
Operational notes

Document updated on **December 15, 2021**.



The following colors are **not** part of the final product, but serve as highlights in the editing/review process:

- text that needs attention from the Subject Matter Experts: Mirco, Anna,& Jan
- terms that have not yet been defined in the book
- text that needs advice from the communications/marketing team: Aaron & Shane
- text that needs to be completed or otherwise edited (by Sylvia)

NB: This PDF only includes the Arithmetics chapter

Todo list

zero-knowledge proofs	12
played with	12
finite field	12
elliptic curve	12
book?	12
Update reference when content is finalized	12
methatical	12
numerical	13
a list of additional exercises	13
think about them	13
add some more informal explanation of absolute value	14
We haven't really talked about what a ring is at this point	14
What's the significance of this distinction?	15
reverse	15
Turing machine	15
polynomial time	15
sub-exponentially, with $\mathcal{O}((1 + \varepsilon)^n)$ and some $\varepsilon > 0$	15
Add text	16
\mathbb{Q} of fractions	16
Division in the usual sense is not defined for integers	16
Add more explanation of how this works	17
pseudocode	18
modular arithmetics	18
actual division	18
multiplicative inverses	18
factional numbers	18
exponentiation function	20
See XXX	20
once they accept that this is a new kind of calculations, its actually not that hard	20
perform Euclidean division on them	20
This Sage snippet should be described in more detail.	21
prime fields	23
residue class rings	23
Algorithm sometimes floated to the next page, check this for final version	23
Add a number and title to the tables	25
(-1) should be (-a)?	26
we have	28
rephrase	32
subtrahend	33

 minuend	33
 what does this mean?	38

MoonMath manual

TechnoBob and the Least Scruples crew

December 15, 2021

Contents

1	Introduction	5
1.1	Target audience	5
1.2	The Zoo of Zero-Knowledge Proofs	6
	To Do List	8
	Points to cover while writing	8
2	Preliminaries	9
2.1	Preface and Acknowledgements	9
2.2	Purpose of the book	9
2.3	How to read this book	10
2.4	Cryptological Systems	10
2.5	SNARKS	10
2.6	complexity theory	10
	2.6.1 Runtime complexity	10
2.7	Software Used in This Book	11
	2.7.1 Sagemath	11
3	Arithmetics	12
3.1	Introduction	12
	3.1.1 Aims and target audience	12
	3.1.2 The structure of this chapter	13
3.2	Integer Arithmetics	13
	Euclidean Division	16
	The Extended Euclidean Algorithm	18
3.3	Modular arithmetic	19
	Congurency	20
	Modular Arithmetics	20
	The Chinese Remainder Theorem	23
	Modular Inverses	26
3.4	Polynomial Arithmetics	29
	Polynomial Arithmetics	33
	Euklidean Division	34
	Prime Factors	36
	Lange interpolation	38
4	Algebra	40
4.1	Groups	40
	Commutative Groups	41
	Finite groups	43

	Generators	43
	The discrete Logarithm problem	43
4.1.1	Cryptographic Groups	44
	The discret logarithm assumption	45
	The decisional Diffi Hellman assumption	47
	The computational Diffi Hellman assumption	47
	Cofactor Clearing	48
4.1.2	Hashing to Groups	48
	Hash functions	48
	Hashing to cyclic groups	50
	Hashing to modular arithmetics	51
	Pederson Hashes	54
	MimC Hashes	55
	Pseudo Random Functions in DDH-A groups	55
4.2	Commutative Rings	55
	Hashing to Commutative Rings	58
4.3	Fields	58
	Prime fields	59
	Square Roots	61
	Exponentiation	62
	Hashing into Prime fields	62
	Extension Fields	62
	Hashing into extension fields	65
4.4	Projective Planes	66
5	Elliptic Curves	68
5.1	Elliptic Curve Arithmetics	68
5.1.1	Short Weierstraß Curves	68
	Affine short Weierstraß form	69
	Affine compressed representation	73
	Affine group law	73
	Scalar multiplication	77
	Projective short Weierstraß form	80
	Projective Group law	81
	Coordinate Transformations	82
5.1.2	Montgomery Curves	82
	Affine Montgomery Form	82
	Affine Montgomery coordinate transformation	85
	Montgomery group law	86
5.1.3	Twisted Edwards Curves	87
	Twisted Edwards Form	87
	Twisted Edwards group law	88
5.2	Elliptic Curves Pairings	90
	Embedding Degrees	90
	Elliptic Curves over extension fields	91
	Full Torsion groups	92
	Torsion-Subgroups	93
	The Weil Pairing	94

5.3	Hashing to Curves	97
	Try and increment hash functions	97
5.4	Constructing elliptic curves	99
	The Trace of Frobenius	100
	The j -invariant	101
	The Complex Multiplication Method	101
	The <i>BLS6_6</i> pen& paper curve	108
	Hashing to the pairing groups	113
6	Statements	115
6.1	Formal Languages	115
	Checking Relations	115
	Instance and Witness	117
	Modularity	120
6.2	Statement Representations	120
6.2.1	Rank-1 Quadratic Constraint Systems	120
	R1CS representation	120
	R1CS Satisfiability	122
	Modularity	122
6.2.2	Algebraic Circuits	123
	Algebraic circuit representation	123
	Circuit Execution	125
	Circuit Satisfiability	127
	Circuit to R1CS compilers	128
6.3	Gadgets	132
6.3.1	Atomic Types	133
	The Basefield type	133
	The Subtraction Constraints System	133
	The Inversion Constraint System	133
	The Division Constraint System	134
	Modularity	135
	The Boolean Type	135
	The Boolean Constraint System	135
	The AND operator constraint system	136
	The OR operator constraint system	136
	The NOT operator constraint system	137
	Modularity	138
	Binary representations	140
	Range Proofs	141
	UIntN	142
	Bit constraints	142
6.3.2	Control Flow	142
	The Conditional Assignment	142
	Loops	143
6.3.3	Cryptographic Primitives	143
	Twisted Edwards curves	143
	Twisted Edwards curves constraints	144
	Twisted Edwards curves addition	145

	Twisted Edwards curves inversion	145
	Twisted Edwards curves scalar multiplication	146
	A Simple Pen and Paper Compiler Example	146
6.3.4	Outlook on Real World Implementations	146
7	Proof Systems	147
7.1	Pairing Based Proof Systems	147
7.1.1	Quadratic Arithmetic Programs	147
7.1.2	Quadratic span programs	150
7.2	proof system	150
7.2.1	Pairing Based SNARKS	150
7.2.2	Succinct NIZK	151
	Common Reference String Generation	152
	Groth16	152
8	Exercises and Solutions	160

Chapter 3

Arithmetics

3.1 Introduction

The goal of this chapter is to bring a reader who is starting out with nothing more than basic school-level algebra up to speed in in arithmetics. We start with a brief recapitulation of basic integer arithmetics like long division, the greatest common divisor and Euclidean division. After that, we introduce modular arithmetics as **the most important** skill to compute our pen-and-paper examples. We then introduce polynomials, compute their analogs to integer arithmetics and introduce the important concept of Lagrange interpolation.

Even though the terms and concepts in this chapter might not appear in literature on zero-knowledge proofs directly, understanding them is necessary to follow subsequent chapters introducing terms like **groups** or **fields**, which crop up very frequently in academic papers on the topic.

3.2 Integer Arithmetics

In a sense, integer arithmetics is at the heart of large parts of modern cryptography, because it provides the most basic tools for doing computations in those systems. Fortunately, most readers will probably remember integer arithmetics from school. It is, however, important that you can confidently apply those concepts to understand and execute computations in the many pen-and-paper examples that form an integral part of the MoonMath Manual. We will therefore recapitulate basic arithmetics concepts to refresh your memory and fill any knowledge gaps.

In what follows, we apply standard mathematical notations, and use the symbol \mathbb{Z} for the set of all **integers**: S: I think it'd be useful to explain the difference between $:=$ and $=$ as well. We have a table on this in the ZKAPs whitepaper.

M: Yeah maybe we use the more suggestive leftarrows \leftarrow ? If a table of symbols is unavoidable then ok, I find I super ugly, though

S: The table below is similar to what we have in the ZKAPs whitepaper. I think it's easier to read than a wall of text explaining the same things. We can make it more visually different (e.g. typesetting it in "dark mode", and probably move it earlier in the chapter.

Notation used in this chapter

Symbol	Meaning of Symbol	Example	Explanation
=	equals	$a = r$	a and r have the same value
:=	defining a variable	$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$	\mathbb{Z} is the set of integers
\in	from the set	$a \in \mathbb{Z}$	a is an integer

$$\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} \quad (3.1)$$

Integers are also known as **whole numbers**, that is, numbers that can be written without fractional parts. Examples of numbers that are **not** integers are $\frac{2}{3}$, 1.2 and -1280.006 .

