of the assumption on  $d$ . So  $r = 0$  and  $m$  divides  $g$ . So  $J = \langle m \rangle$ .

Now consider the function  $\theta$  from the set of non-zero monic polynomials in  $F[x]$  to ideals of  $F[x]$ , given by  $m \mapsto \langle m \rangle$ .

By what we just showed,  $\theta$  is onto.

We wish to show that  $\theta$  is one-to-one. That means, if  $\langle m_1 \rangle = \langle m_2 \rangle$ , where  $m_1$  and  $m_2$  are monic polynomials in  $F[x]$ , then  $m_1 = m_2$ .

But if  $\langle m_1 \rangle = \langle m_2 \rangle$ , then  $m_1 = rm_2$  and  $m_2 = sm_1$  for some polynomials  $r$  and  $s$ . By the degree formula,  $\deg(m_1) = \deg(r) + \deg(m_2)$  and  $\deg(m_2) = \deg(s) + \deg(m_1)$ , where  $\deg(r)$  and  $\deg(s)$

are  $\geq 0$ . Thus  $\deg(m_1) \leq \deg(m_2)$  and  $\deg(m_2) \leq \deg(m_1)$ . Thus  $\deg(m_1) = \deg(m_2)$ , and  $r$  and  $s$  are non-zero elements of  $F$ .

But if  $m_1$  and  $m_2$  are monic,  $m_1 = rm_2$  and  $r$  is an element of  $F$ , then looking at leading coefficients, we see that  $r = 1$ . So  $m_1 = m_2$ .

Hence  $\theta$  is one-to-one. □

## 18.4 Cosets and Quotient Rings

In Chapter 5 we constructed the commutative ring  $\mathbb{Z}/m\mathbb{Z}$  as the set of cosets of the ideal  $m\mathbb{Z}$ . By doing so, we could work with representatives of those cosets, but we were free to replace one representative by another whenever convenient.

Two integers  $a$  and  $b$  are representatives of the same coset of  $m\mathbb{Z}$  if  $a$  and  $b$  are congruent modulo  $m$ :  $a + m\mathbb{Z} = b + m\mathbb{Z}$  if and only if  $a \equiv b \pmod{m}$ .

Thus we could work with elements of  $\mathbb{Z}/m\mathbb{Z}$  as though they were integers, remembering always that any conclusions were only meaningful modulo  $m$ .

We can do the same with polynomials modulo an ideal. To construct new commutative rings, the idea is to take an ideal  $\langle m \rangle$  of  $F[x]$  and form the quotient ring, consisting of the cosets of  $\langle m \rangle$  in  $F[x]$ .

We recall the general construction of a quotient ring that we introduced in Chapter 5, and then applied to obtain the ring  $\mathbb{Z}/m\mathbb{Z}$ .

Given a commutative ring  $R$ , an ideal  $J$  of  $R$ , and an element  $a$  of  $R$ , the coset  $a + J$  is the subset of  $R$ :

$$a + J = \{a + s \mid s \text{ in } J\}.$$

Two cosets  $a + J$  and  $a' + J$  are equal precisely if  $a - a'$  is in  $J$  (Proposition 5.15).

Given elements  $a$  and  $b$  of  $R$ , we define addition and multiplication of cosets by

$$\begin{aligned}(a + J) + (b + J) &= (a + b) + J \\ (a + J) \cdot (b + J) &= ab + J.\end{aligned}$$

We showed in Proposition 5.18 that these operations are “well-defined”. This means that if  $a + J = a' + J$  and  $b + J = b' + J$ , then

$$\begin{aligned}(a + b) + J &= (a' + b') + J \\ ab + J &= a'b' + J.\end{aligned}$$

Consequently, the operations of addition and multiplication on the set  $R/J$  of cosets of  $J$  in  $R$  make the set  $R/J$  into a commutative ring (Theorem 5.13).

In Section 5.4 we applied this construction to the ring of integers  $\mathbb{Z}$  and the ideal  $m\mathbb{Z}$  consisting of all multiples of a number  $m$ , and obtained  $\mathbb{Z}/m\mathbb{Z}$ , the ring of integers modulo  $m$ .

Now we apply the same construction to the ring  $F[x]$  of polynomials with coefficients in a field  $F$ . Here, as with  $\mathbb{Z}$ , every ideal  $J$  of  $F[x]$  is a principal ideal, generated by a unique monic polynomial  $m(x)$  of minimal degree in  $J$ . Then  $J = \langle m \rangle$  consists of all polynomial multiples of  $m(x)$ . In set notation,

$$J = \{a(x)m(x) \mid a(x) \text{ in } F[x]\}.$$

We'll denote this ideal by  $\langle m(x) \rangle$ , or just  $\langle m \rangle$  (leaving out the “(x)” for brevity) and we'll write the quotient ring  $F[x]/J$  as  $F[x]/\langle m(x) \rangle$  or  $F[x]/\langle m \rangle$ , the ring of polynomials modulo  $m(x)$ .

Any element of a coset of  $J$  in  $F[x]$  is called a representative of that coset. If we write a coset as  $f(x) + \langle m(x) \rangle$ , then  $f(x)$  is a representative of the coset. But so is  $f(x) + m(x)s(x)$  for every polynomial  $s(x)$  in  $F[x]$ . In particular, if the degree of  $f(x)$  is not less than the degree of  $m(x)$ , then we can divide  $f(x)$  by  $m(x)$ , and by the Division Theorem for polynomials, we have

$$f(x) = m(x)q(x) + r(x)$$

where  $\deg(r(x)) < \deg(m(x))$ . Then  $r(x) = f(x) - m(x)q(x)$  is in the coset  $f(x) + \langle m(x) \rangle$ , and so  $r(x)$  is a representative of the coset  $f(x) + \langle m(x) \rangle$ :

$$f(x) + \langle m(x) \rangle = r(x) + \langle m(x) \rangle.$$

So, just as every element of  $\mathbb{Z}/m\mathbb{Z}$  is represented by a unique number  $a$  with  $0 \leq a < m$ , we have

**Proposition 18.17** *Every coset  $f(x) + \langle m(x) \rangle$  in  $F[x]/\langle m(x) \rangle$  is represented by a unique polynomial  $r(x)$  of degree  $< \deg(m(x))$ .*

To summarize what we have just observed:

**Theorem 18.18** *Let  $F$  be a field, and  $m$  a monic polynomial of degree  $\geq 1$  in  $F[x]$ . Then  $F[x]/\langle m \rangle$  is a commutative ring, made up of the cosets  $a + \langle m \rangle$  for  $a$  in  $F[x]$ . Every coset has a representative  $a$  of degree  $< \deg(m)$ . Thus there is a bijection between the elements of  $F[x]/\langle m \rangle$  and polynomials in  $F[x]$  of degree  $< \deg(m)$ .*

*Example 18.19* For  $F$  a field, let  $m = x^2 + 1$  in  $F[x]$ . Then  $F[x]/\langle m \rangle$  is the set of cosets  $f + \langle m \rangle$ . Since  $m = x^2 + 1$  has degree 2, every coset is represented by a polynomial in  $x$  of degree  $< 2$ . Thus

$$F[x]/\langle m \rangle = \{a + bx + \langle m \rangle : a, b \text{ in } F\}.$$

For example, let  $F = \mathbb{F}_2 = \{0, 1\}$ . Then there are four polynomials of degree  $< 2$ , so  $\mathbb{F}_2[x]/\langle m \rangle$  has four elements:

$$0 + \langle m \rangle, 1 + \langle m \rangle, x + \langle m \rangle, x + 1 + \langle m \rangle.$$

Addition in  $F[x]/\langle m \rangle$  is clear. Multiplication is clear except when we multiply two cosets represented by polynomials of degree 1.

Since  $x^2 - 1$  is in  $\langle m \rangle$  and  $-1 = 1$  in  $\mathbb{F}_2$ , we have

$$\begin{aligned} x^2 + \langle m \rangle &= x^2 - (x^2 + 1) + \langle m \rangle \\ &= -1 + \langle m \rangle \\ &= 1 + \langle m \rangle. \end{aligned}$$

So we have

$$\begin{aligned} (x + \langle m \rangle)(x + \langle m \rangle) &= x^2 + \langle m \rangle \\ &= 1 + \langle m \rangle, \end{aligned}$$

$$\begin{aligned} ((x + 1) + \langle m \rangle)(x + \langle m \rangle) &= x^2 + x + \langle m \rangle \\ &= (x + 1) + \langle m \rangle, \end{aligned}$$

$$\begin{aligned} ((x + 1) + \langle m \rangle)((x + 1) + \langle m \rangle) &= x^2 + 1 + \langle m \rangle \\ &= -1 + 1 + \langle m \rangle \\ &= 0 + \langle m \rangle. \end{aligned}$$

Let's denote the cosets  $0 + \langle m \rangle$ ,  $1 + \langle m \rangle$  by 0, 1, respectively, and denote  $x + \langle m \rangle$  by  $\alpha$ . The four elements of  $\mathbb{F}_2[x]/\langle m \rangle$  are

$$0, 1, \alpha, \alpha + 1$$

since  $x + 1 + \langle m \rangle = (x + \langle m \rangle) + (1 + \langle m \rangle)$ . Then  $\alpha^2 = -1 = 1$  in  $\mathbb{F}_2$ . So here is the multiplication table:

.	0	1	$\alpha$	$\alpha + 1$
0	0	0	0	0
1	0	1	$\alpha$	$\alpha + 1$
$\alpha$	0	$\alpha$	1	$\alpha + 1$
$\alpha + 1$	0	$\alpha + 1$	$\alpha + 1$	0

This ring has two units, 1 and  $\alpha$ , and one zero divisor,  $\alpha + 1$ .

The element  $\alpha = x + \langle m(x) \rangle$  has the useful property that  $\alpha^2 + 1 = 0$  in  $F[x]/\langle m(x) \rangle$ :

$$\begin{aligned} \alpha^2 + 1 &= (x + \langle m(x) \rangle)^2 + (1 + \langle m(x) \rangle) \\ &= (x^2 + 1) + \langle m(x) \rangle \\ &= 0 + \langle m(x) \rangle, \end{aligned}$$

because  $x^2 + 1 = m(x)$  is in the ideal  $\langle m(x) \rangle$ . So  $\alpha = x + \langle m(x) \rangle$  is a root in  $F[x]/\langle m(x) \rangle$  of the polynomial  $m(x)$ .

This last observation holds for every polynomial  $m(x)$ :

**Proposition 18.20** *Let  $m(x)$  be a monic polynomial with coefficients in  $F$ . Let  $R = F[x]/\langle m(x) \rangle$  be the quotient ring of cosets  $f(x) + \langle m(x) \rangle$  for  $f(x)$  in  $F[x]$ . Let  $\alpha = x + \langle m(x) \rangle$  and identify  $r + \langle m(x) \rangle$  with  $r$  for  $r$  in the field  $F$ . Then  $R = F[\alpha]$  where the coset  $\alpha = x + \langle m(x) \rangle$  is a root in  $R$  of  $m(x)$ .*

*Proof* Let

$$f(x) = a_0 + a_1x + \dots + a_dx^d.$$

be in  $F[x]$ , and let  $J$  be the ideal  $\langle m(x) \rangle$ . Let  $\alpha$  denote the coset  $x + \langle m(x) \rangle$ . We evaluate  $f(x)$  at  $\alpha$ :

$$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_d\alpha^d.$$

Now we identified elements of  $F$  with their cosets in  $F[x]/J$ . So writing those coefficients  $a_0, \dots, a_m$  as elements of  $F[x]/J$ , that is, as cosets of polynomials of degree  $\leq 0$ , we have

$$f(\alpha) = (a_0 + J) + (a_1 + J)(x + J) + \dots + (a_d + J)(x + J)^d.$$

To add and multiply cosets, we add and multiply the representatives in  $F[x]$ , then take the coset of the result. So

$$f(\alpha) = (a_0 + a_1x + \dots + a_dx^d) + J = f(x) + J.$$

In particular,  $m(\alpha) = m(x) + J$ . Since  $m(x)$  is in the ideal  $J = \langle m(x) \rangle$  generated by  $m(x)$ ,

$$m(\alpha) = m(x) + \langle m(x) \rangle = 0 + \langle m(x) \rangle = 0.$$

Note that  $\alpha$  is not a root of a polynomial  $f(x)$  of degree  $< \deg(m(x))$ , because  $f(x) + \langle m(x) \rangle \neq 0 + \langle m(x) \rangle$ :  $m(x)$  does not divide any non-zero polynomial of degree  $< \deg(m(x))$ .  $\square$

*Example 18.21* Let  $R = \mathbb{R}[x]/(x^2 + 1)$  and let  $x + (x^2 + 1) = \alpha$ . Then

$$R = \mathbb{R}[\alpha] = \{a + b\alpha \mid a, b \text{ in } R\}$$

where  $\alpha^2 + 1 = 0$ . For this example, the element  $x + (x^2 + 1)$  is commonly denoted by  $i$ . Thus  $R = \mathbb{R}[i] = \mathbb{C}$ , the complex numbers. Viewed in this way,  $i$  is not “imaginary”, but rather the coset  $x + (x^2 + 1)$ .

*Example 18.22* We construct a field with 8 elements.

Let  $F = \mathbb{F}_2$  and let  $m(x) = x^3 + x + 1$ . Let  $R = F[x]/\langle m(x) \rangle = F[\alpha]$  where  $\alpha = x + \langle m(x) \rangle$ . Since  $m(x)$  has degree 3, there is a bijection between elements of  $R$  and polynomials in  $\mathbb{F}_2[x]$  of degree  $\leq 2$ . There are eight polynomials of degree  $\leq 2$ , so  $R$  has eight elements:

$$0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1,$$

and  $\alpha^3 + \alpha + 1 = 0$ .

It turns out that  $F$  is a field. Since  $F$  has eight elements, we'll call it  $\mathbb{F}_8$ .