If $a \in \mathbb{Z}$ is an integer, then $|a|$ stands for the **absolute value** of a , that is, the non-negative value of a without regard to its sign:

$$|4| = 4 \quad (3.2)$$

$$|-4| = 4 \quad (3.3)$$

add some more informal explanation of absolute value

In addition, we use the symbol \mathbb{N} for the set of all **counting numbers** (also called natural numbers). So whenever you see the symbol \mathbb{N} , think of the set of all non negative integers including the number 0:

$$\mathbb{N} := \{0, 1, 2, 3, \dots\} \quad (3.4)$$

Any number that is smaller than 0, that is, any number that has a minus sign, is not part of \mathbb{N} . All counting numbers are integers, but not the other way round. In other words, counting numbers are a subset of integers.

To make it easier to memorize new concepts and symbols, we might frequently link to definitions (See 3.1 for a definition of \mathbb{Z}) in the beginning, but as to many links render a text unreadable, we will assume the reader will become familiar with definitions as the text proceeds at which point we will not link them anymore.

Both sets \mathbb{N} and \mathbb{Z} have a notion of addition and multiplication defined on them. Most of us are probably able to do many integer computations in our head, but this gets more and more difficult as these increase in complexity. We will frequently invoke the SageMath system (2.7.1) for more complicated computations. One way to invoke the integer type in Sage is: **We haven't really talked about what a ring is at this point**

```
sage: ZZ # A sage notation for the integer type
Integer Ring
sage: NN # A sage notation for the counting number type
Non negative integer semiring
sage: ZZ(5) # Get an element from the Ring of integers
5
sage: ZZ(5) + ZZ(3)
8
sage: ZZ(5) * NN(3)
15
sage: ZZ.random_element(10**50)
61902477905204399784317350280236793711210996981837
```

add some more informal explanation of absolute value

We haven't really talked about what a ring is at this point

```

sage: ZZ(27713).str(2) # Binary string representation 13
110110001000001 14
sage: NN(27713).str(2) # Binary string representation 15
110110001000001 16
sage: ZZ(27713).str(16) # Hexadecimal string representation 17
6c41 18

```

One set of numbers that is of particular interest to us is **prime numbers**, which are counting numbers $p \in \mathbb{N}$ with $p \geq 2$, which are only divisible by themselves and by 1. All prime numbers apart from the number 2 are called **odd** (since even numbers greater than 2 are all divisible by 2, they are not prime numbers). We write \mathbb{P} for the set of all prime numbers and $\mathbb{P}_{\geq 3}$ for the set of all odd prime numbers. \mathbb{P} is infinite and can be ordered according to size, so that we can write them as follows:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, \dots \quad (3.5)$$

This is sequence A000040 in OEIS, the On-Line Encyclopedia of Integer Sequences. In particular, we can talk about small and large prime numbers.

As the **fundamental theorem of arithmetics** tells us, prime numbers are, in a certain sense, the basic building blocks from which all other natural numbers are composed. To see that, let $n \in \mathbb{N}_{\geq 2}$ be any natural number. Then there are always prime numbers $p_1, p_2, \dots, p_k \in \mathbb{P}$, such that

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k. \quad (3.6)$$

This representation is unique for each natural number (except for the order of the factors) and is called the **prime factorization** of n .

Example 1 (Prime Factorization). *To see what we mean by prime factorization of a number, let's look at the number $19214758032624000 \in \mathbb{N}$. To get its prime factors, we can successively divide it by all prime numbers in ascending order starting with 2:*

$$19214758032624000 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 17 \cdot 23 \cdot 43 \cdot 43 \cdot 47$$

We can double check our findings invoking Sage, which provides an algorithm to factor counting numbers:

```

sage: n = NN(19214758032624000) 19
sage: factor(n) 20
2^7 * 3^3 * 5^3 * 7 * 11 * 17^2 * 23 * 43^2 * 47 21

```

This computation reveals an important observation: Computing the factorization of an integer is computationally expensive, while the **reverse**, that is, computing the product of given a set of prime numbers, is fast. **MIRCO**: inverse process? Its not reversing something actually, but my english doesn't resolve to this level very well

From this, an important question arises: How fast we can compute the prime factorization of a natural number? This is the famous **factorization problem** and, as far as we know, there is no method on a classical **Turing machine** that is able to compute this representation in **polynomial time**. The fastest algorithm known today run **sub-exponentially**, with $\mathcal{O}((1 + \varepsilon)^n)$ and some $\varepsilon > 0$.

It follows that ~~number factorization \Leftrightarrow prime number multiplication is an example of a~~ so-called **one-way function**: Something that is easy to compute in one direction, but hard to

What's the significance of this distinction?

reverse

Turing machine

polynomial time

sub-exponentially with $\mathcal{O}((1 + \varepsilon)^n)$ and

compute in the other direction. **The existence of one-way functions is a basic cryptographic assumptions that the security of many crypto systems is based on.**

It should be pointed out, however, that the American mathematician Peter Williston Shor developed an algorithm in 1994 which can calculate the prime factor representation of a natural number in polynomial time on a quantum computer. The consequence of this is that cryptosystems, which are based on the time complexity of the prime factor problem, are unsafe as soon as practically usable quantum computers become available. *Add text along the lines of "this is the best we got for now" Possibly something on when we can reasonably expect quantum computers to become accessible/usable enough*

Add text

Exercise 1. What is the absolute value of the integers -123 , 27 and 0 ?

Exercise 2. Compute the factorization of 6469693230 and double check your results using Sage.

Exercise 3. Consider the following equation $4 \cdot x + 21 = 5$. Compute the set of all solutions for x under the following alternative assumptions:

1. The equation is defined over the type of natural numbers.
2. The equation is defined over the type of integers.

Exercise 4. Consider the following equation $2x^3 - x^2 - 2x = -1$. Compute the set of all solutions x under the following assumptions:

1. The equation is defined over the type of natural numbers.
2. The equation is defined over the type of integers.
3. The equation is defined over the type \mathbb{Q} of fractions.

 \mathbb{Q} of fractions

Euclidean Division Division in the usual sense is not defined for integers, as, for example, 7 divided by 3 will not be an integer again. However it is possible to divide any two integers with a remainder. So for example 7 divided by 3 is equal to 2 with a remainder of 1 , since $7 = 2 \cdot 3 + 1$.

Division in the usual sense is not defined for integers

Doing integer division like this is probably something many of us remember from school. It is usually called **Euclidean division**, or **division with a remainder**, and it is an essential technique to understand many concepts in this book. The precise definition is as follows:

Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ be two integers with $b \neq 0$. Then there is always another integer $m \in \mathbb{Z}$ and a counting number $r \in \mathbb{N}$, with $0 \leq r < |b|$ such that

$$a = m \cdot b + r \quad (3.7)$$

This decomposition of a given b is called **Euclidean division**, where a is called the **dividend**, b is called the **divisor**, m is called the **quotient** and r is called the **remainder**.

Notation and Symbols 1. Suppose that the numbers a, b, m and r satisfy equation (3.7). Then we often write

$$a \operatorname{div} b := m, \quad a \operatorname{mod} b := r \quad (3.8)$$

to describe the quotient and the remainder of the Euclidean division. We also say, that an integer a is divisible by another integer b if $a \operatorname{mod} b = 0$ holds. In this case we also write $b|a$.

So, in a nutshell Euclidean division is a process of dividing one integer by another in a way that produces a quotient and a non-negative remainder, the latter of which is smaller than the absolute value of the divisor. It can be shown, that both the quotient and the remainder always exist and are unique, as long as the dividend is different from 0.

A special situation occurs whenever the remainder is zero, because in this case the dividend is divisible by the divisor. Our notation $b|a$ reflects that.

Example 2. Applying Euclidean division and our previously defined notation 3.27 to the divisor -17 and the dividend 4, we get

$$-17 \operatorname{div} 4 = -5, \quad -17 \operatorname{mod} 4 = 3$$

because $-17 = -5 \cdot 4 + 3$ is the Euclidean division of -17 and 4 (the remainder is, by definition, a non-negative number). In this case 4 does not divide -17 , as the remainder is not zero. The truth value of the expression $4|-17$ therefore is FALSE. On the other hand, the truth value of $4|12$ is TRUE, since 4 divides 12, as $12 \operatorname{mod} 4 = 0$. We can invoke SageMath to do the computation for us. We get

```
sage: ZZ(-17) // ZZ(4) # Integer quotient      22
-5                                              23
sage: ZZ(-17) % ZZ(4) # remainder             24
3                                              25
sage: ZZ(4).divides(ZZ(-17)) # self divides other 26
False                                          27
sage: ZZ(4).divides(ZZ(12))                   28
True                                          29
```

Methods to compute Euclidean division for integers are called **integer division algorithms**. Probably the best known algorithm is the so-called **long division**, which most of us might have learned in school. (It should be noted, however, that there are faster methods like **Newton–Raphson division**.)

As long division is the standard method used for pen-&-paper division of multi-digit numbers expressed in decimal notation, the reader should become familiar with it as we use it throughout this book when we do simple pen-and-paper computations. However, instead of defining the algorithm formally, we rather give some examples that will hopefully make the process clear.

In a nutshell, the algorithm loops through the digits of the dividend from the left to right, subtracting the largest possible multiple of the divisor (at the digit level) at each stage; the multiples then become the digits of the quotient, and the remainder is the first digit of the dividend. [Add more explanation of how this works](#)

Example 3 (Integer Long Division). To give an example of integer long division algorithm, let's divide the integer $a = 143785$ by the number $b = 17$. Our goal is therefore to find solutions to equation 3.7, that is, we need to find the quotient $m \in \mathbb{Z}$ and the remainder $r \in \mathbb{N}$ such that $143785 = m \cdot 17 + r$. Using a notation that is mostly used in Commonwealth countries, we

Add more
explanation
of
how this
works

compute as follows

$$\begin{array}{r}
 8457 \\
 17 \overline{) 143785} \\
 \underline{136} \\
 77 \\
 \underline{68} \\
 98 \\
 \underline{85} \\
 135 \\
 \underline{119} \\
 16
 \end{array}
 \tag{3.9}$$

We therefore get $m = 8457$ as well as $r = 16$ and indeed we have $143785 = 8457 \cdot 17 + 16$, which we can double check invoking Sage:

```

sage: ZZ(143785).quo_rem(ZZ(17)) # Euclidean Division      30
      (8457, 16)                                           31
sage: ZZ(143785) == ZZ(8457)*ZZ(17) + ZZ(16) # check      32
True                                                       33

```

Exercise 5 (Integer Long Division). Find an $m \in \mathbb{Z}$ as well as an $r \in \mathbb{N}$ such that $a = m \cdot b + r$ holds for the following pairs $(a, b) = (27, 5)$, $(a, b) = (27, -5)$, $(a, b) = (127, 0)$, $(a, b) = (-1687, 11)$ and . In which cases are your solutions unique?

$$(a, b) = (0, 7)$$

Exercise 6 (Long Division Algorithm). Write an algorithm in *pseudocode* that computes integer long division, handling all edge cases properly.

pseudocode

The Extended Euclidean Algorithm One of the most critical parts in this book is modular arithmetics XXX and its application in the computations in so-called **finite fields**, as we explain in XXX. In **modular arithmetics**, it is sometimes possible to define **actual division** and **multiplicative inverses** of numbers, that is very different from inverses as we know them from other systems like **factional numbers**.

modular
arith-
metics

However, to actually compute those inverses, we have to get familiar with the so-called **extended Euclidean algorithm**. A few more terms are necessary to explain the concept: The **greatest common divisor** (GCD) of two nonzero integers a and b is the greatest non-zero counting number d such that d divides both a and b ; that is $d|a$ as well as $d|b$. We write $\gcd(a, b) := d$ for this number. In addition, two counting numbers are called **relative primes** or **coprimes**, if their greatest common divisor is 1.

actual
division

multiplicative
inverses

The extended Euclidean algorithm is a method to calculate the greatest common divisor of two counting numbers a and $b \in \mathbb{N}$, as well as two additional integers $s, t \in \mathbb{Z}$, such that the following equation holds:

factional
numbers

$$\gcd(a, b) = s \cdot a + t \cdot b \tag{3.10}$$

The following pseudocode shows in detail how to calculate these numbers with the extended Euclidean algorithm:

The algorithm is simple enough to be done effectively in pen-&-paper examples, where it is common to write it as a table where the rows represent the while-loop and the columns represent the values of the the array r , s and t with index k . The following example provides a simple execution:

Algorithm 1 Extended Euclidean Algorithm**Require:** $a, b \in \mathbb{N}$ with $a \geq b$ **procedure** EXT-EUCLID(a, b) $r_0 \leftarrow a$ $r_1 \leftarrow b$ $s_0 \leftarrow 1$ $s_1 \leftarrow 0$ $k \leftarrow 1$ **while** $r_k \neq 0$ **do** $q_k \leftarrow r_{k-1} \text{ div } r_k$ $r_{k+1} \leftarrow r_{k-1} - q_k \cdot r_k$ $s_{k+1} \leftarrow s_{k-1} - q_k \cdot s_k$ $k \leftarrow k + 1$ **end while****return** $\gcd(a, b) \leftarrow r_{k-1}$, $s \leftarrow s_{k-1}$ and $t := (r_{k-1} - s_{k-1} \cdot a) \text{ div } b$ **end procedure****Ensure:** $\gcd(a, b) = s \cdot a + t \cdot b$

Example 4. To illustrate the algorithm, let's apply it to the numbers $a = 12$ and $b = 5$. Since $12, 5 \in \mathbb{N}$ as well as $12 \geq 5$ all requirements are met and we compute

k	r_k	s_k	$t_k = (r_k - s_k \cdot a) \text{ div } b$
0	12	1	0
1	5	0	1
2	2	1	-2
3	1	-2	5

From this we can see that 12 and 5 are relatively prime (coprime), since their greatest common divisor is $\gcd(12, 5) = 1$ and that the equation $1 = (-2) \cdot 12 + 5 \cdot 5$ holds. We can also invoke sage to double check our findings:

```
sage: ZZ(12).xgcd(ZZ(5)) # (gcd(a, b), s, t)
(1, -2, 5)
```

34

35

Exercise 7 (Extended Euclidean Algorithm). Find integers $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = s \cdot a + t \cdot b$ holds for the following pairs $(a, b) = (45, 10)$, $(a, b) = (13, 11)$, $(a, b) = (13, 12)$. What pairs (a, b) are coprime?

Exercise 8 (Towards Prime fields). Let $n \in \mathbb{N}$ be a counting number and p a prime number, such that $n < p$. What is the greatest common divisor $\gcd(p, n)$?

Exercise 9. Find all numbers $k \in \mathbb{N}$ with $0 \leq k \leq 100$ such that $\gcd(100, k) = 5$.

Exercise 10. Show that $\gcd(n, m) = \gcd(n + m, m)$ for all $n, m \in \mathbb{N}$.

3.3 Modular arithmetic

In mathematics, **modular arithmetic** is a system of arithmetic for integers, where numbers "wrap around" when reaching a certain value, much like calculations on a clock wrap around

whenever the value exceeds the number 12. For example, if the clock shows that it is 11 o'clock, then 20 hours later it will be 7 o'clock, not 31 o'clock. The number 31 has no meaning on a normal clock that shows hours.

The number at which the wrap occurs is called the **modulus**. Modular arithmetics generalizes the clock example to arbitrary moduli and studies equations and phenomena that arise in this new kind of arithmetics. It is of central importance for understanding most modern crypto systems, in large parts because the **exponentiation function** has an inverse with respect to certain moduli that is hard to compute. In addition, we will see that it provides the foundation of what is called finite fields ().

Although modular arithmetic appears very different from ordinary integer arithmetic that we are all familiar with, we encourage the interested reader to work through the example and to discover that, **once they accept that this is a new kind of calculations, its actually not that hard**.

Congruency In what follows, let $n \in \mathbb{N}$ with $n \geq 2$ be a fixed counting number, that we will call the **modulus** of our modular arithmetics system. With such an n given, we can then group integers into classes, by saying that two integers are in the same class, whenever their Euclidean division 3.2 by n will give the same remainder. We then say that two numbers are **congruent** whenever they are in the same class.

Example 5. If we choose $n = 12$ as in our clock example, then the integers $-7, 5, 17$ and 29 are all congruent with respect to 12, since all of them have the remainder 5 if we **perform Euclidean division on them** by 12. In the picture of an analog 12-hour clock, starting at 5 o'clock, when we add 12 hours we are again at 5 o'clock, representing the number 17. On the other hand, when we subtract 12 hours, we are at 5 o'clock again, representing the number -7 .

We can formalize this intuition of what congruency should be into a proper definition utilizing Euclidean division (as explained previously in 3.2): Let $a, b \in \mathbb{Z}$ be two integers and $n \in \mathbb{N}$ a natural number. Then a and b are said to be **congruent with respect to the modulus n** , if and only if the following equation holds

$$a \bmod n = b \bmod n \quad (3.11)$$

If, on the other hand, two numbers are not congruent with respect to a given modulus n , we call them **incongruent** w.r.t. n .

A **congruency** is then nothing but an equation "up to congruency", which means that the equation only needs to hold if we take the modulus on both sides. In which case we write

$$a \equiv b \pmod{n} \quad (3.12)$$

Exercise 11. Which of the following pairs of numbers are congruent with respect to the modulus 13: $(5, 19), (13, 0), (-4, 9), (0, 0)$.