To see that  $\mathbb{F}_8$  is a field, we show that  $\alpha$  is a primitive root of  $F$ . To do so, recall that  $\alpha^3 + \alpha + 1 = 0$  and in  $\mathbb{F}_2$ ,  $-1 = 1$ , so  $\alpha^3 = \alpha + 1$ . So we can write down all the powers of  $\alpha$  as polynomials in  $\alpha$  of degree  $\leq 2$  by multiplying the previous power by  $\alpha$  and using the relation  $\alpha^3 = \alpha + 1$  to reduce any  $\alpha^3$ :

$$\begin{aligned}\alpha &= \alpha \\ \alpha^2 &= \alpha^2 \\ \alpha^3 &= \alpha + 1 \\ \alpha^4 &= \alpha^2 + \alpha \\ \alpha^5 &= \alpha^3 + \alpha^2 = (\alpha + 1) + \alpha^2 = \alpha^2 + \alpha + 1 \\ \alpha^6 &= \alpha^3 + \alpha^2 + \alpha = (\alpha + 1) + \alpha^2 + \alpha = \alpha^2 + 1 \\ \alpha^7 &= \alpha^3 + \alpha = (\alpha + 1) + \alpha = 1.\end{aligned}$$

From this computation it is clear that  $\mathbb{F}_8$  is a field, because

$$\mathbb{F}_8 = \{0, \alpha, \alpha^2, \dots, \alpha^6, \alpha^7\},$$

$\alpha^7 = 1$ , and the inverse of  $\alpha^e$  is  $\alpha^{7-e}$  for  $e = 1, \dots, 7$ .

In  $\mathbb{F}_2[x]$ , the polynomial  $x^3 + x + 1$  is irreducible. To see this, observe that since it has degree 3, if it has a factor of degree  $> 0$ , then it must have a factor of degree 1 by the degree formula, and therefore it must have a root. But  $x^3 + x + 1$  has no roots in  $\mathbb{F}_2$ . (The field  $\mathbb{F}_2$  has only two elements, 0 and 1, and neither is a root.)

The fact that  $x^3 + x + 1$  is irreducible and the commutative ring  $\mathbb{F}_2[x]/(x^3 + x + 1) = \mathbb{F}_2[\alpha] = \mathbb{F}_8$  is a field is true in general:

**Theorem 18.23** *Let  $F$  be a field, let  $m = m(x)$  be a polynomial of degree  $d$  with coefficients in  $F$ . Then  $F[x]/\langle m \rangle$  is a field if and only if  $m(x)$  is irreducible in  $F[x]$ .*

*Proof* If  $m(x) = r(x)s(x)$  is a non-trivial factorization of  $m(x)$  in  $F[x]$ , then  $r(x)$  and  $s(x)$  have degrees  $< d$ , so the cosets  $r(x) + \langle m(x) \rangle$  and  $s(x) + \langle m(x) \rangle$  are non-zero in  $F[x]/\langle m(x) \rangle$ , but their product is  $m(x) + \langle m(x) \rangle = 0 + \langle m(x) \rangle$ , the zero element of  $F[x]/\langle m(x) \rangle$ . So  $F[x]/\langle m(x) \rangle$  has zero divisors, hence cannot be a field.

On the other hand, suppose that  $m(x)$  is irreducible. It suffices to show that every non-zero element of  $F[\alpha] = F[x]/\langle m \rangle$  is invertible.

Given a non-zero polynomial  $f(x)$  of degree  $< \deg(m(x))$ , to show that  $f(\alpha)$  has an inverse, we observe that  $\deg(f(x)) < \deg(m(x))$  and  $m(x)$  is irreducible in  $F[x]$ . So the greatest common divisor of  $m(x)$  and  $f(x)$  is 1. By Bezout's Identity, there are polynomials  $g(x)$  and  $s(x)$  so that

$$f(x)g(x) + m(x)s(x) = 1.$$

So  $f(\alpha)g(\alpha) + m(\alpha)s(\alpha) = 1$ . But  $m(\alpha) = 0$ . So  $f(\alpha)g(\alpha) = 1$ .

Thus if  $m(x)$  is irreducible, then every non-zero element  $f(\alpha)$  of  $F[\alpha]$  has an inverse. So  $F[\alpha]$  is a field.  $\square$

*Remark* Viewing  $F[x]/\langle m(x) \rangle$  as  $F[\alpha]$  is similar to viewing  $\mathbb{Z}/m\mathbb{Z}$  as  $\mathbb{Z}_m$  with operations “modulo  $m$ ”. To see this, define congruence modulo a polynomial just as for integers:

**Definition** In  $F[x]$ , two polynomials  $f(x)$  and  $g(x)$  are congruent modulo  $m(x)$ , written

$$f(x) \equiv g(x) \pmod{m(x)},$$

if

$$f(x) = g(x) + m(x)q(x)$$

for some polynomial  $q(x)$  in  $F[x]$ .

Congruence modulo  $m(x)$  in  $F[x]$  is identical to congruence modulo the ideal  $\langle m(x) \rangle$ , defined in Section 5.4, just as congruence modulo  $m$  in  $\mathbb{Z}$  is identical to congruence modulo the ideal  $m\mathbb{Z}$ . The reason that congruence satisfies so many properties of equality is that  $f(x) \equiv g(x) \pmod{m(x)}$  if and only if the cosets  $f(x) + \langle m(x) \rangle$  and  $g(x) + \langle m(x) \rangle$  are equal, just as in  $\mathbb{Z}$ ,  $a \equiv b \pmod{m}$  if and only if the cosets  $a + m\mathbb{Z}$  and  $b + m\mathbb{Z}$  are equal.

When we look at  $F[x]/\langle m(x) \rangle$  as  $F[\alpha]$  where  $\alpha = x + \langle m(x) \rangle$  is a root of  $m(x)$ , then for any two polynomials  $f(x)$  and  $g(x)$  in  $F[x]$ , we have

$$\begin{aligned} f(x) + \langle m(x) \rangle &= g(x) + \langle m(x) \rangle, \text{ iff} \\ f(x) &\equiv g(x) \pmod{m(x)}, \text{ iff} \\ f(x) &= g(x) + m(x)q(x) \text{ for some polynomial } q(x), \text{ iff} \\ f(\alpha) &= g(\alpha). \end{aligned}$$

So operations on polynomials “modulo  $m(x)$ ” is the same as operations on polynomials evaluated at  $\alpha$ .

When we defined  $\mathbb{Z}_m$  as  $\{0, 1, \dots, m-1\}$  with operations modulo  $m$ , the possibility of confusion arises if the “mod  $m$ ” is not kept in mind. For example,  $1+1=2$  in  $\mathbb{Z}$ , but  $1+1=0$  in  $\mathbb{Z}_2$ . But viewing  $F[x]/\langle m(x) \rangle$  as  $F[\alpha]$  avoids the possibility of confusing elements of  $F[x]$  with elements of  $F[x]/\langle m(x) \rangle$ .

For example, if  $F = \mathbb{Q}$  and  $m(x) = x^2 + 2$ ,

$$x^3 + 3x + 1 \text{ is clearly in } F[x]$$

while

$$\alpha^3 + 3\alpha + 1 \text{ is clearly in } F[\alpha] = F[x]/\langle m(x) \rangle.$$

Since  $\alpha^2 + 2 = 0$ ,  $\alpha^3 + 3\alpha + 1 = -2\alpha + 3\alpha + 1 = \alpha + 1$ , while of course in  $F[x]$ ,  $x^3 + 3x + 1 \neq x + 1$ . (In this example, instead of  $\alpha$  one typically uses  $\sqrt{-2}$  as a symbol for  $x + \langle x^2 + 2 \rangle$ .)

## 18.5 Constructing Many Finite Fields

To get a field, pick a prime  $p$  and find an irreducible polynomial  $m(x)$  of degree  $d$  in  $\mathbb{F}_p[x]$ . Then  $\mathbb{F}_p[x]/\langle m(x) \rangle$  is a field with  $p^d$  elements.

*Example 18.24* Here is a field with  $2^4 = 16$  elements.

Let  $F = \mathbb{F}_2$  and let  $m(x) = x^4 + x + 1$ . Then  $m$  is irreducible in  $\mathbb{F}_2[x]$  by Exercise 18.14. So  $\mathbb{F}_2[x]/(x^4 + x + 1)$  is a field with  $2^4 = 16$  elements. Let  $\alpha = x + \langle m(x) \rangle$ . Then  $\alpha^4 + \alpha + 1 = 0$ , and we can write  $\mathbb{F}_2[x]/(x^4 + x + 1)$  as  $\mathbb{F}_2[\alpha]$ .

It turns out that  $\alpha$  has order 15 in the group of units of  $\mathbb{F}_2[\alpha]$ , and so  $\alpha$  is a primitive root of  $\mathbb{F}_2[\alpha]$ .

Here is another field with 16 elements. Let  $F = \mathbb{F}_2$  and let  $s(x) = x^4 + x^3 + x^2 + x + 1$ . Then  $s(x)$  is irreducible in  $\mathbb{F}_2[x]$ , so  $\mathbb{F}_2[x]/(s(x))$  is a field. Let  $\beta$  be the coset  $x + (s(x))$ . Then  $\beta$  is not a primitive root of  $\mathbb{F}_2[x]/(s(x))$ . To see this, observe that in  $F[x]$  for  $F$  any field,

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1) = (x - 1)s(x).$$

Since  $\beta$  is a root of  $s(x)$  in  $\mathbb{F}_2[x]/(s(x))$ , it follows that  $\beta$  is a root of  $x^5 - 1$ . So  $\beta$  has order  $\leq 5$  in  $\mathbb{F}_2[x]/(s(x))$ , not order 15.

Because  $\alpha^3$  is a root of  $x^4 + x^3 + x^2 + x + 1$ , there is an isomorphism of rings

$$j : \mathbb{F}_2[x]/(s(x)) \rightarrow \mathbb{F}_2[x]/(x^4 + x + 1),$$

given by  $j(f(\beta)) = f(\alpha^3)$  for every polynomial  $f(x)$  in  $\mathbb{F}_2[x]$ .

We can write down a field with  $p^d$  elements for every prime power  $< 100$ . There are 35 of them. There are the 25 prime fields  $\mathbb{F}_p$  for the 25 primes  $p < 100$ . The others have the form  $F = \mathbb{F}_p[x]/\langle m(x) \rangle$  for some prime  $p$  and some polynomial  $m(x)$  of degree  $d > 1$ ; then  $F$  has  $p^d$  elements. The possibilities for  $p^d < 100$  are listed in the following table.

$p$	# elements	$m(x)$
2	4	$x^2 + x + 1$
2	8	$x^3 + x + 1$
2	16	$x^4 + x + 1$
2	32	$x^5 + x^2 + 1$
2	64	$x^6 + x + 1$
3	9	$x^2 + x + 2$
3	27	$x^3 + 2x + 1$
3	81	$x^4 + x + 2$
5	25	$x^2 + x + 2$
7	49	$x^2 + x + 3$

We summarize some facts about finite fields.

**Proposition 18.25** (i) Every finite field contains  $\mathbb{F}_p$  for some prime number  $p$ .

(ii) Every finite field containing  $\mathbb{F}_p$  is of the form  $\mathbb{F}_p[x]/\langle m(x) \rangle$  for some irreducible polynomial  $m(x)$  in  $\mathbb{F}_p[x]$ , hence has  $p^n$  elements where  $n = \deg(m(x))$ .

(iii) If  $F$  and  $F'$  are two fields with  $p^n$  elements, there is a ring isomorphism from  $F$  to  $F'$ . Thus, up to isomorphism, for each  $n$  there is only one field of  $p^n$  elements.

(iv) For every prime  $p$  and every  $n > 0$ , there is an irreducible polynomial in  $\mathbb{F}_p[x]$  of degree  $n$ . Thus for every prime power  $p^n$ , there is a field with  $p^n$  elements.

All of these facts can be found in [Ch09] and in many other references.

**Primitive polynomials.** To find a field with  $p^n$  elements, all that is needed is an irreducible polynomial  $m(x)$  of degree  $n$  in  $\mathbb{F}_p[x]$ . Then, up to isomorphism, you can construct “the” field with  $p^n$  elements, as  $\mathbb{F}_p[x]/\langle m(x) \rangle$ . The only wrinkle might be that if you choose an irreducible polynomial  $m(x)$  and construct the field  $\mathbb{F}_p[\alpha] = \mathbb{F}_p[x]/\langle m(x) \rangle$ , you might like to know that  $\alpha$  is a primitive root of the field. Such is not always the case. We saw that with  $\mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1)$ , above.

*Example 18.26* A smaller example is  $\mathbb{F}_3[x]/\langle x^2 + 1 \rangle = \mathbb{F}_3[i]$ , the analogue over  $\mathbb{F}_3$  of the complex numbers.  $\mathbb{F}_3[i]$  is a field with nine elements, including eight units, but  $i$  is not a primitive root of  $\mathbb{F}_3[i]$  because  $i^4 = 1$ . There are four primitive roots of  $\mathbb{F}_3[i]$ , namely  $i + 1, 2i + 1, i + 2$  and  $2i + 2$ , but none is a root of the polynomial  $x^2 + 1$ .

*Example 18.27* Consider  $\mathbb{F}_3[x]/\langle x^2 + x + 2 \rangle = \mathbb{F}_3[\beta]$  where  $\beta = x + \langle x^2 + x + 2 \rangle$ . Then  $\mathbb{F}_3[\beta]$  is a field of degree 9. One can check that  $\beta$  is a primitive root of  $\mathbb{F}_3[\beta]$ .

It turns out that  $\mathbb{F}_3[\beta]$  and  $\mathbb{F}_3[i]$  are isomorphic fields.

To see this, observe that in  $\mathbb{F}_3[i]$ ,

$$(i+1)^2 = i^2 + 2i + 1 = 2i = 2(i+1) + 1.$$

So  $i+1$  is a root of the polynomial  $x^2 + x + 2$ . So we can define a function  $\psi_{i+1}$ , the “evaluate at  $i+1$  homomorphism” from  $\mathbb{F}_3[x]$  to  $\mathbb{F}_3[i]$  by

$$\psi_{i+1}(f(x)) = f(i+1).$$

The kernel of  $\psi_{i+1}$  is the ideal  $J = \langle x^2 + x + 2 \rangle$ . So by the Fundamental Homomorphism Theorem (Section 12.4),  $\psi_{i+1}$  induces a one-to-one homomorphism

$$\overline{\psi}_{i+1} : \mathbb{F}_3[\beta] \rightarrow \mathbb{F}_3[i]$$

which is an isomorphism of rings since both domain and codomain have 9 elements. This isomorphism illustrates part (iii) of the last proposition.