Exercise 12. Find all integers x , such that the congruency $x \equiv 4 \pmod{6}$ is satisfied.

Modular Arithmetics One particularly useful thing about congruencies is, that we can do calculations (arithmetics), much like we can with integer equations. That is, we can add or multiply numbers on both sides. The main difference is probably that the congruency $a \equiv b \pmod{n}$ is only equivalent to the congruency $k \cdot a \equiv k \cdot b \pmod{n}$ for some non zero integer $k \in \mathbb{Z}$, whenever k and the modulus n are coprime. The following list gives a set of useful rules:

Suppose that the congruencies $a_1 \equiv b_1 \pmod{n}$ as well as $a_2 \equiv b_2 \pmod{n}$ are satisfied for integers $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and that $k \in \mathbb{Z}$ is another integer. Then:

exponentiation
function

See XXX

once they
accept
that this
is a new
kind of
calcula-
tions, its
actually
not that
hard

perform
Euclidean
division
on them

- $a_1 + k \equiv b_1 + k \pmod{n}$ (compatibility with translation)
- $k \cdot a_1 \equiv k \cdot b_1 \pmod{n}$ (compatibility with scaling)
- $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ (compatibility with addition)
- $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n}$ (compatibility with multiplication)

Other rules, such as compatibility with subtraction and exponentiation, follow from the rules above. For example, compatibility with subtraction follows from compatibility with scaling by $k = -1$ and compatibility with addition.

Note that the previous rules are implications, not equivalences, which means that you can not necessarily reverse those rules. The following rules makes this precise:

- If $a_1 + k \equiv b_1 + k \pmod{n}$, then $a_1 \equiv b_1 \pmod{n}$
- If $k \cdot a_1 \equiv k \cdot b_1 \pmod{n}$ and k is coprime with n , then $a_1 \equiv b_1 \pmod{n}$
- If $k \cdot a_1 \equiv k \cdot b_1 \pmod{k \cdot n}$, then $a_1 \equiv b_1 \pmod{n}$

Another property of congruencies, not known in the traditional arithmetics of integers is the **Fermat's Little Theorem**. In simple words, it states that, in modular arithmetics, every number raised to the power of a prime number modulus is congruent to the number itself. Or, to be more precise, if $p \in \mathbb{P}$ is a prime number and $k \in \mathbb{Z}$ is an integer, then:

$$k^p \equiv k \pmod{p}, \quad (3.13)$$

If k is coprime to p , then we can divide both sides of this congruency by k and rewrite the expression into the equivalent form

$$k^{p-1} \equiv 1 \pmod{p} \quad (3.14)$$

We can use Sage to compute examples for both k being coprime and not coprime to p :

```

sage: ZZ(137).gcd(ZZ(64))
1
sage: ZZ(64)**ZZ(137) % ZZ(137) == ZZ(64) % ZZ(137)
True
sage: ZZ(64)**ZZ(137-1) % ZZ(137) == ZZ(1) % ZZ(137)
True
sage: ZZ(1918).gcd(ZZ(137))
137
sage: ZZ(1918)**ZZ(137) % ZZ(137) == ZZ(1918) % ZZ(137)
True
sage: ZZ(1918)**ZZ(137-1) % ZZ(137) == ZZ(1) % ZZ(137)
False

```

This Sage snippet should be described in more detail.

Now, since for the sake of readers who have never encountered modular arithmetics before, let's compute an example that contains most of the concepts described in this section:

Example 6. Assume that we choose the modulus 6 and that our task is to solve the following congruency for $x \in \mathbb{Z}$

$$7 \cdot (2x + 21) + 11 \equiv x - 102 \pmod{6}$$

As many rules for congruencies are more or less same as for integers *why integers?* **MIRCO:** *I think this is emergent. Congruencies work on integers*, we can proceed in a similar way as we would if we had an equation to solve. Since both sides of a congruency contain ordinary integers, we can rewrite the left side as follows: $7 \cdot (2x + 21) + 11 = 14x + 147 = 14x + 158$. We can therefore rewrite the congruency into the equivalent form

$$14x + 158 \equiv x - 102 \pmod{6}$$

In the next step we want to shift all instances of x to left and every other term to the right. So we apply the “compatibility with translation” rules two times. In a first step we choose $k = -x$ and in a second step we choose $k = -158$. Since “compatibility with translation” transforms a congruency into an equivalent form, the solution set will not change and we get

$$\begin{aligned} 14x + 158 &\equiv x - 102 \pmod{6} \Leftrightarrow \\ 14x - x + 158 - 158 &\equiv x - x - 102 - 158 \pmod{6} \Leftrightarrow \\ 13x &\equiv -260 \pmod{6} \end{aligned}$$

If our congruency would just be a normal integer equation, we would divide both sides by 13 to get $x = -20$ as our solution. However, in case of a congruency, we need to make sure that the modulus and the number we want to divide by are coprime first – only then will we get an equivalent expression. So we need to find the greatest common divisor $\gcd(13, 6)$. Since 13 is prime and 6 is not a multiple of 13, we know that $\gcd(13, 6) = 1$, so these numbers are indeed coprime. We therefore compute

$$13x \equiv -260 \pmod{6} \Leftrightarrow x \equiv -20 \pmod{6}$$

Our task is now to find all integers x , such that x is congruent to -20 with respect to the modulus 6. So we have to find all x such

$$x \bmod 6 = -20 \bmod 6$$

Since $-4 \cdot 6 + 4 = -20$ we know $-20 \bmod 6 = 4$ and hence we know that $x = 4$ is a solution to this congruency. However, 22 is another solution since $22 \bmod 6 = 4$ as well, and so is -20 . In fact, there are infinitely many solutions given by the set

$$\{\dots, -8, -2, 4, 10, 16, \dots\} = \{4 + k \cdot 6 \mid k \in \mathbb{Z}\}$$

Putting all this together, we have shown that the every x from the set $\{x = 4 + k \cdot 6 \mid k \in \mathbb{Z}\}$ is a solution to the congruency $7 \cdot (2x + 21) + 11 \equiv x - 102 \pmod{6}$. We double check for, say, $x = 4$ as well as $x = 14 + 12 \cdot 6 = 86$ using sage:

```
sage: (ZZ(7) * (ZZ(2) * ZZ(4) + ZZ(21)) + ZZ(11)) % ZZ(6) == (ZZ 48
(4) - ZZ(102)) % ZZ(6)
True 49
sage: (ZZ(7) * (ZZ(2) * ZZ(76) + ZZ(21)) + ZZ(11)) % ZZ(6) == ( 50
ZZ(76) - ZZ(102)) % ZZ(6)
True 51
```

Readers who had not been familiar with modular arithmetics until now and who might be discouraged by how complicated modular arithmetics seems at this point, should keep two things in mind. First, computing congruencies in modular arithmetics is not really more complicated than computations in more familiar number systems (e.g. fractional numbers), it is just

a matter of getting used to it. Second, the theory of **prime fields** (and more general **residue class rings**) takes a different view on modular arithmetics with the attempt to simplify matters. In other words, once we understand prime field arithmetics, things become conceptually cleaner and more easy to compute.

prime
fieldsresidue
class rings

Exercise 13. Choose the modulus 13 and find all solutions $x \in \mathbb{Z}$ to the following congruency $5x + 4 \equiv 28 + 2x \pmod{13}$

Exercise 14. Choose the modulus 23 and find all solutions $x \in \mathbb{Z}$ to the following congruency $69x \equiv 5 \pmod{23}$

Exercise 15. Choose the modulus 23 and find all solutions $x \in \mathbb{Z}$ to the following congruency $69x \equiv 46 \pmod{23}$

The Chinese Remainder Theorem We have seen how to solve congruencies in modular arithmetic. However, one question that remains is how to solve systems of congruencies with different moduli? The answer is given by the **Chinese remainder theorem**, which states that for any $k \in \mathbb{N}$ and coprime natural numbers $n_1, \dots, n_k \in \mathbb{N}$ as well as integers $a_1, \dots, a_k \in \mathbb{Z}$, the so-called **simultaneous congruency**

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\dots \\ x &\equiv a_k \pmod{n_k} \end{aligned} \tag{3.15}$$

has a solution, and all possible solutions of this congruence system are congruent modulo the product $N = n_1 \cdot \dots \cdot n_k$.¹ In fact, the following algorithm computes the solution set: **Algorithm sometimes floated to the next page, check this for final version**

Algorithm
sometimes
floated
to the
next page,
check this
for final
version

Algorithm 2 Chinese Remainder Theorem

Require: $n_0, \dots, n_{k-1} \in \mathbb{N}$ coprime

procedure CONGRUENCY-SYSTEMS-SOLVER($k, a_0, \dots, a_{k-1}, n_0, \dots, n_{k-1}$)

$N \leftarrow n_0 \cdot \dots \cdot n_{k-1}$

while $j < k$ **do**

$N_j \leftarrow N / n_j$

$(_, s_j, t_j) \leftarrow \text{EXT-EUCLID}(N_j, n_j)$

$$\triangleright 1 = s_j \cdot N_j + t_j \cdot n_j$$

end while

$x' \leftarrow \sum_{j=0}^{k-1} a_j \cdot s_j \cdot N_j$

$x \leftarrow x' \bmod N$

return $\{x + m \cdot N \mid m \in \mathbb{Z}\}$

end procedure

Ensure: $\{x + m \cdot N \mid m \in \mathbb{Z}\}$ is the complete solution set to 3.15.

¹This is the classical Chinese remainder theorem as it was already known in ancient China. Under certain circumstances, the theorem can be extended to non-coprime moduli n_1, \dots, n_k but this is beyond the scope of this book. Interested readers should consult XXX [add references](#)

Example 7. *To illustrate how to solve simultaneous congruences using the Chinese remainder theorem, let's look at the following system of congruencies:*

$$\begin{aligned}x &\equiv 4 \pmod{7} \\x &\equiv 1 \pmod{3} \\x &\equiv 3 \pmod{5} \\x &\equiv 0 \pmod{11}\end{aligned}$$

Clearly all moduli are coprime and we have $N = 7 \cdot 3 \cdot 5 \cdot 11 = 1155$, as well as $N_1 = 165$, $N_2 = 385$, $N_3 = 231$ and $N_4 = 105$. From this we calculate with the extended Euclidean algorithm

$$\begin{aligned}1 &= 2 \cdot 165 + (-47) \cdot 7 \\1 &= 1 \cdot 385 + (-128) \cdot 3 \\1 &= 1 \cdot 231 + (-46) \cdot 5 \\1 &= 2 \cdot 105 + (-19) \cdot 11\end{aligned}$$

so we have $x = 4 \cdot 2 \cdot 165 + 1 \cdot 1 \cdot 385 + 3 \cdot 1 \cdot 231 + 0 \cdot 2 \cdot 105 = 2398$ as one solution. Because $2398 \bmod 1155 = 88$ the set of all solutions is $\{\dots, -2222, -1067, 88, 1243, 2398, \dots\}$. In particular, there are infinitely many different solutions. We can invoke Sage's computation of the Chinese Remainder Theorem (CRT) to double check our findings:

```
sage: CRT_list([4, 1, 3, 0], [7, 3, 5, 11])
88
```

52

53

As we have seen in various examples before, computing congruencies can be cumbersome and solution sets are large in general. It is therefore advantageous to find some kind of simplification for modular arithmetic.

Fortunately, this is possible and relatively straightforward once we consider all integers that have the same remainder with respect to a given modulus n in Euclidean division to be equivalent. Then we can go a step further, and identify each set of numbers with equal remainder with that remainder and call it a **remainder class** or **residue class** in modulo n arithmetics.

It then follows from the properties of Euclidean division that there are exactly n different remainder classes for every modulus n and that integer addition and multiplication can be projected to a new kind of addition and multiplication on those classes.

Roughly speaking, the new rules for addition and multiplication are then computed by taking any element of the first equivalence class and some element of the second, then add or multiply them in the usual way and see which equivalence class the result is contained in. The following example makes this abstract description more concrete:

Example 8 (Arithmetics modulo 6). *Choosing the modulus $n = 6$, we have six equivalence classes of integers which are congruent modulo 6 (they have the same remainder when divided by 6) and when we identify each of those remainder classes with the remainder, we get the following identification:*

$$\begin{aligned}0 &:= \{\dots, -6, 0, 6, 12, \dots\} \\1 &:= \{\dots, -5, 1, 7, 13, \dots\} \\2 &:= \{\dots, -4, 2, 8, 14, \dots\} \\3 &:= \{\dots, -3, 3, 9, 15, \dots\} \\4 &:= \{\dots, -2, 4, 10, 16, \dots\} \\5 &:= \{\dots, -1, 5, 11, 17, \dots\}\end{aligned}$$

Now to compute the addition of those equivalence classes, say $2 + 5$, one chooses arbitrary elements from both sets, say 14 and -1 , adds those numbers in the usual way and then looks at the equivalence class of the result.

So we get $14 + (-1) = 13$, and 13 is in the equivalence class (of) 1. Hence we find that $2 + 5 = 1$ in modular 6 arithmetics, which is a more readable way to write the congruency $2 + 5 \equiv 1 \pmod{6}$.

Applying the same reasoning to all equivalence classes, addition and multiplication can be transferred to equivalence classes. The results for modulus 6 arithmetics are summarized in the following addition and multiplication tables:

+	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

·	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	2	3	2	1

This way, we have defined a new arithmetic system that contains just 6 numbers and comes with its own definition of addition and multiplication. It is called **modular 6 arithmetics** and written as \mathbb{Z}_6 .

To see why such an identification of a congruency class with its remainder is useful and actually simplifies congruency computations a lot, let's go back to the congruency from example 6 again:

$$7 \cdot (2x + 21) + 11 \equiv x - 102 \pmod{6} \quad (3.16)$$

As shown in example 6, the arithmetics of congruencies can deviate from ordinary arithmetics: For example, division needs to check whether the modulus and the dividend are co-primes, and solutions are not unique in general.

We can rewrite this congruency as an **equation** over our new arithmetic type \mathbb{Z}_6 by **projecting onto the remainder classes**. In particular, since $7 \bmod 6 = 1$, $21 \bmod 6 = 3$, $11 \bmod 6 = 5$ and $102 \bmod 6 = 0$ we have

$$7 \cdot (2x + 21) + 11 \equiv x - 102 \pmod{6} \text{ over } \mathbb{Z} \\ \Leftrightarrow 1 \cdot (2x + 3) + 5 = x \text{ over } \mathbb{Z}_6$$

We can use the multiplication and addition table above to solve the equation on the right like we would solve normal integer equations: *Add a number and title to the tables*

$$\begin{aligned} 1 \cdot (2x + 3) + 5 &= x \\ 2x + 3 + 5 &= x && \# \text{ addition-table: } 3 + 5 = 2 \\ 2x + 2 &= x && \# \text{ add 4 and } -x \text{ on both sides} \\ 2x + 2 + 4 - x &= x + 4 - x && \# \text{ addition-table: } 2 + 4 = 0 \\ x &= 4 \end{aligned}$$

Add a number and title to the tables

So we see that, despite the somewhat unfamiliar rules of addition and multiplication, solving congruencies this way is very similar to solving normal equations. And, indeed, the solution set is identical to the solution set of the original congruency, since 4 is identified with the set $\{4 + 6 \cdot k \mid k \in \mathbb{Z}\}$.

We can invoke Sage to do computations in our modular 6 arithmetics type. This is particularly useful to double-check our computations:

<code>sage: Z6 = Integers(6)</code>	54
<code>sage: Z6(2) + Z6(5)</code>	55
<code>1</code>	56
<code>sage: Z6(7) * (Z6(2) * Z6(4) + Z6(21)) + Z6(11) == Z6(4) - Z6(102)</code>	57
<code>True</code>	58

Jargon 1 (k -bit modulus). In cryptographic papers, we can sometimes read phrases like “[...] using a 4096-bit modulus”. This means that the underlying modulus n of the modular arithmetic used in the system has a binary representation with a length of 4096 bits. In contrast, the number 6 has the binary representation 110 and hence our example 8 describes a 3-bit modulus arithmetics system.

Exercise 16. Let a, b, k be integers, such that $a \equiv b \pmod{n}$ holds. Show $a^k \equiv b^k \pmod{n}$.

Exercise 17. Let a, n be integers, such that a and n are not coprime. For which $b \in \mathbb{Z}$ does the congruency $a \cdot x \equiv b \pmod{n}$ have a solution x and how does the solution set look in that case?

Modular Inverses As we know, integers can be added, subtracted and multiplied so that the result is also an integer, but this is not true for the division of integers in general: for example, $3/2$ is not an integer anymore. To see why this is, from a more theoretical perspective, let us consider the definition of a multiplicative inverse first. When we have a set that has some kind of multiplication defined on it and we have a distinguished element of that set, that behaves neutrally with respect to that multiplication (doesn’t change anything when multiplied with any other element), then we can define **multiplicative inverses** in the following way:

Let S be our set that has some notion $a \cdot b$ of multiplication and a **neutral element** $1 \in S$, such that $1 \cdot a = a$ for all elements $a \in S$. Then a **multiplicative inverse** a^{-1} of an element $a \in S$ is defined as follows:

$$a \cdot a^{-1} = 1 \quad (3.17)$$

Informally speaking, the definition of a multiplicative inverse means that it “cancels” the original element to give 1 when they are multiplied.