Since every finite field has a primitive root, the last example also illustrates the next fact:

**Proposition 18.28** *For every prime  $p$  and every  $n > 0$ , there is an irreducible polynomial  $m(x)$  in  $\mathbb{F}_p[x]$  of degree  $n$  so that every root of  $m(x)$  in  $\mathbb{F}_p[x]/\langle m(x) \rangle$  is a primitive root (that is, has order  $p^n - 1$  in the group of units of  $\mathbb{F}_p[x]/\langle m(x) \rangle$ ).*

The proof of this proposition involves a simple generalization of the last example.

**Definition** A primitive polynomial in  $\mathbb{F}_p[x]$  is an irreducible polynomial  $m(x)$  of degree  $n$  so that if  $\alpha$  is a root of  $m(x)$  and  $\mathbb{F}_p[\alpha] \cong \mathbb{F}_p[x]/\langle m(x) \rangle$ , a field with  $p^n$  elements, then  $\alpha$  itself is a primitive root of  $\mathbb{F}_p[\alpha]$ .

Not every irreducible polynomial in  $\mathbb{F}_p[x]$  is primitive, as we've seen.

In working with finite fields, it is often convenient when the irreducible polynomial that defines the field has a root  $\alpha$  that is a primitive root of the field. For example, for a field of 16 elements, the polynomials  $x^4 + x + 1$  and  $x^4 + x^3 + 1$  are primitive, but as we saw, the irreducible polynomial  $x^4 + x^3 + x^2 + x + 1$  is not primitive, because it divides  $x^5 - 1$ .

A primitive polynomial of degree 8 over  $\mathbb{F}_2$  is  $x^8 + x^4 + x^3 + x^2 + 1$ .

In the table of fields with under 100 elements in the last section, all of the polynomials  $m(x)$  in the third column are primitive polynomials.

For a comprehensive list of primitive polynomials, see [HM92].

**AES.** One important use of a finite field other than  $\mathbb{F}_p$  is in a very widely used private key, symmetric cryptosystem known as the Advanced Encryption Standard. This system was adopted by the U.S. government in 2002, the winner of a five-year world-wide competition to replace the previous U. S. government standard, known as DES (Digital Encryption Standard), which was viewed as insecure. The winner was called Rijndael, created by two Belgian cryptographers, J. Daemen and V. Rijmen. An essential part of its architecture involves computations in  $\mathbb{F}_{256}$ .

Rijndael takes an eight-bit word  $(b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0)$ , called a *byte*, and views it as

$$b_7\alpha^7 + b_6\alpha^6 + b_5\alpha^5 + b_4\alpha^4 + b_3\alpha^3 + b_2\alpha^2 + b_1\alpha + b_0,$$

an element of the field  $\mathbf{F} = \mathbb{F}_{256} = \mathbb{F}_2[\alpha] = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$ . (Elements of  $\mathbb{F}_{256}$  are also written as two digit base 16 (or hexadecimal) numbers.) A plaintext word consisting of 16 elements of  $\mathbf{F}$  is placed in a  $4 \times 4$  matrix, called a state array, and then transformed via a process which involves the cipher key, which has 128, 192 or 256 bits (or 16, 24 or 32 elements of  $\mathbf{F}$ ). Encryption involves a sequence of 10, 12 or 14 rounds, depending on the length of the key. Each round involves a sequence of three or four transformations of the state array, consisting of

- a substitution of the entries of the state array by replacing individual entries according to a fixed non-linear function;
- a cyclic shift within each row of the state array;
- multiplication of the state array by a fixed  $4 \times 4$  matrix with entries in  $\mathbf{F}$ ;
- addition of a four-tuple of elements of  $\mathbf{F}$  derived from the key to each column.

The decryption process reverses the rounds and the steps within each round.

Readers interested in the details of AES can find at least one book and numerous online sources that discuss the cryptosystem in depth. One example is [AES01].

## Exercises

- 18.1. Let  $\mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$ . Find the greatest common divisor and Bezout's identity for  $f(x) = x^4 + x^2 + 1$  and  $x^5 + x^4 + 1$ .
- 18.2. In  $\mathbb{F}_2[x]$ , find all polynomials of degree 3 that are coprime to  $x + 1$ . (Recall the Root Theorem.)
- 18.3. Find the greatest common divisor in  $\mathbb{Q}[x]$  of  $x^5 + x^4 + 2x^3 + 4x^2 + 4x + 8$  and  $x^4 + 4x^3 + 8x^2 + 7x + 2$ .
- 18.4. Prove Proposition 18.4.
- 18.5. Prove Theorem 18.10.
- 18.6. Prove Theorem 18.14.
- 18.7. Find an algebraic condition on  $b$  and  $c$  that is equivalent to the polynomial  $x^2 - bx + c$  being irreducible in  $\mathbb{R}[x]$  ( $\mathbb{R}$  is the field of real numbers.)
- 18.8. Let  $K = \mathbb{Q}[x]/\langle x^2 + 23 \rangle$ , where  $\langle x^2 + 23 \rangle$  is the principal ideal of  $\mathbb{Q}[x]$  consisting of all multiples of the irreducible polynomial  $x^2 + 23$  in  $\mathbb{Q}[x]$ . Let  $\alpha$  be the coset  $x + \langle x^2 + 23 \rangle$ . Show that every element of  $K$  is uniquely in the form  $a + b\alpha$  for  $a, b$  in  $\mathbb{Q}$ . We usually call  $\alpha = \sqrt{-23}$ , because

$$\alpha^2 \equiv -23 \pmod{\langle x^2 + 23 \rangle}.$$

$$\text{So } K = \mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{-23}].$$

- 18.9. Let  $F$  be a finite field. Prove that for every  $n > 0$  there is a polynomial  $p(x)$  in  $F[x]$  of degree  $> n$  that is irreducible in  $F[x]$ . (Hint: why are there infinitely many prime numbers?)
- 18.10. Find the monic polynomial  $d(x)$  in  $\mathbb{F}_2[x]$  so that the ideal  $\langle x^4 + x^3 + x + 1, x^5 + x^4 + 1 \rangle = \langle d(x) \rangle$ .
- 18.11. For a real number  $a$ , let  $\psi_a : \mathbb{Q}[x] \rightarrow \mathbb{R}$  be the function defined by

$$\psi_a(f(x)) = f(a)$$

for  $f(x)$  in  $\mathbb{Q}[x]$ :  $\psi_a$  is the “evaluation at  $a$ ” map.

- (i) Show that  $\psi_a(f(x) + g(x)) = \psi_a(f(x)) + \psi_a(g(x))$  and  $\psi_a(f(x)g(x)) = \psi_a(f(x))\psi_a(g(x))$ , so that  $\psi_a$  is a ring homomorphism (Chapter 12).
- (ii) Let

$$J = \{f(x) \text{ in } \mathbb{Q}[x] : \psi_a(f(x)) = 0\}.$$

Show that  $J$  is an ideal of  $\mathbb{Q}[x]$ . ( $J$  is the kernel of  $\psi_a$ .)

- (iii) Let  $a = \sqrt{2}$ . Find a monic polynomial  $m(x)$  in  $\mathbb{Q}[x]$  so that  $J = \langle m(x) \rangle$ .

- 18.12. Find the monic polynomial  $m(x)$  of smallest degree in  $\mathbb{R}[x]$  so that  $m(\frac{1+i\sqrt{3}}{2}) = 0$ . (Note that  $(\frac{1+i\sqrt{3}}{2})^6 = 1$ .)
- 18.13. Show that  $x^2 + x + 1$  is the only irreducible polynomial of degree 2 in  $\mathbb{F}_2[x]$ .
- 18.14. Let  $F = \mathbb{F}_2[x]/(x^4 + x + 1)$ . Show that  $F$  is a field by showing that  $x^4 + x + 1$  is irreducible in  $\mathbb{F}_2[x]$ , as follows:
- (i) Show that  $x^4 + x + 1$  has no roots in  $\mathbb{F}_2$ .
  - (ii) Show that  $x^2 + x + 1$  does not divide  $x^4 + x + 1$ .
  - (iii) With no computations, explain why no polynomial of degree 3 divides  $x^4 + x + 1$ .
- 18.15. Let  $m(x) = x^4 + x + 1$  and let  $\alpha = x + \langle m(x) \rangle$ .
- (i) Show that  $\alpha$  has order 15 in the group of units of  $\mathbb{F}_2[\alpha]$ , and so  $\alpha$  is a primitive root of  $\mathbb{F}_2[\alpha]$ .
  - (ii) For  $k = 1, \dots, 15$ , write  $\alpha^k$  as a polynomial in  $\alpha$  of degree  $\leq 3$ , similar to Example 18.22.
- 18.16. Show that a polynomial  $m(x)$  of degree 5 in  $F[x]$ ,  $F$  a field, is irreducible in  $F[x]$  if and only if  $m(x)$  has no roots in  $F$  and is not divisible by a polynomial in  $F[x]$  of degree 2.
- 18.17. Let  $\omega = \frac{-1+i\sqrt{3}}{2}$  in  $\mathbb{C}$ . Then  $\omega^3 = 1$ .
- (i) Show that  $\mathbb{R}[\omega] \subset \mathbb{C}$  is a field.
  - (ii) Show that  $\mathbb{R}[x]/\langle x^3 - 1 \rangle$  is not a field, so we can't identify  $\mathbb{R}[x]/(x^3 - 1)$  as  $\mathbb{R}[\omega]$ . What's going on?
- 18.18. Why does every finite field have a primitive root?
- 18.19. Show that  $x^4 + x^3 + x^2 + x + 1$  in  $\mathbb{F}_2[x]$  is irreducible.
- 18.20. Show that if  $F$  is a field with 32 elements, then every element of  $F$  except 0 and 1 is a primitive root of  $F$ .
- 18.21. Find a condition on  $n > 2$  so that there is a field  $F$  with  $n$  elements in which every element except 0 and 1 is a primitive root of  $F$ .
- 18.22. (i) Show that  $m(x) = x^3 + 2x + 1$  is an irreducible and primitive polynomial in  $\mathbb{F}_3[x]$   
(ii) Let  $F = \mathbb{F}_3[x]/\langle m(x) \rangle$  where  $m(x) = x^3 + 2x + 1$ . Describe a multiplicative Caesar cipher using the field  $F$ .
- 18.23. Use Euler's Lemma (Lemma 16.15) to characterize the odd primes  $p$  for which the commutative ring  $\mathbb{F}_p[x]/(x^2 + 1)$  is a field.
- 18.24. Let  $F = \mathbb{F}_p[x]/\langle m(x) \rangle$  be a field with  $p^n$  elements.
- (i) Explain why  $m(x)$  must have degree  $n$  and be irreducible.
  - (ii) Show that every element of  $F$  is a root of the polynomial  $x^{p^n} - x$ .
  - (iii) Show that  $m(x)$  divides  $x^{p^n} - x$  in  $\mathbb{F}_p[x]$ .
  - (iv) Show that every irreducible polynomial of degree  $n$  in  $\mathbb{F}_p[x]$  divides the polynomial  $x^{p^n} - x$ .

- 18.25. It turns out that in the field  $\mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1) = \mathbb{F}_2[\alpha]$  where  $\alpha = x + (x^8 + x^4 + x^3 + x + 1)$ , the element  $\alpha$  is not a primitive root.
- (i) What are the possible orders of  $\alpha$ ?
  - (ii) Find the order of  $\alpha$ .
  - (iii) How many primitive roots are there in  $\mathbb{F}_2[\alpha]$ ?
  - (iv) Show that  $\alpha + 1$  is a primitive root of  $\mathbb{F}_2[\alpha]$ .

# Chapter 19

## Reed-Solomon Codes II



In Chapter 15 we introduced Reed-Solomon error-correcting codes. We gave examples of Reed-Solomon codes using the fields  $\mathbb{F}_p$  for various primes  $p$ . This chapter presents examples of Reed-Solomon codes over finite fields other than  $\mathbb{F}_p$ , and also introduces the discrete Fourier transform, whose use reduces the amount of computation needed for decoding.

### 19.1 Roots of Unity and the Discrete Fourier Transform

The set of all units in a field  $\mathbb{F}$  is denoted  $U_{\mathbb{F}}$ , a group under multiplication. An  $n$ -th root of unity in a field  $\mathbb{F}$  is a root  $\zeta$  of the polynomial  $x^n - 1$ . The set of all  $n$ -th roots of unity in  $\mathbb{F}$  is the subgroup  $U_{\mathbb{F}}(n)$  of  $U_{\mathbb{F}}$ .

**Definition** An element  $\zeta$  of  $U_{\mathbb{F}}$  is called a primitive  $n$ -th root of unity in  $\mathbb{F}$  if  $\zeta$  has order  $n$  in  $U_{\mathbb{F}}$ .

Examples: In  $U_7$ , 3 and 5 are primitive 6-th roots of unity, while 2 and 4 are primitive 3rd roots of unity, and 6 is a primitive 2nd root of unity.

Suppose  $\mathbb{F}$  is a field and  $\zeta$  is a primitive  $n$ -th root of unity in  $\mathbb{F}$ . By D'Alembert's Theorem (Chapter 6) there are at most  $n$   $n$ -th roots of unity in  $\mathbb{F}$ . So  $U_{\mathbb{F}}(n)$ , the group of  $n$ -th roots of unity in  $\mathbb{F}$ , consist of  $\zeta, \zeta^2, \zeta^3, \dots, \zeta^{n-1}$  and  $\zeta^n = 1$ . They are the roots of the polynomial  $x^n - 1$  in  $\mathbb{F}[x]$ .