Numbers that have multiplicative inverses are of particular interest, because they immediately lead to the definition of division by those numbers. In fact, if a is number such that the multiplicative inverse a^{-1} exists, then we define **division** by a simply as multiplication by the inverse:

$$\frac{b}{a} := b \cdot a^{-1} \quad (3.18)$$

Example 9. Consider the set of rational numbers, also known as fractions, \mathbb{Q} . For this set, the neutral element of multiplication is 1, since $1 \cdot a = a$ for all rational numbers. For example, $1 \cdot 4 = 4$, $1 \cdot \frac{1}{4} = \frac{1}{4}$, or $1 \cdot 0 = 0$ and so on.

Every rational number $a \neq 0$ has a multiplicative inverse, given by $\frac{1}{a}$. For example, the multiplicative inverse of 3 is $\frac{1}{3}$, since $3 \cdot \frac{1}{3} = 1$, the multiplicative inverse of $\frac{5}{7}$ is $\frac{7}{5}$, since $\frac{5}{7} \cdot \frac{7}{5} = 1$, and so on.

Example 10. Looking at the set \mathbb{Z} of integers, we see that with respect to multiplication the neutral element is the number 1 and we notice, that no integer $a \neq 1$ has a multiplicative inverse, since the equation $a \cdot x = 1$ has no integer solutions for $a \neq 1$.

The definition of multiplicative inverse works verbatim for addition as well. In the case of integers, the neutral element with respect to addition is 0, since $a + 0 = 0$ for all integers $a \in \mathbb{Z}$. The additive inverse always exist and is given by the negative number $-a$, since $a + (-1) = 0$.

(-1)
should
be (-a)?

Example 11. Looking at the set \mathbb{Z}_6 of residual classes modulo 6 from example 8, we can use the multiplication table to find multiplicative inverses. To do so, we look at the row of the element and then find the entry equal to 1. If such an entry exists, the element of that column is the multiplicative inverse. If, on the other hand, the row has no entry equal to 1, we know that the element has no multiplicative inverse.

For example in \mathbb{Z}_6 the multiplicative inverse of 5 is 5 itself, since $5 \cdot 5 = 1$. We can also see that 5 and 1 are the only elements that have multiplicative inverses in \mathbb{Z}_6 .

Now, since 5 has a multiplicative inverse modulo 6, it makes sense to “divide” by 5 in \mathbb{Z}_6 . For example

$$\frac{4}{5} = 4 \cdot 5^{-1} = 4 \cdot 5 = 2$$

From the last example, we can make the interesting observation that while 5 has no multiplicative inverse as an integer, it has a multiplicative inverse in modular 6 arithmetics.

The remaining question is to understand which elements have multiplicative inverses in modular arithmetics. The answer is that, in modular n arithmetics, a residue class r has a multiplicative inverse, if and only if n and r are coprime. Since $\text{ggt}(n, r) = 1$ in that case, we know from the extended Euclidean algorithm that there are numbers s and t , such that

$$1 = s \cdot n + t \cdot r \quad (3.19)$$

If we take the modulus n on both sides, the term $s \cdot n$ vanishes, which tells us that $t \bmod n$ is the multiplicative inverse of r in modular n arithmetics.

Example 12 (Multiplicative inverses in \mathbb{Z}_6). In the previous example, we looked up multiplicative inverses in \mathbb{Z}_6 from the lookup-table in Example 8. In real world examples, it is usually impossible to write down those lookup tables, as the modulus is way too large, and the sets occasionally contain more elements than there are atoms in the observable universe.

Now, trying to determine that $2 \in \mathbb{Z}_6$ has no multiplicative inverse in \mathbb{Z}_6 without using the lookup table, we immediately observe that 2 and 6 are not coprime, since their greatest common divisor is 2. It follows that equation 3.19 has no solutions s and t , which means that 2 has no multiplicative inverse in \mathbb{Z}_6 .

The same reasoning works for 3 and 4, as neither of these are coprime with 6. The case of 5 is different, since $\text{ggt}(6, 5) = 1$. To compute the multiplicative inverse of 5, we use the extended Euclidean algorithm and compute the following:

k	r_k	s_k	$t_k = (r_k - s_k \cdot a) \div b$
0	6	1	0
1	5	0	1
2	1	1	-1
3	0	.	.

We get $s = 1$ as well as $t = -1$ and have $1 = 1 \cdot 6 - 1 \cdot 5$. From this, it follows that $-1 \bmod 6 = 5$ is the multiplicative inverse of 5 in modular 6 arithmetics. We can double check using Sage:

```
sage: ZZ(6).xgcd(ZZ(5))
(1, 1, -1)
```

59
60

At this point, the attentive reader might notice that the situation where the modulus is a prime number is of particular interest, because we know from exercise XXX that in these cases all remainder classes must have modular inverses, since $\text{ggt}(r, n) = 1$ for prime n and $r < n$. In

fact, Fermat's little theorem provides a way to compute multiplicative inverses in this situation, since in case of a prime modulus p and $r < p$, **we have**

we have

$$\begin{aligned} r^p &\equiv r \pmod{p} \Leftrightarrow \\ r^{p-1} &\equiv 1 \pmod{p} \Leftrightarrow \\ r \cdot r^{p-2} &\equiv 1 \pmod{p} \end{aligned}$$

This tells us that the multiplicative inverse of a residue class r in modular p arithmetic is precisely r^{p-2} .

Example 13 (Modular 5 arithmetics). *To see the unique properties of modular arithmetics whenever the modulus is a prime number, we will replicate our findings from example 8, but this time for the prime modulus 5. For $n = 5$ we have five equivalence classes of integers which are congruent modulo 5. We write*

$$\begin{aligned} 0 &:= \{\dots, -5, 0, 5, 10, \dots\} \\ 1 &:= \{\dots, -4, 1, 6, 11, \dots\} \\ 2 &:= \{\dots, -3, 2, 7, 12, \dots\} \\ 3 &:= \{\dots, -2, 3, 8, 13, \dots\} \\ 4 &:= \{\dots, -1, 4, 9, 14, \dots\} \end{aligned}$$

Addition and multiplication can be transferred to the equivalence classes, in a way exactly parallel to Example 8. This results in the following addition and multiplication tables:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Calling the set of remainder classes in modular 5 arithmetics with this addition and multiplication \mathbb{F}_5 (for reasons we explain in more detail in XXX), we see some subtle but important differences to the situation in \mathbb{Z}_6 . In particular, we see that in the multiplication table, every remainder $r \neq 0$ has the entry 1 in its row and therefore has a multiplicative inverse. In addition, there are no non-zero elements such that their product is zero.

To use Fermat's little theorem in \mathbb{F}_5 for computing multiplicative inverses (instead of using the multiplication table), let's consider $3 \in \mathbb{F}_3$. We know that the multiplicative inverse is given by the remainder class that contains $3^{5-2} = 3^3 = 3 \cdot 3 \cdot 3 = 4 \cdot 3 = 2$. And indeed $3^{-1} = 2$, since $3 \cdot 2 = 1$ in \mathbb{F}_5 .

We can invoke Sage to do computations in our modular 5 arithmetics type to double-check our computations:

```
sage: Z5 = Integers(5) 61
sage: Z5(3) ** (5-2) 62
2 63
sage: Z5(3) ** (-1) 64
2 65
sage: Z5(3) ** (5-2) == Z5(3) ** (-1) 66
True 67
```


Example 14. To understand one of the principal differences between prime number modular arithmetics and non-prime number modular arithmetics, consider the linear equation $a \cdot x + b = 0$ defined over both types \mathbb{F}_5 and \mathbb{Z}_6 . Since in \mathbb{F}_5 every non zero element has a multiplicative inverse, we can always solve these types of equations in \mathbb{F}_5 , which is not true in \mathbb{Z}_6 . To see that, consider the equation $3x + 3 = 0$. In \mathbb{F}_5 we have the following:

$$\begin{array}{ll}
 3x + 3 = 0 & \# \text{ add 2 and on both sides} \\
 3x + 3 + 2 = 2 & \# \text{ addition-table: } 2 + 3 = 0 \\
 3x = 2 & \# \text{ divide by 3} \\
 2 \cdot (3x) = 2 \cdot 2 & \# \text{ multiplication-table: } 2 + 2 = 4 \\
 x = 4 &
 \end{array}$$

So in the case of our prime number modular arithmetics, we get the unique solution $x = 4$. Now consider \mathbb{Z}_6 :

$$\begin{array}{ll}
 3x + 3 = 0 & \# \text{ add 3 and on both sides} \\
 3x + 3 + 3 = 3 & \# \text{ addition-table: } 3 + 3 = 0 \\
 3x = 3 & \# \text{ no multiplicative inverse of 3 exists}
 \end{array}$$

So, in this case, we cannot solve the equation for x by dividing by 3. And, indeed, when we look at the multiplication table of \mathbb{Z}_6 (Example 8), we find that there are three solutions $x \in \{1, 3, 5\}$, such that $3x + 3 = 0$ holds true for all of them.