Now  $x^n - 1$  factors as

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + x^2 + x + 1).$$

Since the only root of  $x - 1$  is 1, all of the other  $n$ -th roots of unity,  $\zeta, \zeta^2, \dots, \zeta^{n-1}$ , must be roots of

$$x^{n-1} + x^{n-2} + \dots + x^2 + x + 1.$$

So we have

**Proposition 19.1** *Let  $\mathbb{F}$  be a field. If  $\zeta$  in  $\mathbb{F}$  is a non-trivial  $n$ -th root of unity (“non-trivial” means “not = 1”), then*

$$1 + \zeta + \zeta^2 + \dots + \zeta^{n-1} = 0.$$

*Example 19.2* In  $\mathbb{Z}_7$ , 3 and 4 are sixth roots of unity, and

$$1 + 3 + 3^2 + 3^3 + 3^4 + 3^5 \equiv 1 + 3 + 2 + 6 + 4 + 5 = 21 \equiv 0 \pmod{7}.$$

$$1 + 4 + 4^2 + 4^3 + 4^4 + 4^5 \equiv 1 + 4 + 2 + 1 + 4 + 2 = 14 \equiv 0 \pmod{7}.$$

Let  $\mathbb{F}$  be a field and let  $\zeta$  be a primitive  $n$ -th root of unity in  $\mathbb{F}$ . Consider the  $n \times n$  matrix

$$\mathbf{F} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \zeta & \zeta^2 & \dots & \zeta^{n-2} & \zeta^{n-1} \\ 1 & \zeta^2 & \zeta^4 & \dots & \zeta^{(n-2)2} & \zeta^{(n-1)2} \\ \vdots & & & & & \vdots \\ 1 & \zeta^{n-2} & \zeta^{2(n-2)} & \dots & \zeta^{(n-2)(n-2)} & \zeta^{(n-1)(n-2)} \\ 1 & \zeta^{n-1} & \zeta^{2(n-1)} & \dots & \zeta^{(n-2)(n-1)} & \zeta^{(n-1)(n-1)} \end{pmatrix}.$$

The matrix  $\mathbf{F}$  is an example of a Vandermonde matrix. These matrices showed up in Section 15.2, where it was noted that every Vandermonde matrix is an invertible matrix. Here, because of Proposition 19.1, the matrix  $\mathbf{F}$  turns out to have an inverse that is easy to write down. Let  $\hat{\mathbf{F}}$  be the matrix  $\mathbf{F}$  with  $\zeta$  replaced by  $\zeta^{n-1} = \zeta^{-1}$ :

$$\hat{\mathbf{F}} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \zeta^{-1} & \zeta^{-2} & \dots & \zeta^{-(n-2)} & \zeta^{-(n-1)} \\ 1 & \zeta^{-2} & \zeta^{-4} & \dots & \zeta^{-(n-2)2} & \zeta^{-(n-1)2} \\ \vdots & & & & & \vdots \\ 1 & \zeta^{-(n-2)} & \zeta^{-2(n-2)} & \dots & \zeta^{-(n-2)(n-2)} & \zeta^{-(n-1)(n-2)} \\ 1 & \zeta^{-(n-1)} & \zeta^{-2(n-1)} & \dots & \zeta^{-(n-2)(n-1)} & \zeta^{-(n-1)(n-1)} \end{pmatrix}.$$

**Proposition 19.3**  $\hat{\mathbf{F}}\mathbf{F} = n\mathbf{I}$ , where  $\mathbf{I}$  is the identity matrix.

*Proof* It is enough to show that the  $j$ th row of  $\hat{\mathbf{F}}$  times the  $k$ th column of  $\mathbf{F}$  is 0 if  $j \neq k$ , and is  $n$  if  $j = k$ . Now,

$$\begin{aligned} (1 & \quad \zeta^{-j} & \zeta^{-2j} & \dots & \zeta^{-(n-2)j} & \zeta^{-(n-1)j}) \begin{pmatrix} 1 \\ \zeta^k \\ \zeta^{2k} \\ \vdots \\ \zeta^{(n-2)k} \\ \zeta^{(n-1)k} \end{pmatrix} \\ &= 1 \cdot 1 + \zeta^{-j}\zeta^k + \zeta^{-2j}\zeta^{2k} + \dots + \zeta^{-(n-2)j}\zeta^{(n-2)k} + \zeta^{-(n-1)j}\zeta^{(n-1)k} \\ &= 1 + \zeta^{k-j} + \zeta^{2(k-j)} + \dots + \zeta^{(n-2)(k-j)} + \zeta^{(n-1)(k-j)}. \end{aligned}$$

If  $k = j$ , then this sum is

$$= 1 + 1 + \dots + 1 + 1 = n.$$

If  $k \neq j$ , then let  $k - j = e$ , then  $\zeta^{k-j} = \zeta^e$  is a non-trivial  $n$ th root of unity, and the sum is

$$= 1 + \zeta^e + (\zeta^e)^2 + \dots + (\zeta^e)^{n-2} + (\zeta^e)^{n-1}.$$

For  $e \neq 0$ , this sum = 0 by Proposition 19.1. □

*Example 19.4* In  $\mathbb{F}_{11}$ , 4 is a 5th root of unity:

$$(4, 4^2, 4^3, 4^4, 4^5) \equiv (4, 5, 9, 3, 1) \pmod{11}.$$

Then the matrix  $\mathbf{F}$  corresponding to 4 is

$$\mathbf{F} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 5 & 9 & 3 \\ 1 & 5 & 3 & 4 & 9 \\ 1 & 9 & 4 & 3 & 5 \\ 1 & 3 & 9 & 5 & 4 \end{pmatrix}.$$

Since  $4^{-1} = 3$  in  $\mathbb{F}_{11}$ ,

$$\hat{\mathbf{F}} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 9 & 5 & 4 \\ 1 & 9 & 4 & 3 & 5 \\ 1 & 5 & 3 & 4 & 9 \\ 1 & 4 & 5 & 9 & 3 \end{pmatrix}.$$

It is routine to check that  $\hat{\mathbf{F}}\mathbf{F} = 5\mathbf{I}$ .

The matrix  $\mathbf{F}$  is called a *discrete Fourier transform*. The matrix  $\hat{\mathbf{F}}$  is the *inverse Fourier transform*.

## 19.2 A Field with 8 Elements

Our first Reed-Solomon example will use a field with 8 elements. We can obtain such a field by finding an irreducible polynomial of degree 3 in  $\mathbb{F}_2[x]$  where  $\mathbb{F}_2$  is the field of two elements, which we denote by 0 and 1. Since  $2 = 0$  in  $\mathbb{F}_2$ ,  $-1 = 1$ , and subtraction is the same as addition.

There are two irreducible polynomials of degree 3 in  $\mathbb{F}_2[x]$ ,  $x^3 + x + 1$  and  $x^3 + x^2 + 1$ . We'll choose  $m(x) = x^3 + x + 1$ . Then our field  $\mathbb{F}_8$  of eight elements is  $\mathbb{F}_2[\alpha]$  where  $\alpha$  is a root of  $x^3 + x + 1$ . Thus  $\alpha^3 + \alpha + 1 = 0$ , and so  $\alpha^3 = \alpha + 1$  (subtraction is the same as addition).

The elements of  $\mathbb{F}_8$  are polynomials in  $\alpha$  of degree  $\leq 2$ :

$$0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1.$$

The group of units of  $\mathbb{F}_8$  has order 7, a prime, so every unit other than 1 is a primitive root of  $\mathbb{F}_8$ . In particular,  $\alpha$  is a primitive 7th root of unity in  $\mathbb{F}_8$ , and every non-zero element of  $\mathbb{F}_2[\alpha]$  is a power of  $\alpha$ . Here is a “log table” for  $\mathbb{F}_2[\alpha]$ :

$$\begin{aligned} \alpha &= \alpha \\ \alpha^2 &= \alpha^2 \\ \alpha^3 &= \alpha + 1 \\ \alpha^4 &= \alpha^2 + \alpha \\ \alpha^5 &= \alpha^2 + \alpha + 1 \\ \alpha^6 &= \alpha^2 + 1 \\ \alpha^7 &= 1. \end{aligned}$$

A convenient fact about addition in  $\mathbb{F}_2[\alpha]$  is that for every exponent  $e$ ,  $\alpha^e + \alpha^{e+1} + \alpha^{e+3} = 0$ . Using this equation and the fact that addition and subtraction are the same modulo 2 allows us to add powers easily in  $\mathbb{F}_2[\alpha]$ . For example,

$$\begin{aligned}
\alpha^4 + \alpha &= \alpha^2 \\
\alpha^4 + \alpha^2 &= \alpha^1 \\
\alpha^4 + \alpha^3 &= \alpha^6 \\
\alpha^4 + \alpha^4 &= 0 \\
\alpha^4 + \alpha^5 &= \alpha^7 = 1 \\
\alpha^4 + \alpha^6 &= \alpha^3 \\
\alpha^4 + 1 &= \alpha^4 + \alpha^7 = \alpha^5
\end{aligned}$$

etc. (This situation is special to the field of 8 elements. It is not true for other finite fields!)

### 19.3 A Reed-Solomon Code Using $\mathbb{F}_8$

The notation  $RS(n, m)$  denotes a Reed-Solomon code defined over a field  $\mathbb{F}$  that starts with a plaintext word  $W$  consisting of  $m$  elements of  $\mathbb{F}$ , and generates a coded word  $C$  consisting of  $n$  elements of  $\mathbb{F}$ , where  $m + 2e = n$ . The code corrects up to  $e$  errors. The example we give here illustrates a case where the field  $\mathbb{F}$  being used has  $n + 1$  elements. Thus  $\mathbb{F}$  has the zero element 0, and every other element is a power of some primitive root  $\alpha$ . The encoding will evaluate the polynomial  $W(x)$  at all of the powers of the primitive root. As we'll see, that will enable a preprocessing of the  $n \times (n + 1)$  matrix of coefficients of the equations we need to solve in order to decode. So we will only need to do row operations on the last  $e$  columns of the resulting matrix.

*Example 19.5* Our Reed-Solomon code will take plaintext messages consisting of three elements of  $\mathbb{F}_2[\alpha]$  and correct two errors.

Alice's plaintext messages will be triples  $(n_0, n_1, n_2)$  of numbers  $0 \leq n_i < 7$ . To use  $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ , we translate the numbers into the corresponding powers of  $\alpha$  and write Alice's plaintext message as a polynomial

$$W(x) = \alpha^{n_0} + \alpha^{n_1}x + \alpha^{n_2}x^2.$$

The encoded vector  $C$  will be a seven-tuple that we get by evaluating  $W(x)$  at all seven powers of  $\alpha$ :

$$C = (W(1), W(\alpha), W(\alpha^2), W(\alpha^3), W(\alpha^4), W(\alpha^5), W(\alpha^6))^T.$$

The received vector

$$R = (r_0, r_1, r_2, r_3, r_4, r_5, r_6)^T$$

is assumed to differ from  $C$  in at most two components. (Here, as elsewhere,  $(\ )^T$  means transpose: a (row vector) $^T$  is the corresponding column vector.)

To decode  $R$  to find the plaintext message  $W(x)$ , we assume the error polynomial has degree 2,

$$E(x) = (x - \alpha^e)(x - \alpha^f).$$

So, as in Chapter 15 we seek a polynomial

$$E^*(x) = s_0 + s_1x + s_2x^2$$

and a polynomial

$$G^*(x) = t_0 + t_1x + t_2x^2 + t_3x^3 + t_4x^4$$

so that  $G^*(x) = W(x)E^*(x)$ . So the coefficients  $s_0, s_1, s_2, t_0, t_1, t_2, t_3, t_4$  are unknown. All we know about  $E^*(x)$  and  $G^*(x)$  is that

$$G^*(\alpha^i) = r_i E^*(\alpha^i)$$

for  $i = 0, 1, \dots, 6$ . And this is enough information to recover  $W(x) = G^*(x)/E^*(x)$ , provided that  $r_i = W(\alpha^i)$  for at least five different  $i$ .

Suppose Alice wants to send  $W = (3, 1, 5)$ . She writes down the polynomial

$$W(x) = \alpha^3 + \alpha x + \alpha^5 x^2.$$

She computes  $C = (W(1), W(\alpha), \dots, W(\alpha^6))^T$ :

$$\begin{aligned} W(1) &= \alpha^3 + \alpha + \alpha^5 \\ W(\alpha) &= \alpha^3 + \alpha \cdot \alpha + \alpha^5 \cdot \alpha^2 &= \alpha^3 + \alpha^2 + \alpha^7 \\ W(\alpha^2) &= \alpha^3 + \alpha \cdot \alpha^2 + \alpha^5 \cdot \alpha^4 &= \alpha^3 + \alpha^3 + \alpha^9 \\ W(\alpha^3) &= \alpha^3 + \alpha \cdot \alpha^3 + \alpha^5 \cdot \alpha^6 &= \alpha^3 + \alpha^4 + \alpha^{11} \\ W(\alpha^4) &= \alpha^3 + \alpha \cdot \alpha^4 + \alpha^5 \cdot \alpha^8 &= \alpha^3 + \alpha^5 + \alpha^{13} \\ W(\alpha^5) &= \alpha^3 + \alpha \cdot \alpha^5 + \alpha^5 \cdot \alpha^{10} &= \alpha^3 + \alpha^6 + \alpha^{15} \\ W(\alpha^6) &= \alpha^3 + \alpha \cdot \alpha^6 + \alpha^5 \cdot \alpha^{12} &= \alpha^3 + \alpha^7 + \alpha^{17} \end{aligned}$$

Using that  $\alpha^7 = 1$  and the observations about the sum of two powers of  $\alpha$  described just before the beginning of this section, she gets

$$\begin{aligned} C &= (W(1), W(\alpha), W(\alpha^2), W(\alpha^3), W(\alpha^4), W(\alpha^5), W(\alpha^6))^T \\ &= (\alpha^4, \alpha^4, \alpha^2, \alpha^3, 1, \alpha^2, 1)^T. \end{aligned}$$

Alice sends  $C$  to Bob.

Let us suppose that

$$R = (r_0, r_1, \dots, r_6)^T = (\alpha^4, \alpha^6, \alpha^2, \alpha^3, \alpha^4, \alpha^2, 1)^T.$$

Then there are two errors, in the  $\alpha$  component and the  $\alpha^4$  component. (We know that, but Bob doesn't.)