Exercise 18. Consider the modulus $n = 24$. Which of the integers 7, 1, 0, 805, -4255 have multiplicative inverses in modular 24 arithmetics? Compute the inverses, in case they exist.

Exercise 19. Find the set of all solutions to the congruency $17(2x + 5) - 4 \equiv 2x + 4 \pmod{5}$. Then project the congruency into \mathbb{F}_5 and solve the resulting equation in \mathbb{F}_5 . Compare the results.

Exercise 20. Find the set of all solutions to the congruency $17(2x + 5) - 4 \equiv 2x + 4 \pmod{6}$. Then project the congruency into \mathbb{Z}_6 and try to solve the resulting equation in \mathbb{Z}_6 .

3.4 Polynomial Arithmetics

A polynomial is an expression consisting of variables (also called indeterminates) and coefficients, that involves only the operations of addition, subtraction, multiplication, and non-negative integer exponentiation of variables. All coefficients of a polynomial must have the same type, e.g. being integers or fractions etc. To be more precise a *univariate polynomial* is an expression

$$P(x) := \sum_{j=0}^m a_j x^j = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0, \quad (3.20)$$

where x is called the **indeterminate**, each a_j is called a **coefficient**. If R is the type of the coefficients, then the set of all **univariate polynomials with coefficients in R** is written as $R[x]$. We often simply use **polynomial** instead of univariate polynomial, write $P(x) \in R[x]$ for a polynomial and denote the constant term as $P(0)$.

A polynomial is called the **zero polynomial** if all coefficients are zero and a polynomial is called the **one polynomial** if the constant term is 1 and all other coefficients are zero.

If an univariate polynomial $P(x) = \sum_{j=0}^m a_j x^j$ is given, that is not the zero polynomial, we call

$$\deg(P) := m \quad (3.21)$$

the *degree* of P and define the degree of the zero polynomial to be $-\infty$, where $-\infty$ (negative infinity) is a symbol with the property that $-\infty + m = -\infty$ for all counting numbers $m \in \mathbb{N}$. In addition, we write

$$\text{Lc}(P) := a_m \quad (3.22)$$

and call it the **leading coefficient** of the polynomial P . We can restrict the set $R[x]$ of **all** polynomials with coefficients in R , to the set of all such polynomials that have a degree that does not exceed a certain value. If m is the maximum degree allowed, we write $R_{\leq m}[x]$ for the set of all polynomials with a degree less than or equal to m .

Example 15 (Integer Polynomials). *The coefficients of a polynomial must all have the same type. The set of polynomials with integer coefficients is written as $\mathbb{Z}[x]$. Examples of such polynomials are:*

$P_1(x) = 2x^2 - 4x + 17$	# with $\deg(P_1) = 2$ and $\text{Lc}(P_1) = 2$
$P_2(x) = x^{23}$	# with $\deg(P_2) = 23$ and $\text{Lc}(P_2) = 1$
$P_3(x) = x$	# with $\deg(P_3) = 1$ and $\text{Lc}(P_3) = 1$
$P_4(x) = 174$	# with $\deg(P_4) = 0$ and $\text{Lc}(P_4) = 174$
$P_5(x) = 1$	# with $\deg(P_5) = 0$ and $\text{Lc}(P_5) = 1$
$P_6(x) = 0$	# with $\deg(P_5) = -\infty$ and $\text{Lc}(P_6) = 0$
$P_7(x) = (x-2)(x+3)(x-5)$	

In particular, every integer can be seen as an integer polynomial of degree zero. P_7 is a polynomial, because we can expand its definition into $P_7(x) = x^3 - 4x^2 - 11x + 30$, which is polynomial of degree 3 and leading coefficient 1. The following expressions are not integer polynomial

$$\begin{aligned} Q_1(x) &= 2x^2 + 4 + 3x^{-2} \\ Q_2(x) &= 0.5x^4 - 2x \\ Q_3(x) &= 1/x \end{aligned}$$

We can invoke Sage to do computations with polynomials. To do so, we have to specify the symbol for the indeterminate and the type for the coefficients. Note, however, that Sage defines the degree of the zero polynomial to be -1 .

```

sage: Zx = ZZ['x'] # integer polynomials with indeterminate x 68
sage: Zt.<t> = ZZ[] # integer polynomials with indeterminate t 69
sage: Zx 70
Univariate Polynomial Ring in x over Integer Ring 71
sage: Zt 72
Univariate Polynomial Ring in t over Integer Ring 73
sage: p1 = Zx([17, -4, 2]) 74
sage: p1 75
2*x^2 - 4*x + 17 76
sage: p1.degree() 77
2 78

```

```

sage: p1.leading_coefficient() 79
2 80
sage: p2 = Zt(t^23) 81
sage: p2 82
t^23 83
sage: p6 = Zx([0]) 84
sage: p6.degree() 85
-1 86

```

Example 16 (Polynomials over \mathbb{Z}_6). Recall our definition of the residue classes \mathbb{Z}_6 and their arithmetics as defined in Example 8. The set of all polynomials with indeterminate x and coefficients in \mathbb{Z}_6 is symbolized as $\mathbb{Z}_6[x]$. Example of polynomials from \mathbb{Z}_6 are:

$$\begin{aligned}
P_1(x) &= 2x^2 - 4x + 5 && \# \text{ with } \deg(P_1) = 2 \text{ and } \text{Lc}(P_1) = 2 \\
P_2(x) &= x^{23} && \# \text{ with } \deg(P_2) = 23 \text{ and } \text{Lc}(P_2) = 1 \\
P_3(x) &= x && \# \text{ with } \deg(P_3) = 1 \text{ and } \text{Lc}(P_3) = 1 \\
P_4(x) &= 3 && \# \text{ with } \deg(P_4) = 0 \text{ and } \text{Lc}(P_4) = 3 \\
P_5(x) &= 1 && \# \text{ with } \deg(P_5) = 0 \text{ and } \text{Lc}(P_5) = 1 \\
P_6(x) &= 0 && \# \text{ with } \deg(P_5) = -\infty \text{ and } \text{Lc}(P_6) = 0 \\
P_7(x) &= (x-2)(x+3)(x-5)
\end{aligned}$$

Just like in the previous example, P_7 is a polynomial. However, since we are working with coefficients from \mathbb{Z}_6 now the expansion of P_7 is computed differently, as we have to invoke addition and multiplication in \mathbb{Z}_6 as defined in XXX. We get:

$$\begin{aligned}
(x-2)(x+3)(x-5) &= (x+4)(x+3)(x+1) && \# \text{ additive inverses in } \mathbb{Z}_6 \\
&= (x^2 + 4x + 3x + 3 \cdot 4)(x+1) && \# \text{ bracket expansion} \\
&= (x^2 + 1x + 0)(x+1) && \# \text{ computation in } \mathbb{Z}_6 \\
&= (x^3 + x^2 + x^2 + x) && \# \text{ bracket expansion} \\
&= (x^3 + 2x^2 + x)
\end{aligned}$$

Again, we can use Sage to do computations with polynomials that have their coefficients in \mathbb{Z}_6 . To do so, we have to specify the symbol for the indeterminate and the type for the coefficients:

```

sage: Z6 = Integers(6) 87
sage: Z6x = Z6['x'] 88
sage: Z6x 89
Univariate Polynomial Ring in x over Ring of integers modulo 6 90
sage: p1 = Z6x([5, -4, 2]) 91
sage: p1 92
2*x^2 + 2*x + 5 93
sage: p1 = Z6x([17, -4, 2]) 94
sage: p1 95
2*x^2 + 2*x + 5 96
sage: Z6x(x-2)*Z6x(x+3)*Z6x(x-5) == Z6x(x^3 + 2*x^2 + x) 97
True 98

```

Given some element from the same type as the coefficients of a polynomial, the polynomial can be evaluated at that element, which means that we insert the given element for every occurrence of the indeterminate x in the polynomial expression.