To decode, Bob sets up the seven linear equations  $G^*(\alpha^i) = r_i E^*(\alpha^i)$ , or, what is the same,

$$G^*(\alpha^i) + r_i E^*(\alpha^i) = 0$$

for  $i = 0, 1, \dots, 6$ , where  $G^*(x) = t_0 + t_1 x + t_2 x^2 + t_3 x^3 + t_4 x^4$  and  $E^*(x) = s_0 + s_1 x + s_2$ . He wants to solve for the column vector of unknown coefficients  $X = (t_0, t_1, t_2, t_3, t_4, s_0, s_1, s_2)^T$ . The equation  $G^*(\alpha^i) + r_i E^*(\alpha^i) = 0$  is

$$t_0 + \alpha^i t_1 + \alpha^{2i} t_2 + \alpha^{3i} t_3 + \alpha^{4i} t_4 + r_i s_0 + r_i \alpha^i s_1 + r_i \alpha^{2i} s_2 = 0.$$

If we write these down for  $i = 0, \dots, 6$  we get seven homogeneous equations in eight unknowns. In matrix form this becomes  $\mathbf{M}X = \mathbf{0}$  where  $\mathbf{M}$  is the  $7 \times 8$  matrix

$$\mathbf{M} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \alpha^4 & \alpha^4 & \alpha^4 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^6 & 1 & \alpha \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^3 & \alpha^6 & \alpha^2 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^4 & \alpha & \alpha^5 \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^2 & 1 & \alpha^5 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & 1 & \alpha^6 & \alpha^5 \end{pmatrix}.$$

As we did in Chapter 15, to solve the equation  $\mathbf{M}X = 0$ , we want to reduce the coefficient matrix  $\mathbf{M}$  to reduced row echelon form.

Notice that the first five columns of the matrix  $\mathbf{M}$  coincide with the first five columns of the matrix  $\mathbf{F}$  that we called the discrete Fourier transform, because  $\alpha$  is a primitive 7th root of unity in  $\mathbb{F}_2[\alpha]$ .

We know that if  $\hat{\mathbf{F}}$  is the inverse Fourier transform, then  $\hat{\mathbf{F}}\mathbf{F} = 7\mathbf{I} = \mathbf{I}$ . So if we multiply the first five columns of  $\mathbf{M}$  by  $\hat{\mathbf{F}}$ , we get a  $7 \times 5$  matrix  $\mathbf{I}_{7,5}$  which is the matrix of the first five columns of the  $7 \times 7$  identity matrix. So write

$$\mathbf{M} = [\mathbf{F}_1, \mathbf{G}]$$

where  $\mathbf{F}_1$  is the  $7 \times 5$  matrix consisting of the first five columns of  $\mathbf{M}$ ,  $=$  the first five columns of the discrete Fourier transform matrix  $\mathbf{F}$ , and  $\mathbf{G}$  is a  $7 \times 3$  matrix consisting of the last three columns of  $\mathbf{M}$ . Then

$$\hat{\mathbf{F}}\mathbf{M} = [\hat{\mathbf{F}}\mathbf{F}_1, \hat{\mathbf{F}}\mathbf{G}] = [\mathbf{I}_{7,5}, \hat{\mathbf{F}}\mathbf{G}].$$

So multiplying the equation

$$\mathbf{M}X = 0$$

by  $\hat{\mathbf{F}}$  yields a matrix of coefficients that is already mostly in reduced row echelon form. We're left with cleaning up the matrix  $\hat{\mathbf{F}}\mathbf{G}$ . We find that

$$\hat{\mathbf{F}}\mathbf{G} = \begin{pmatrix} \alpha^5 & \alpha & \alpha \\ \alpha^2 & \alpha^5 & \alpha \\ \alpha^3 & \alpha^2 & \alpha^5 \\ 0 & \alpha^3 & \alpha^2 \\ \alpha^4 & 0 & \alpha^3 \\ \alpha & \alpha^4 & 0 \\ \alpha & \alpha & \alpha^4 \end{pmatrix}.$$

To get our matrix  $\mathbf{M}$  into reduced row echelon form, we want to get  $\hat{\mathbf{F}}\mathbf{G}$  into the form

$$\begin{pmatrix} 0 & 0 & * \\ 0 & 0 & * \\ 0 & 0 & * \\ 0 & 0 & * \\ 0 & 0 & * \\ 1 & 0 & * \\ 0 & 1 & * \end{pmatrix}$$

by row operations. So starting from  $\hat{\mathbf{F}}\mathbf{G}$ , we add the sixth row to the seventh row, then divide the sixth row by  $\alpha$ , and the seventh row by  $\alpha^2$ , then add  $\alpha^3$  times the seventh row to the sixth row to get

$$\begin{pmatrix} \alpha^5 & \alpha & \alpha \\ \alpha^2 & \alpha^5 & \alpha \\ \alpha^3 & \alpha^2 & \alpha^5 \\ 0 & \alpha^3 & \alpha^2 \\ \alpha^4 & 0 & \alpha^3 \\ 1 & 0 & \alpha^5 \\ 0 & 1 & \alpha^2 \end{pmatrix}.$$

Then do row operations to turn every element in the last two columns and the first five rows equal to zero. Doing so, the original matrix  $\mathbf{M}$  becomes the matrix

$$(\mathbf{I}, \mathbf{S}),$$

where  $\mathbf{I}$  is the  $7 \times 7$  identity matrix and  $\mathbf{S}$  is the column vector

$$\mathbf{S} = (\alpha, \alpha, \alpha^3, \alpha^3, \alpha^5 \alpha^5, \alpha^2)^T.$$

Setting  $s_2 = 1$ , we get the solution:

$$(t_0, t_1, t_2, t_3, t_4, s_0, s_1, s_2) = (\alpha, \alpha, \alpha^3, \alpha^3, \alpha^5, \alpha^5, \alpha^2, 1).$$

So

$$G(x) = \alpha + \alpha x + \alpha^3 x^2 + \alpha^3 x^3 + \alpha^5 x^4,$$

$$E(x) = \alpha^5 + \alpha^2 x + x^2 = (x - \alpha^4)(x - \alpha),$$

and dividing  $G(x)$  by  $E(x)$  gives  $W(x) = \alpha^3 + \alpha x + \alpha^5 x^2$ , Alice's plaintext polynomial.

## 19.4 An Example Using $\mathbb{F}_{13}$

In this example, we'll construct a Reed-Solomon code which will take plaintext messages consisting of two elements of  $\mathbb{F}_{13}$  and correct two errors. We will encode by evaluating at powers of a primitive 6th root of unity in  $\mathbb{F}_{13}$ . Since the group of units of  $\mathbb{F}_{13}$  is cyclic of order 12, there are primitive 6th roots of unity in  $\mathbb{F}_{13}$ . One of them is  $\zeta = -3$ , whose powers are

$$\begin{aligned} -3, (-3)^2 &= 9 = -4, (-3)^3 = (-3)(-4) = -1, \\ (-3)^4 &= 3, (-3)^5 = 4, (-3)^6 = 1. \end{aligned}$$

(As usual, we'll think of  $\mathbb{F}_{13}$  as  $\mathbb{Z}_{13}$  and compute with integers, always modulo 13.)

*Example 19.6* Alice's plaintext messages will be pairs  $(w_0, w_1)$  of numbers  $0 \leq w_i \leq 12$ . We write Alice's plaintext message as a polynomial

$$W(x) = w_0 + w_1 x.$$

The encoded vector  $C$  will be the six-tuple obtained by evaluating  $W(x)$  at all six powers of  $\alpha = 7$ :

$$C = (W(1), W(-3), W(-4), W(-1), W(3), W(4)).$$

Suppose Alice's message polynomial is

$$W(x) = 7 + 5x$$

in  $\mathbb{F}_{13}[x]$ . Then

$$C = (W(1), W(-3), W(-4), W(-1), W(3), W(4)) = (12, 5, 0, 2, 9, 1)$$

in  $\mathbb{F}_{13}$ .

The received vector,

$$R = (r_0, r_1, r_2, r_3, r_4, r_5)$$

is assumed to differ from  $C$  in at most two components. So in order to find  $W(x)$ , Bob assumes the error polynomial has degree 2, and sets

$$E^*(x) = s_0 + s_1x + s_2x^2$$

where the coefficients  $s_0, s_1, s_2$  are unknown. As before,

$$G^*(x) = t_0 + t_1x + t_2x^2 + t_3x^3$$

where the coefficients of  $G^*(x)$  are also unknown, but

$$G^*(\zeta^i) = r_i E^*(\zeta^i)$$

for  $i = 0, 1, \dots, 6$ .

With  $C = (12, 5, 0, 2, 9, 1)$ , suppose

$$R = (12, 5, 8, 2, 2, 1),$$

so  $r_2 \neq W((-3)^2)$  and  $r_4 \neq W((-3)^4)$ . Of course, Bob doesn't know where the errors are.

To decode, Bob sets up the six equations  $G^*((-3)^i)$ , or, what is the same,

$$G^*((-3)^i) - r_i E^*((-3)^i) = 0$$

for  $i = 0, 1, \dots, 5$ , where  $G^*(x) = t_0 + t_1x + t_2x^2 + t_3x^3$  and  $E^*(x) = s_0 + s_1x + s_2x^2$ . He wants to solve for the column vector of unknown coefficients  $X = (t_0, t_1, t_2, t_3, s_0, s_1, s_2)^T$ . The equation  $G^*(\alpha^i) - r_i E^*(\alpha^i) = 0$  is

$$t_0 + (-3)^i t_1 + (-3)^{2i} t_2 + (-3)^{3i} t_3 - r_i s_0 - r_i (-3)^i s_1 - r_i (-3)^{2i} s_2.$$

If we write these down for  $i = 0, \dots, 5$ , we get six homogeneous equations in seven unknowns, which in matrix form looks like

$$\mathbf{M}X = 0,$$

where  $\mathbf{M}$  is the  $6 \times 7$  matrix with entries in  $\mathbb{F}_{13}$ :

$$\begin{aligned} \mathbf{M} &= \begin{pmatrix} 1 & 1 & 1 & 1 & -r_0 & -r_0 & -r_0 \\ 1 & -3 & -4 & -1 & -r_1 & 3r_1 & 4r_1 \\ 1 & -4 & 3 & 1 & -r_2 & 4r_2 & -3r_2 \\ 1 & -1 & 1 & -1 & -r_3 & r_3 & -r_3 \\ 1 & 3 & -4 & 1 & -r_4 & -3r_4 & 4r_4 \\ 1 & 4 & 3 & -1 & -r_5 & -4r_5 & -3r_5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -3 & -4 & -1 & -5 & 2 & 7 \\ 1 & -4 & 3 & 1 & 5 & 6 & 2 \\ 1 & -1 & 1 & -1 & -2 & 2 & -2 \\ 1 & 3 & -4 & 1 & -2 & -7 & 8 \\ 1 & 4 & 3 & -1 & -1 & -4 & -3 \end{pmatrix}. \end{aligned}$$

To reduce the coefficient matrix  $\mathbf{M}$  to reduced row echelon form, we begin by multiplying  $\mathbf{M}$  on the left by the inverse

$$\mathbf{F}^{-1} = \begin{pmatrix} -2 & -2 & -2 & -2 & -2 & -2 \\ -2 & 5 & -6 & 2 & -5 & 6 \\ -2 & -6 & -5 & -2 & -6 & -5 \\ -2 & 2 & -2 & 2 & -2 & 2 \\ -2 & -5 & -6 & -2 & -5 & -6 \\ -2 & 6 & -5 & 2 & -6 & 5 \end{pmatrix}$$

of the discrete Fourier transform matrix

$$\mathbf{F} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -3 & -4 & -1 & 3 & 4 \\ 1 & -4 & 3 & 1 & -4 & 3 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 3 & -4 & 1 & 3 & -4 \\ 1 & 4 & 3 & -1 & -4 & -3 \end{pmatrix},$$

to get

$$\mathbf{F}^{-1}\mathbf{M} = \begin{pmatrix} 1 & 0 & 0 & 0 & -5 & -2 & 0 \\ 0 & 1 & 0 & 0 & -5 & -5 & -2 \\ 0 & 0 & 1 & 0 & -2 & -5 & -5 \\ 0 & 0 & 0 & 1 & 2 & -2 & -5 \\ 0 & 0 & 0 & 0 & 0 & 2 & -2 \\ 0 & 0 & 0 & 0 & -2 & 0 & 2 \end{pmatrix}.$$

To reduce this to reduced echelon form, we only need to work with the last three columns. Doing so, we obtain

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & -7 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -5 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}.$$

We set  $s_2 = 1$  and get a solution

$$(t_0, t_1, t_2, t_3, s_0, s_1, s_2) = (7, -1, -1, 5, 11, 1)$$

which corresponds to

$$E^*(x) = x^2 + x + 1, \text{ and } G^*(x) = 5x^3 - x^2 - x + 7.$$

Dividing  $G(x)$  by  $E(x)$  gives

$$W(x) = 5x + 7,$$

Alice's original polynomial. Note that in this example,

$$E(x) = (x - (-4))(x - 3) = x^2 + x + 1 = E^*(x).$$

*Example 19.7* Now suppose the same situation as in the last example, except assume that  $R = C$ : there are no errors.

Suppose Alice's message polynomial is

$$W(x) = 7 + 5x$$

in  $\mathbb{F}_{13}[x]$ . Then

$$C = (W(1), W(-3), W(-4), W(-1), W(3), W(4)) = (12, 5, 0, 2, 9, 1)$$

in  $\mathbb{F}_{13}$ . Suppose  $R = C$ .

The received vector,

$$R = (r_0, r_1, r_2, r_3, r_4, r_5),$$

is assumed to differ from  $C$  in at most two components. So in order to find  $W(x)$ , Bob still assumes the error polynomial is

$$E^*(x) = s_0 + s_1x + s_2x^2$$

As before,

$$G^*(x) = t_0 + t_1x + t_2x^2 + t_3x^3 + t_4x^4$$

where the coefficients of  $G^*(x)$  are also unknown, but

$$G^*((-3)^i) = r_i E^*((-3)^i)$$

for  $i = 0, 1, \dots, 5$ .

With  $R = (12, 5, 0, 2, 9, 1)$ , Bob sets up the six equations

$$G^*((-3)^i) - r_i E^*((-3)^i) = 0$$

for  $i = 0, 1, \dots, 5$ , which in matrix form looks like

$$\mathbf{M}X = 0$$

where  $\mathbf{M}$  is the  $6 \times 7$  matrix with entries in  $\mathbb{F}_{13}$ :

$$\begin{aligned} \mathbf{M} &= \begin{pmatrix} 1 & 1 & 1 & 1 & -r_0 & -r_0 & -r_0 \\ 1 & -3 & -4 & -1 & -r_1 & 3r_1 & 4r_1 \\ 1 & -4 & 3 & 1 & -r_2 & 4r_2 & -3r_2 \\ 1 & -1 & 1 & -1 & -r_3 & r_3 & -r_3 \\ 1 & 3 & -4 & 1 & -r_4 & -3r_4 & 4r_4 \\ 1 & 4 & 3 & -1 & -r_5 & -4r_5 & -3r_5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -3 & -4 & -1 & -5 & 2 & 7 \\ 1 & -4 & 3 & 1 & 0 & 0 & 0 \\ 1 & -1 & 1 & -1 & -2 & 2 & -2 \\ 1 & 3 & -4 & 1 & 4 & -1 & -3 \\ 1 & 4 & 3 & -1 & -1 & -4 & -3 \end{pmatrix}. \end{aligned}$$

Multiplying  $\mathbf{M}$  on the left by the inverse

$$\mathbf{F}^{-1} = \begin{pmatrix} -2 & -2 & -2 & -2 & -2 & -2 \\ -2 & 5 & -6 & 2 & -5 & 6 \\ -2 & -6 & -5 & -2 & -6 & -5 \\ -2 & 2 & -2 & 2 & -2 & 2 \\ -2 & -5 & -6 & -2 & -5 & -6 \\ -2 & 6 & -5 & 2 & -6 & 5 \end{pmatrix}$$

of the discrete Fourier transform matrix, we get

$$\mathbf{F}^{-1}\mathbf{M} = \begin{pmatrix} 1 & 0 & 0 & 0 & 6 & 8 & 0 \\ 0 & 1 & 0 & 0 & -5 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 6 & 6 \\ 0 & 0 & 0 & 1 & 0 & 5 & -5 \\ 0 & 0 & 0 & 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \end{pmatrix}.$$

To reduce this to reduced echelon form, we only need to work with the last three columns. Doing so, we obtain

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 6 & 0 & 0 \\ 0 & 1 & 0 & 0 & -5 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 1 & 0 & 0 & -5 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We set  $s_2 = 1, s_0 = 0$  and get a solution

$$(t_0, t_1, t_2, t_3, s_0, s_1, s_2) = (0, 0, -6, 5, 0, 0, 1)$$

which corresponds to

$$E^*(x) = x^2, \text{ and } G^*(x) = 5x^3 - 6x^2.$$

Dividing  $G^*(x)$  by  $E^*(x)$  gives

$$W(x) = 5x - 6 = 5x + 7,$$

Alice's original polynomial. If we had set  $s_2 = 0, s_0 = 1$ , we would get  $E^*(x) = 1, G^*(x) = 5x + 7 = W(x)$ . ( $E(x) = 1$  is the appropriate error polynomial with no errors.)

*Remark 19.8* 1. A widely used Reed-Solomon code is  $R(255, 223)$ . It uses the field  $\mathbb{F} = \mathbb{F}_{2^8}$  of 256 elements. The code takes plaintext words (elements of  $\mathbb{F}$ ) of length 223, encodes them to code words of length 255, and is able to correct  $(255-223)/2 = 16$  errors.

One way to construct a field of 256 elements is to let  $m(x) = x^8 + x^4 + x^3 + x^2 + 1$ , an irreducible polynomial in  $\mathbb{F}_2[x]$ , and let  $\alpha$  be a root of  $m(x)$ . Then  $\mathbb{F}_2[\alpha]$  is a field of 256 elements. It turns out that  $\alpha$  is a primitive root in  $\mathbb{F}_2[\alpha]$ : that is,  $\alpha$  has order 255 in the group of units of  $\mathbb{F}_2[\alpha]$ . So a plaintext word is a polynomial  $W(x)$  of degree 222, and the encoded vector is the 255-tuple

$$W(1), W(\alpha), W(\alpha^2), \dots, W(\alpha^{254}).$$

As in the previous examples, Bob obtains

$$(r_0, r_1, \dots, r_{254})$$

and sets up the equations  $G^*(\alpha^i) = r_i E^*(\alpha^i)$  for  $i = 0, \dots, 254$ , where  $E^*(x)$  is an unknown polynomial of degree 16 and  $G^*(x)$  is an unknown polynomial of degree  $222 + 16 = 238$ . As in the last two examples, we can simplify the  $255 \times 256$  matrix of coefficients  $\mathbf{M}$  of the equations by multiplying by the inverse of the discrete Fourier transform (which in this case is exactly  $\hat{\mathbf{F}}$ , the inverse Fourier transform). We end up with the problem of doing row operations to reduce the  $16 \times 17$  matrix in the bottom right corner of  $\hat{\mathbf{F}}\mathbf{M}$  to reduced row echelon form, then use that reduced matrix to clear out the  $239 \times 17$  matrix above it by row operations, to yield the reduced row echelon form of  $\mathbf{M}$ .

The number of multiplications to obtain the reduced row echelon form of  $\mathbf{M}$  without premultiplying by  $\hat{\mathbf{F}}$  is about 5,600,000. By contrast, multiplying  $\mathbf{M}$  by  $\hat{\mathbf{F}}$  at the start requires around 1,100,000 multiplications to determine the entries of the last 17 columns of  $\hat{\mathbf{F}}\mathbf{M}$ . Then reducing  $\hat{\mathbf{F}}\mathbf{M}$  to reduced row echelon form requires around 34,000 multiplications. So when we evaluate the code polynomial at a complete set of roots of unity, applying the discrete Fourier transform reduces the number of multiplications required to decode to about one fifth of the number required by direct row reduction.

For this reason it is common to construct Reed-Solomon codes  $RS(n, m)$  over a field  $\mathbb{F}$  where to encode, the plaintext polynomial  $W(x)$  is evaluated at a complete set of  $n$ -th roots of unity in  $\mathbb{F}$ .

2. The field  $\mathbb{F}_{2^8} = \mathbb{F}_{256}$  is widely used with Reed-Solomon codes. The codes used on a CD are the 2-error correcting RS(32, 28) and RS(28, 24) code, both over  $\mathbb{F}_{256}$ . DVDs use an 8-error correcting RS(208, 192) code and a 5-error correcting RS(182, 172) code. The Voyager used a 16-error correcting RS(255, 223) code.

## Exercises

- 19.1. Why is every element of  $\mathbb{F}_8$  other than 0 and 1 a primitive root of  $\mathbb{F}_8$ ?
- 19.2. Suppose  $\mathbb{F}$  is a finite field with  $n + 1$  elements and  $\beta$  is a primitive root of  $\mathbb{F}$ , so that  $\beta$  has order  $n$ . Show that if  $\mathbf{F}$  is the  $n \times n$  discrete Fourier transform constructed from  $\beta$ , then the inverse  $\mathbf{F}^{-1} = -\hat{\mathbf{F}}$ .

Suppose given an  $(m, n)$ -Reed Solomon code defined over a finite field  $\mathbb{F}$ , in which the degree  $m - 1$  plaintext polynomial  $W(x)$  is evaluated at  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  for a fixed  $n$ -th root of unity  $\alpha$  of  $\mathbb{F}$ . The coefficient matrix  $\mathbf{M}$  of the equation  $\mathbf{M}\mathbf{X} = 0$  whose solution yields the polynomials  $G^*(x)$  and  $E^*(x)$  where  $E^*(x)W(x) = G^*(x)$  is then an  $n \times (n + 1)$  matrix.

- 19.3. Suppose the equation  $\mathbf{M}\mathbf{X} = 0$  is solved by directly reducing  $\mathbf{M}$  to reduced row echelon form. One source claims that the number of multiplications of elements of  $\mathbb{F}$  required to reduce  $\mathbf{M}$  is on the order of  $n^3/3$  for  $n$  large. Is this estimate accurate? Explain.
- 19.4. Now suppose that the matrix  $\mathbf{M}\mathbf{X} = 0$  is multiplied first by the inverse  $\mathbf{F}^{-1} = -\hat{\mathbf{F}}$  of the discrete Fourier transform matrix  $\mathbf{F}$ .
  - (i) Show that it takes approximately  $n^2(e + 1)$  multiplications in  $\mathbb{F}$  to multiply the last  $e + 1$  columns of  $\mathbf{M}$  by  $\mathbf{F}^{-1}$ .
  - (ii) Suppose given an  $n \times n + 1$  matrix  $\mathbf{F}^{-1}\mathbf{M}$  whose left  $n - e$  columns are the left  $n - e$  columns of the  $n \times n$  identity matrix  $I_n$ :

$$\mathbf{F}^{-1}\mathbf{M} = \begin{pmatrix} \mathbf{I}_{n-e-1} & \mathbf{B} \\ 0 & \mathbf{C} \end{pmatrix}$$

Assume that  $\mathbf{F}^{-1}\mathbf{M}$  can be reduced to a matrix of the form  $(\mathbf{I}_n, \mathbf{S})$  where  $\mathbf{I}_n$  is the  $n \times n$  identity matrix and  $\mathbf{S}$  is a column vector of  $n$  components. Show that it takes approximately  $e^3/3$  multiplications to transform  $\mathbf{C}$  to reduced row echelon form, and then takes approximately  $(n - e)e$  multiplications in  $\mathbb{F}$  to transform  $\mathbf{F}^{-1}\mathbf{M}$  to  $(\mathbf{I}_n, \mathbf{S})$ .

- 19.5. Given the accuracy of the estimates in the last two exercises, compare the number of multiplications required to reduce the matrix  $\mathbf{M}$  required in a Reed-Solomon code to reduced row echelon form
  - (a) using the discrete Fourier transform, with
  - (b) not using the discrete Fourier transform, for
    - (i) RS(32, 28) ( $n = 32, e = 2$ )
    - (ii) RS(255, 223) ( $n = 235, e = 16$ ).
- 19.6. In Example 19.6, suppose  $R = (1, 5, 0, 2, 9, 1)$ . Use the Reed-Solomon decoding procedure to find polynomials  $G^*(x), E^*(x)$  of degrees 3, 2, respectively, so that  $G^*(x) = W(x)E^*(x)$  where  $W(x)$  is Alice's plaintext polynomial.

# References

- [AB15] Adrian, D., Bhargavan, K., et al. (2015) Imperfect forward secrecy: how Diffie-Hellman fails in practice, 22nd ACM Conference on Computer and Communications Security (CCS '15), Denver, CO, 2015. Retrieved from <http://weakdh.org>.
- [AD15] Australia Defence and Strategic Goods List, in force on 8 April 2015. Retrieved from <https://www.comlaw.gov.au/Details/F2015C00310/Html/Text#Toc416345138>.
- [AES01] Announcing the Advanced Encryption Standard (AES) (2001), Federal Information Processing Standards Publication 197, Retrieved from <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- [AGL94] Atkins, D., Graff, M., Lenstra, A., Leyland, P. (1994) RSA-129. Retrieved from <http://www.crypto-world.com/announcements/RSA129.txt>.
- [AGP94] Alford, W.R., Granville, A. and Pomerance, C. (1994), There are infinitely many Carmichael numbers, Ann. of Math. 139, 703–722.
- [BBS86] Blum, L., Blum, M., and Shub, M. (1986), A simple unpredictable pseudorandom number generator SIAM J. Comput. 15, 364–383.
- [BG85] Blum, M. and Goldwasser, S. (1985), An efficient probabilistic public key encryption scheme which hides all partial information, Proceedings of Advances in Cryptology - CRYPTO '84, pp. 289–299, Springer Verlag, New York.
- [Bg13] Bogacki, P. (2000–2013) Linear Algebra Toolkit. Retrieved from [www.math.odu.edu/bogacki/cgi-bin/lat.cgi](http://www.math.odu.edu/bogacki/cgi-bin/lat.cgi).
- [Bo12] The Diffie-Hellman protocol -Cryptography-Professor Dan Boneh (2012), Retrieved from <https://www.youtube.com/watch?v=3gfrL5-G3qc>.
- [Bo99] Boneh, D. (1999), Twenty years of attacks on the RSA cryptosystem, Notices of the American Mathematical Society (AMS), Vol. 46, No. 2, pp. 203–213.
- [BJN00] Boneh D., Joux A., Nguyen P.Q. (2000) Why Textbook ElGamal and RSA Encryption Are Insecure. In: Okamoto T. (eds) Advances in Cryptology—ASIACRYPT 2000. ASIACRYPT 2000. Lecture Notes in Computer Science, vol 1976. Springer, Berlin, Heidelberg.
- [BS02] Boneh, D., Shacham, H. (2002), Fast variants of RSA. CryptoBytes, Vol. 5, No. 1, pp. 1–9.
- [BV98] Boneh, D., Venkatesan, R. (1998), Breaking RSA may not be equivalent to factoring., In Proceedings Eurocrypt '98, Lecture Notes in Computer Science, Vol. 1233, Springer-Verlag, pp. 59–71.
- [Ca16] Caldwell, C., The Prime Pages (2016), Retrieved from <https://primes.utm.edu>.
- [CDL00] Cavallar, S.H., Dodson, B., Lenstra, A.K., Lioen, W.M., Montgomery, P.L., Murphy, B., Riele, H.J.J. te, Aardal, K., Gilchrist, J., Guillern, G., Leyland, P.C., Marchand, J., Morain, F., Muffet, A., Putnam, C., Putnam, C., Zimmermann, P. (2000), Factorization of a 512-bit RSA modulus, Advances in Cryptology, Springer Lecture Notes in Computer Science, 1807, 1–18.
- [Ch09] Childs, L. (2009), A Concrete Introduction to Higher Algebra, 3rd edn, Springer, New York.
- [Ci93] Cipra, B. (1993), The ubiquitous Reed-Solomon codes, SIAM News. January, 1993. Retrieved from [www.eccpage.com/reed\\_solomon\\_codes.html](http://www.eccpage.com/reed_solomon_codes.html).
- [Cs15] Cisco Systems (2012–2015), Next Generation Encryption, Retrieved from [http://www.cisco.com/web/about/security/intelligence/nextgen\\_crypto.html](http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html).
- [Cla19] Clarke, J. (2019), An Optimist's View of the 4 Challenges to Quantum Computing, IEEE Spectrum, retrieved 22 March, 2019 from <https://spectrum.ieee.org/tech-talk/computing/hardware/an-optimists-view-of-the-4-challenges-to-quantum-computing>.

- [CH97] Collins, T., Hopkins, D., Langford, S., Sabin, M., Public Key Cryptographic Apparatus and Method, U. S. Patent # 5,848,159, January, 1997.
- [Co00] Cohen, H., Advanced Topics in Computational Number Theory, Graduate Texts in Mathematics, Springer-Verlag, 2000.
- [CP05] Crandall, R. E. and Pomerance C. (2005), Prime Numbers, A Computational Perspective, 2nd edn. Springer, New York.
- [Del84] Delaurentis, J.M. (1984), A further weakness in the common modulus protocol for the RSA cryptoalgorithm, *Cryptologia* 8, 253–259.
- [DH76] Diffie, W. and Hellman, M. (1976), New directions in cryptography, *IEEE Trans. Inform. Theory* IT22, 644–654.
- [DF99] Dummit, D. S., Foote, R. M. (1999), Abstract Algebra, 2nd edn., John Wiley & Sons, New York.
- [El85] ElGamal, T. (1985), “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, *IEEE Transactions on Information Theory* 31 (4): 469–472.
- [El87] Ellis, J. H. (1987), The story of non-secret encryption (made public, 1997). Retrieved from <https://web.archive.org/web/20030610193721/http://jya.com/ellisdoc.htm>.
- [Eu00] Euclid (300 BC), The Elements, Heath, T. L., transl (1925–1936), Dover, New York.
- [FM82] Fishman, G.S. and Moore, L.R. (1982), A statistical evaluation of multiplicative congruential random number generators with modulus  $2^{31} - 1$ , *J. Amer. Statist. Assoc.* 77, 129–136.
- [Ga16] Gallian, J. A. (2016), FBI adopts new checksum algorithm, *MAA Focus* 36, No. 1, p. 6.
- [Go15] Goodin, D. (2015) How the NSA can break trillions of encrypted Web and VPN connections, Retrieved from <http://arstechnica.com/security/2015/10/how-the-nsa-can-break-trillions-of-encrypted-web-and-vpn-connections/>.
- [Go15b] Goodin, D. (2015), NSA preps quantum-resistant algorithms to head off crypto-apocalypse, Retrieved from <https://arstechnica.com/security/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocalypse/>.
- [Gra92] Granville, A. (1992), Primality testing and Carmichael numbers, *Notices Amer. Math. Soc.* 39, 696–700.
- [Gra04] Granville, A. (2004), Smooth numbers: computational number theory and beyond, in J. Buhler and P. Stevenhagen, eds. (2008), Algorithmic Number Theory, Cambridge Univ. Press.
- [GW16] Guruswami, V. , Wootters, M., Repairing Reed-Solomon Codes, [arXiv:1509.04764v2](https://arxiv.org/abs/1509.04764v2) [cs.IT], last revised 9 August 2016.
- [Ha03] Haiman, M. (2003), Notes on Reed-Solomon Codes, Retrieved from <https://math.berkeley.edu/~mhaiman/math55/reed-solomon.pdf>.
- [Ham50] Hamming, R.W. (1950), Error detecting and error correcting codes, *Bell System Tech. J.* 29, 147–160.
- [Ham80] Hamming, R.W. (1980), Coding and Information Theory, Prentice-Hall, 1980.
- [HM92] Hanson, T, Mullen, G. L., Primitive Polynomials Over Finite Fields, *Math. Comp.* 59 (1992), pp. S47–S50.
- [Hel79] Hellman, M.E. (1979), The mathematics of public-key cryptography, *Scientific American*, August 1979, 146–157.
- [Hi29] Hill, L. S. (1929), Cryptography in an algebraic alphabet, *Amer. Math. Monthly* 36, 306–312.
- [Hi31] Hill, L. S. (1931), Concerning certain linear transformation apparatus of cryptography, *Amer. Math. Monthly* 38, 135–154.
- [HK71] Hoffman, K., Kunze, R. (1971), Linear Algebra, 2nd edition, Prentice-Hall, Englewood Cliffs, NJ.
- [HPS10] Hoffstein, J, Pipher, J, Silverman, J. H. (2010), An Introduction to Mathematical Cryptography, Springer, New York.
- [IBM17] [www.research.ibm.com/ibm-q/](http://www.research.ibm.com/ibm-q/) Retrieved May 29, 2017.
- [Im94] Immink, K. A. S. (1994), Reed-Solomon Codes and the Compact Disc, in Wicker, S. B.; Bhargava, V. K., Reed-Solomon Codes and Their Applications, IEEE Press.
- [Ja85] Jacobson, N. (1985), Basic Algebra I, 2nd ed., Freeman, New York.
- [JOP14] Joux, A., Odlyzko, A., Pierrot, C. (2014), The past, evolving present and future of discrete logarithm, in C. K. Koc, ed., Open Problems in Mathematical and Computational Sciences, Springer, New York, 5–36.
- [Kah67] Kahn, D. (1967), The Codebreakers, Macmillan, New York.
- [Kal16] Kalai, G. (2016), The quantum computer puzzle, *Notices of the American Mathematical Society*, vol. 63, No. 5 (2016), pp. 508–516.
- [Kat98] Katz, V. J. (1998), A History of Mathematics, an introduction (2nd edition), Addison Wesley, Reading, MA.
- [KAF10] Kleinjung, T., Aoki, K., Franke, J., Lenstra, A.K., Thomé, E., Bos, J.W., Gaudry, P., Kruppa, A., 91 Montgomery, P.L., Osvik, D.A., te Riele, H., Timofeev, A., Zimmermann, P. (2010), Factorization of a 768-bit RSA modulus, *Proceedings of Advances in Cryptology -CRYPTO 2010*, Santa Barbara, CA, USA , 333–350.
- [Knu98] Knuth, D.E. (1998), The Art of Computer Programming, 3rd edn, Vol. 2, Addison- Wesley, Reading, MA.
- [Kob94] Koblitz, N. (1994), A Course in Number Theory and Cryptography, Springer, New York.
- [Ko94] Kolata, G. (1994), 100 quadrillion calculations later, *Eureka*, New York Times, April 27, 1994.
- [Kon81] Konheim, A.G. (1981), Cryptography, A Primer, Wiley, New York.

- [LO91] LaMacchia, B. A., Odlyzko, A. M. (1991), Solving large sparse linear systems over finite fields, in Advances in Cryptology - CRYPTO '90, A. J. Menezes and S. A. Vanstone (eds.), Springer Verlag, Lecture Notes in Computer Science # 537 109–133.
- [Lu60] Luhn, H. P., (1960) Computer for Verifying Numbers, US Patent 2,950,048, August 23, 1960, retrieved from <https://www.google.com/patents/US2950048>.
- [MS83] MacWilliams, F.J. and Sloane, N.J.A. (1983), The Theory of Error-Correcting Codes, North-Holland, Amsterdam.
- [MvOV96] Menezes, A., van Oorschot, P., Vanstone, S. (1996), Handbook of Applied Cryptography, CRC Press.
- [Mu13a] Mullin, J. (2013), Newegg trial: Crypto legend takes the stand, goes for knockout punch, Retrieved from <http://arstechnica.com/tech-policy/2013/11/newegg-trial-crypto-legend-diffie-takes-the-stand-to-knock-out-patent/>.
- [Mu13b] Mullin, J. (2013), Jury: Newegg infringes Spangenberg patent, must pay \$2.3 million, Retrieved from <http://arstechnica.com/tech-policy/2013/11/jury-newegg-infringes-spangenberg-patent-must-pay-2-3-million/>.
- [Na17] Nature, International weekly journal of science, The week in science: 19–25 May 2017, dated 24 May 2017, “Quantum computing, election pledges and a thief who made science history”, retrieved May 29, 2017 from [www.nature.com/news/quantum-computing-election-pledges-and-a-thief-who-made-science-history-1.22030](http://www.nature.com/news/quantum-computing-election-pledges-and-a-thief-who-made-science-history-1.22030).
- [No16] Nordrum, A (2016), Quantum computer comes closer to cracking RSA encryption, IEEE Spectrum, March 3, 2016, retrieved from <http://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment>.
- [NZ72] Niven, I, Zuckerman, H. S. (1972), An Introduction to the Theory of Numbers, 3rd. edn., Wiley, New York.
- [Od85] Odlyzko, A. M. (1985), Discrete logarithms in finite fields and their cryptographic significance, in T. Beth, N. Cot, and I. Ingemarsson (eds.), Advances in Cryptology: Proceedings of EUROCRYPT 84, Springer-Verlag, Lecture Notes in Computer Science # 209, 224–314.
- [Oeis] The On-Line Encyclopedia of Integer Sequences, Number of groups of order  $n$ , February 2017. Retrieved from [http://oeis.org/wiki/Number\\_of\\_groups\\_of\\_order\\_n](http://oeis.org/wiki/Number_of_groups_of_order_n).
- [PM88] Park, S.K. and Miller, K.W. (1988), Random number generators: Good ones are hard to find, Comm. ACM 31, 1192–1201.
- [Ple98] Pless, V. (1998), Introduction to the Theory of Error-Correcting Codes, 3rd edn., Wiley, New York.
- [PH78] Pohlig , S. and Hellman, M. (1978). “An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance” (PDF). IEEE Transactions on Information Theory (24): 106–110.
- [Pom84] Pomerance, C. (1984), Lecture notes on primality testing and factoring, MAA Notes # 4.
- [Pom90] Pomerance, C., Ed. (1990), Cryptology and computational number theory, Proc. Symposia in Applied Math, American Mathematical Society.
- [PSW80] Pomerance, C., Selfridge, J.L., and Wagstaff, S.S. (1980), The pseudoprimes to  $25 \times 10^9$ , Math. Comp. 35, 1003–1026.
- [Rab80] Rabin, M.O. (1980), Probabilistic algorithm for testing primality, J. Number Theory 12, 128–138.
- [RS60] Reed, I. S.; Solomon, G. (1960), Polynomial codes over certain finite fields, J. Society for Industrial and Applied Mathematics (SIAM) 8 , 300–304.
- [Rib89] Ribenboim, P. (1989), The Book of Prime Number Records, 2nd. ed., Springer-Verlag, New York.
- [Rib96] Ribenboim, P. (1996), The New Book of Prime Number Records, Springer-Verlag, New York.
- [RSA78] Rivest, R., Shamir, A., and Adleman, L. (1978), A method for obtaining digital signatures and public-key cryptosystems, Comm. ACM 21, 120–126.
- [RSA11] Rivest, Shamir, Adleman - The RSA Algorithm Explained (2011). Retrieved from <https://www.youtube.com/watch?v=b57zGAKNKIc>.
- [RSA15] RSA Factoring Challenge (2015), Retrieved from [https://en.wikipedia.org/wiki/RSA\\_Factoring\\_Challenge](https://en.wikipedia.org/wiki/RSA_Factoring_Challenge).
- [She17] Shemanske, Thomas R. (2017), Modern Cryptography and Elliptic Curves, A Beginner’s Guide, Student Mathematical Library vol. 83, American Mathematical Society.
- [Sh97] Shor, P. W. (1997), Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer SIAM J. Comput., 26(5), 1484–1509.
- [St06] Strang, G. (2006), Linear Algebra and its Applications, 4th edition, Brooks/Cole, Belmont, CA.
- [Tr09] Trow, P. (2009), Modular Arithmetic Calculator, Retrieved from <http://ptrow.com/perl/calculator.pl>.
- [Un17] The Unicode Consortium (2017), What is Unicode? Retrieved from <http://www.unicode.org/standard/WhatIsUnicode.html>.
- [US13] U. S. National Institute of Standards, Digital Signature Standard (DSS), U. S. National Institute of Standards and Technology, publication 186–4, issued July 2013. Retrieved from <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>.
- [VL82] Van Lint, J.H. (1982), Introduction to Coding Theory, Springer-Verlag, New York.
- [Zy14] Zyga, L. (2014), New largest number factored on a quantum device is 56,153, Retrieved from <http://phys.org/news/2014-11-largest-factored-quantum-device.html>.

# Index

## Symbols

$(a \bmod m)$ , 2, 13, 21

$R \bmod J$ , 73

$RS(n, m)$ , 334

$R[x]$ , 84

$U_R$ , 70

$U_m$ , 117

$\lambda(m)$ , 230

$\mathbb{F}_8$ , 333

$\mathbb{N}$ , 2

$\mathbb{Z}$ , 2

$\mathbb{Z}/m\mathbb{Z}$ , 198

$\phi(m)$ , 136, 138

$\phi(m)$ –Euler’s phi function, 123

$a$ -pseudoprime, 145, 189, 213

$a$ -pseudoprime test, 144, 213, 251

$e$ -th roots of unity, 243

$m \times n$  matrix, 94

$m$ -to-one function, 199

$n$ -SG prime, 193

$p$ -adic logarithm, 239

2-pseudoprime, 145

2-pseudoprime test , 144

Associative property, 66

Associativity, 66, 100

Associativity of addition, 16

Associativity of multiplication, 16

Australian Defence Controls Act of 2011, 223

## B

Baby step-giant step algorithm, 221, 233, 238

Base 2, 23

Base case, 57

Bezout’s Identity, 33, 37, 58, 59, 61, 117, 172, 173, 175, 179, 185, 208, 212, 313, 316–318

Bezout’s Identity, for polynomials, 315

Bijection, 72, 217

Bijective, 197

Binary form, 23

Binomial coefficient, 125

Binomial Theorem, 125

Bob, 4

Boneh, D., 138, 221, 253

Boneh, Joux and Nguyen, 235

Boneh’s Theorem, 256

## A

Abelian group, 66, 117, 153

Addition modulo  $m$ , 13

Addition, of column vectors, 96

Addition of cosets, 321

Addition of polynomials, 84

Addition of vectors, 36

Addition rule for congruences, 20

Addition table, 205

Addition table mod  $m$ , 14

Additive Caesar cipher, 17

Additive group, 155

Additive group of a ring, 69

Advanced Encryption Standard (AES), 141, 221, 222, 328

Alice, 4

ASCII, 22

Associates, 315

## C

Caesar cipher, 3, 141

Cancel, in congruence, 20, 182

Cancel, in  $\mathbb{Z}_m$ , 16

Cancel modulo  $m$ , 119

Carmichael number, 145, 151, 160, 210, 250, 251

Carmichael numbers, squarefree, 251

Carmichael numbers, strong, 251

Characteristic of a field, 212

Chebyshev, P. , 142

Check digit, 7

Chinese Remainder Theorem (CRT), 124, 171, 172, 189, 192, 196, 207, 209, 230, 231, 233

Chronometer, 9

Cipher, 3

Ciphertext, 3

Classical logarithm, 218

Clock arithmetic, 3

- Closed , 66  
 Coded word, 334  
 Code word, 102  
 Codomain, 196  
 Coefficients, 83  
 Column vector, 94  
 Common divisor, 28  
 Common encrypting exponents in RSA, 180  
 Common multiple, 54  
 Commutative, 96  
 Commutative law, 67  
 Commutativity, 66  
 Commutativity of addition, 16  
 Commutativity of multiplication, 16, 205  
 Complete induction, 57  
 Complete set of representatives modulo  $m$ , 78  
 Complex numbers, 81, 324  
 Component, 94, 97  
 Composite, 51  
 Compositeness test, 144  
 Congreve, William, 6  
 Congruence modulo an ideal, 73  
 Congruence modulo  $m$ , 19  
 Congruences, reversible operations on, 182  
 Congruent modulo an ideal, 325  
 Congruent modulo  $m(x)$ , 325  
 Coprime, 28, 173, 317  
 Coprime Divisibility Lemma, 42, 58, 59, 64, 90, 125, 147, 148, 318  
 Coset, 160, 161, 198, 202, 241, 247, 249, 254, 321  
 Coset of  $J$  represented by  $a$ , 73  
 Cosets and group tables, 162  
 Cosets, of an ideal, 153  
 Cosets, properties of, 164  
 Crossed product, 81  
 Cyclic, 216  
 Cyclic group, 155, 216, 238  
 Cyclic subgroup, 155
- D**  
 D'Alembert's Theorem, 88, 212, 228, 251  
 Decoding, of a (7, 4) code, 104  
 Decrypted, 3  
 Decrypting exponent, for RSA, 136, 237  
 Decrypting in RSA, 177  
 Decrypting multiplier, 29  
 Degree, 84  
 Degree formula, 85, 90  
 de la Vallée Poussin, C. J., 142  
 Diffie–Hellman cryptosystem, 149  
 Diffie–Hellman key exchange, 220  
 Diffie–Hellman over an elliptic curve, 223  
 Diffie–Hellman over  $\mathbb{Z}_p$ , 223  
 Diffie–Hellman problem, 221  
 Diffie–Hellman security, 223  
 Digital Encryption Standard (DES), 141, 328  
 Digital Signature Standard, 222  
 Dimension, 244  
 Discrete Fourier transform, 333, 336, 341  
 Discrete logarithm, 217  
 Discrete logarithm problem, 220–222, 229  
 Distributive law, 67, 85, 99  
 Distributivity, 16, 77, 100  
 Dividend, 2, 28  
 Divides, 28, 53, 54, 87  
 Division Theorem, 2, 13, 21, 28, 30, 62, 64, 314, 316, 320  
 Division Theorem, for polynomials, 86  
 Divisor, 2, 28  
 Domain, 196
- E**  
 EEA vector, 38, 39, 113  
 Efficiency, 102, 110  
 ElGamal cryptosystem, 221  
 Elliptic curve cryptography, 223  
 Encoding, of a (7, 4) code, 103  
 Encrypted, 3  
 Encrypting exponent, for RSA, 136  
 Encrypting multiplier, 34  
 Equality of cosets, 74, 321  
 Equality, of functions, 84, 89  
 Equality, of polynomials, 84  
 Equivalence relation, 20  
 Error polynomial , 334  
 Error vectors, 247  
 Euclid's Algorithm, 32, 59, 90, 174, 313  
 Euclid's Algorithm, for polynomials, 314  
 Euclid's proof, of infinitely many primes, 141  
 Euler's formula, 208  
 Euler's phi function, 118, 123, 195, 209  
 Euler's Theorem, 123, 126, 137, 166, 169, 248, 249  
 Evaluation at  $a$  map, 211, 329  
 Evaluation homomorphism, 199  
 Eve, 6  
 Even integers, as a coset, 161  
 Excel, 13, 40, 129, 234  
 Exponential notation, 52, 319  
 Exponent of a finite abelian group, 224  
 Exponent of an abelian group, 212  
 Extended Euclidean Algorithm (EEA), 37, 97, 174, 316
- F**  
 Factor, 28  
 Factoring, 42, 255  
 Factoring numbers, 89  
 Federal Bureau of Investigation (FBI), 10  
 Fermat's Theorem, 121, 122, 137, 138, 144, 171, 213, 250  
 Fibonacci, 56  
 Fibonacci sequence, 49  
 Field, 70, 79, 88  
 Fields, table of, 326  
 Finite cyclic group, 160  
 Finite field, 313  
 Finite group, 154  
 First Isomorphism Theorem, for groups, 246

FOIL, 80  
 Fractions, addition of, 54  
 Function, 196  
 Fundamental Homomorphism Theorem, 200, 242, 246  
 Fundamental Theorem of Arithmetic (FTA), 51, 52, 57–59

**G**  
 Generalized Associativity, 249  
 Generalized Commutativity, 249  
 General linear group, 167  
 Generator of a cyclic group, 216  
 Generators, of a subgroup, 155  
 Greatest common divisor, 28, 32, 54, 55, 242, 313  
 Greatest common divisor, of two polynomials, 317  
 Greatest common divisors, of polynomials, 314  
 Group, 66, 101, 153  
 Group, abelian, 153  
 Group homomorphism, 201, 217, 241, 242  
 Group of  $e$ -th roots of unity, 159  
 Group table, 162

**H**  
 Hadamard, J., 142  
 Hamming check digit scheme, 11  
 Hamming code, 102  
 Hamming (7, 4) code, 102  
 Hamming (8, 4) code, 108, 204, 246  
 Hamming distance, 110  
 Hamming, R. W., 102  
 Hard problem, 135  
 Hill codes, 114  
 Homogeneous, 101  
 Homogeneous congruences, 185  
 Homogeneous equation, 43, 245, 335  
 Homogeneous linear equations, 156

**I**  
 IBM, 139  
 Ideal, 70, 154, 199, 246, 320  
 Ideals and subgroups, 169  
 Identity element, 66, 154  
 Identity matrix, 96, 336  
 Image, 196  
 Indeterminate, 83, 84  
 Index, 166  
 Index calculus, 222  
 Induction, 56, 89, 126, 176  
 Induction proof, 57  
 Induction step, 57  
 Injective, 196, 199  
 Integer linear combination, 36, 98  
 Integers, 2  
 Inverse, 66, 68  
 Inverse Fourier transform, 333, 336, 342  
 Inverse function, 208  
 Inverse isomorphisms, 218

Inverse modulo  $m$ , 14  
 Inverse of  $a$  modulo  $p$ , 122  
 Irreducible, 318, 324  
 Isomorphic, 198, 206  
 Isomorphism, 198  
 Isomorphism of groups, 209  
 Isomorphism of rings, 206

**K**  
 Karatsuba multiplication, 81  
 Katakana, 49  
 Kernel, 199, 202, 242, 245  
 Kernel, of a group homomorphism, 202  
 Key, 7, 17  
 Kleinjung, T., 139  
 Knuth, Donald, 127

**L**  
 Lagrange's Theorem, 165–167, 200, 203, 241, 254  
 Lamé, 49, 63  
 Last non-zero remainder, 32, 315  
 Leading coefficient, 84  
 Leading term, 84  
 Least common denominator, 54  
 Least common multiple, 54, 61, 120, 176  
 Least non-negative residue, 2, 13  
 Left cancellation, 81  
 Left coset, 160, 167, 246  
 Left solvability, 81  
 Lenstra, A., 139  
 Linear combination, 97  
 Linear combination of vectors, 100  
 Linear congruence, 181  
 Linear transformation, 204, 244  
 Logarithm, 211, 217  
 Logarithm to the base  $g$ , 217  
 Log table, 333  
 Long division, 28  
 Long division, for polynomials, 86  
 Luhn formula, 7, 102

**M**  
 MAPLE, 13  
 Matrix, 94, 204  
 Matrix equation, 100  
 Matrix multiplication, 95  
 Matrix of coefficients, 101  
 Mean Value Theorem, 197  
 Minimal set of generators, 155  
 Modulus, 19  
 Monic, 85, 317  
 Monomial, 84  
 Multiple, 28  
 Multiple factor, 319  
 Multiple root, 319  
 Multiplication by  $a$  homomorphism, 242  
 Multiplication by  $r$  homomorphism, 203

- Multiplication modulo  $m$ , 13  
 Multiplication of cosets, 321  
 Multiplication of polynomials, 84  
 Multiplication rule for congruences, 20  
 Multiplication table, 205, 323  
 Multiplication table mod  $m$ , 14  
 Multiplicative Caesar cipher, 18, 29, 40, 77, 114, 118, 329  
 Multiplicative inverse, 68
- N**  
 Natural logarithm, 142  
 Natural numbers, 2  
 Negatives, 16  
 Non-abelian group, 167  
 Non-trivial  $n$ -th root of unity, 331  
 Non-trivial subgroup, 167  
 Normal subgroup, 168, 246  
 Null space, 101, 111, 244, 245  
 Null space of a matrix, 204  
 Number Field Sieve, 139
- O**  
 Odd integers, as a coset, 161  
 One-to-one, 72, 196, 199, 211  
 One-to-one correspondence, 165, 200  
 One-to-one function, 242  
 Onto, 72, 196, 211  
 Operation, 66  
 Order, 166  
 Ordered pairs, 204  
 Order of  $a$  modulo  $m$ , 119  
 Order of a finite group, 224  
 Order of a group, 166  
 Order of an element, 154, 224  
 Order, of an element of a finite group, 119  
 Order of an element, properties, 224
- P**  
 Partition, 165  
 Pascal's triangle, 125  
 Pigeonhole principle, 118  
 Plaintext, 3, 334  
 Plaintext message, 334  
 Plaintext word, 102, 334  
 Pohlig–Hellman algorithm, 222  
 Pohlig–Hellman method, 238  
 Pollard  $p - 1$  algorithm, 193  
 Polynomial, 83  
 Polynomial function, 84  
 Preprocessing, 235, 239  
 Primality test, 250  
 Prime, 51  
 Prime field, 313  
 Prime number, 51  
 Prime Number Theorem, 142, 144  
 Primes, infinitely many, 141
- Primitive polynomial, 327  
 Primitive root, 79, 80, 82, 222, 228, 324, 327  
 Primitive root modulo  $p$ , 230  
 Primitive root modulo  $p^n$ , 230  
 Primitive Root Theorem, 89, 228  
 Principal ideal, 71, 320  
 Private key, 220  
 Private key cryptosystem, 7, 135  
 Probabilistic primality test, 148  
 Product of rings, 204
- Q**  
 Quadratic formula, 88  
 Quantum computer, 139, 224  
 Quotient, 2, 28, 86  
 Quotient ring, 321
- R**  
 Rabin's Theorem, 148, 251  
 Radix 2, 23  
 Raise to the  $e$ -th power homomorphism, 243  
 Raise to the  $r$ -th power homomorphism, 203  
 Range, 196, 242–244  
 Reduced row echelon form, 244, 336  
 Reduced row echelon form of a matrix, 103  
 Redundancy, 102  
 Reflexive, 20  
 Relatively prime, 28, 317  
 Remainder, 2, 28, 86  
 Remainder Theorem, 87  
 Repetition code, 8, 102  
 Representative, of a coset, 74, 165, 198, 321, 322  
 Right coset, 161  
 Rijndael, 141  
 Ring, as abelian group, 153  
 Ring homomorphism, 77, 197, 200  
 Ring with identity, 66  
 Root, 88  
 Roots of unity, 159, 210, 331  
 Roots of unity, in the complex numbers, 159  
 Root Theorem, 88, 89, 314  
 Rosser, J. B., 142  
 Row operations, 334, 336  
 Row vector, 94, 316  
 RSA, 135, 138, 177, 196, 223, 253  
 RSA-129, 139  
 RSA-768, 139  
 RSA encrypting, 190  
 RSA Factoring Challenge, 139  
 RSA moduli with more than two factors, 179  
 RSA weakness, 235
- S**  
 Safeprime, 193, 213, 217, 222, 229, 236, 237  
 Scalar, 97  
 Scalar multiplication, 36, 70, 97  
 Schoenfeld, L., 142

- Shor, P., 139  
Sieve of Eratosthenes, 143  
Signature, 140  
Signature, RSA, 256  
Signed numbers, 69  
Simultaneous congruences, 176  
Solutions of systems of two congruences, 182  
Sophie Germain prime, 193, 217, 229  
Special prime, 193  
Strong  $a$ -pseudoprime, 147  
Strong  $a$ -pseudoprime test, 147, 251  
Subgroup, 154, 157, 202, 246  
Subgroup of a cyclic group, 155  
Subgroup of a finite group, 154  
Subgroup of a group, 168  
Subgroups of  $U_{24}$ , 158  
Subring, 67  
Subspace, 246  
Subtraction modulo  $m$ , 13  
Surjective, 196  
Symmetric, 20  
Symmetric cryptosystem, 7, 141, 221  
System of congruences, 172  
System of linear equations, 100  
Systems of congruences, 181  
Systems of non-monic linear congruences, 187
- U**  
Unicode, 23  
Unique factorization, 176  
Unique factorization into prime numbers, 313  
Uniqueness of factorization, for polynomials, 319  
Unit, 14, 69, 79, 85, 88, 205, 331  
Units modulo  $m$ , 157  
Units, of  $F[x]$ , 317  
Units, of a commutative ring, 153
- V**  
Vector, 36, 94  
Vector space, 154, 204, 244, 246  
Vernam cipher, 6, 141  
Vigenère cipher, 4, 10, 141, 221  
Vigenère cryptosystem, 49
- W**  
Well-defined, 75, 200, 321  
Well-Ordering, 59, 119, 316  
Well-Ordering Principle, 61, 64  
Word, 22
- X**  
XS binary algorithm, 23, 136, 146, 171, 219  
XS binary method, 122, 127
- Z**  
Zero, 16  
Zero divisor, 15, 79, 85, 88, 205  
Zero element, 66  
Zero polynomial, 85  
Zero vector, 204  
Zhang, Yitang, 212