To be more precise, let $P \in R[x]$, with $P(x) = \sum_{j=0}^m a_j x^j$ be a polynomial with a coefficient of type R and let $b \in R$ be an element of that type. Then the **evaluation** of P at b is given by

$$P(a) = \sum_{j=0}^m a_j b^j \quad (3.23)$$

Example 17. Consider the integer polynomials from example XXX again. To evaluate them at given points, we have to insert the point for all occurrences of x in the polynomial expression. Inserting arbitrary values from \mathbb{Z} , we get:

$$\begin{aligned} P_1(2) &= 2 \cdot 2^2 - 4 \cdot 2 + 17 = 17 \\ P_2(3) &= 3^{23} = 94143178827 \\ P_3(-4) &= -4 = -4 \\ P_4(15) &= 174 \\ P_5(0) &= 1 \\ P_6(1274) &= 0 \\ P_7(-6) &= (-6-2)(-6+3)(-6+5) = -264 \end{aligned}$$

Note, however, that is not possible to evaluate any of those polynomial on values of different type. For example, it is strictly speaking wrong to write $P_1(0.5)$, since 0.5 is not an integer. We can verify our computations using Sage:

rephrase

sage: <code>Zx = ZZ['x']</code>	99
sage: <code>p1 = Zx([17, -4, 2])</code>	100
sage: <code>p7 = Zx(x-2)*Zx(x+3)*Zx(x-5)</code>	101
sage: <code>p1(ZZ(2))</code>	102
17	103
sage: <code>p7(ZZ(-6)) == ZZ(-264)</code>	104
True	105

Example 18. Consider the polynomials with coefficients in \mathbb{Z}_6 from example XXX again. To evaluate them at given values from \mathbb{Z}_6 , we have to insert the point for all occurrences of x in the polynomial expression. We get:

$$\begin{aligned} P_1(2) &= 2 \cdot 2^2 - 4 \cdot 2 + 5 = 2 - 2 + 5 = 5 \\ P_2(3) &= 3^{23} = 3 \\ P_3(-4) &= P_3(2) = 2 \\ P_5(0) &= 1 \\ P_6(4) &= 0 \end{aligned}$$

sage: <code>Z6 = Integers(6)</code>	106
sage: <code>Z6x = Z6['x']</code>	107

<code>sage: p1 = Z6x([5, -4, 2])</code>	108
<code>sage: p1(Z6(2)) == Z6(5)</code>	109
<code>True</code>	110

Exercise 21. Compare both expansions of P_7 from $\mathbb{Z}[x]$ and from $\mathbb{Z}_6[x]$ in example XXX and example XXX, and consider the definition of \mathbb{Z}_6 as given in example XXX. Can you see how the definition of P_7 over \mathbb{Z} projects to the definition over \mathbb{Z}_6 if you consider the residue classes of \mathbb{Z}_6 ?

Polynomial Arithmetics Polynomials behave like integers in many ways. In particular, they can be added, subtracted and multiplied. In addition, they have their own notion of Euclidean division. Informally speaking, we can add two polynomials by simply adding the coefficients of the same index, and we can multiply them by applying the distributive property, that is, by multiplying every term of the left factor with every term of the right factor and adding the results together.

To be more precise let $\sum_{n=0}^{m_1} a_n x^n$ and $\sum_{n=0}^{m_2} b_n x^n$ be two polynomials from $R[x]$. Then the **sum** and the **product** of these polynomials is defined as follows:

$$\sum_{n=0}^{m_1} a_n x^n + \sum_{n=0}^{m_2} b_n x^n = \sum_{n=0}^{\max(\{m_1, m_2\})} (a_n + b_n) x^n \quad (3.24)$$

$$\left(\sum_{n=0}^{m_1} a_n x^n \right) \cdot \left(\sum_{n=0}^{m_2} b_n x^n \right) = \sum_{n=0}^{m_1+m_2} \sum_{i=0}^n a_i b_{n-i} x^n \quad (3.25)$$

A rule for polynomial subtraction can be deduced from these two rules by first multiplying the **subtrahend** with (the polynomial) -1 and then add the result to the **minuend**.

Regarding the definition of the degree of a polynomial, we see that the degree of the sum is always the maximum of the degrees of both summands, and the degree of the product is always the degree of the factors, since we defined $-\infty \cdot m = \infty$ for every integer $m \in \mathbb{Z}$. Using Sage's definition of degree, this would not hold, as the zero polynomials degree is -1 in Sage, which would violate this rule.

Example 19. To given an example of how polynomial arithmetics works, consider the following two integer polynomials $P, Q \in \mathbb{Z}[x]$ with $P(x) = 5x^2 - 4x + 2$ and $Q(x) = x^3 - 2x^2 + 5$. The sum of these two polynomials is computed by adding the coefficients of each term with equal exponent in x . This gives

$$\begin{aligned} (P+Q)(x) &= (0+1)x^3 + (5-2)x^2 + (-4+0)x + (2+5) \\ &= x^3 + 3x^2 - 4x + 7 \end{aligned}$$

The product of these two polynomials is computed by multiplication of each term in the first factor with each term in the second factor. We get

$$\begin{aligned} (P \cdot Q)(x) &= (5x^2 - 4x + 2) \cdot (x^3 - 2x^2 + 5) \\ &= (5x^5 - 10x^4 + 25x^2) + (-4x^4 + 8x^3 - 20x) + (2x^3 - 4x^2 + 10) \\ &= 5x^5 - 14x^4 + 10x^3 + 21x^2 - 20x + 10 \end{aligned}$$

```

sage: Zx = ZZ['x']
sage: P = Zx([2, -4, 5])
sage: Q = Zx([5, 0, -2, 1])
sage: P+Q == Zx(x^3 +3*x^2 -4*x +7)
True
sage: P*Q == Zx(5*x^5 -14*x^4 +10*x^3+21*x^2-20*x +10)
True

```

Example 20. Let us consider the polynomials of the previous example but interpreted in modular 6 arithmetics. So we consider $P, Q \in \mathbb{Z}_6[x]$ again with $P(x) = 5x^2 - 4x + 2$ and $Q(x) = x^3 - 2x^2 + 5$. This time we get

$$\begin{aligned}
 (P+Q)(x) &= (0+1)x^3 + (5-2)x^2 + (-4+0)x + (2+5) \\
 &= (0+1)x^3 + (5+4)x^2 + (2+0)x + (2+5) \\
 &= x^3 + 3x^2 + 2x + 1
 \end{aligned}$$

$$\begin{aligned}
 (P \cdot Q)(x) &= (5x^2 - 4x + 2) \cdot (x^3 - 2x^2 + 5) \\
 &= (5x^2 + 2x + 2) \cdot (x^3 + 4x^2 + 5) \\
 &= (5x^5 + 2x^4 + 1x^2) + (2x^4 + 2x^3 + 4x) + (2x^3 + 2x^2 + 4) \\
 &= 5x^5 + 4x^4 + 4x^3 + 3x^2 + 4x + 4
 \end{aligned}$$

```

sage: Z6x = Integers(6)['x']
sage: P = Z6x([2, -4, 5])
sage: Q = Z6x([5, 0, -2, 1])
sage: P+Q == Z6x(x^3 +3*x^2 +2*x +1)
True
sage: P*Q == Z6x(5*x^5 +4*x^4 +4*x^3+3*x^2+4*x +4)
True

```

Exercise 22. Compare the sum $P+Q$ and the product $P \cdot Q$ from the previous two examples XXX and XXX and consider the definition of \mathbb{Z}_6 as given in example XXX. How can we derive the computations in $\mathbb{Z}_6[x]$ from the computations in $\mathbb{Z}[x]$?

Euklidean Division The ring of polynomials shares a lot of properties with integers. In particular, the concept of Euclidean division and the algorithm of long division is also defined for polynomials. Recalling the Euclidean division of integers XXX, we know that, given two integers a and $b \neq 0$, there is always another integer m and a counting number r with $r < |b|$ such that $a = m \cdot b + r$ holds.

We can generalize this to polynomials whenever the leading coefficient of the dividend polynomial has a notion of multiplicative inverse. In fact, given two polynomials A and $B \neq 0$ from $R[x]$ such that $Lc(B)^{-1}$ exists in R , there exist two polynomials M (the quotient) and R (the remainder), such that

$$A = M \cdot B + R \quad (3.26)$$

and $\deg(R) < \deg(B)$. Similarly to integer Euclidean division, both M and R are uniquely defined by these relations.

$$A \operatorname{div} B := M, \quad A \operatorname{mod} B := R \quad (3.27)$$

Analogously to integers, methods to compute Euclidean division for polynomials are called **polynomial division algorithms**. Probably the best known algorithm is the so called **polynomial long division**.

Require: $A, B \in R[x]$ with $B \neq 0$, such that $Lc(B)^{-1}$ exists in R

$$\begin{array}{l} M \leftarrow 0 \\ R \leftarrow A \\ d \leftarrow \deg(B) \\ c \leftarrow Lc(B) \\ \mathbf{while} \deg(R) \geq d \mathbf{do} \\ \quad S := Lc(R) \cdot c^{-1} \cdot x^{\deg(R)-d} \\ \quad M \leftarrow M + S \\ \quad R \leftarrow R - S \cdot B \end{array}$$
end procedure

Example 21 (Polynomial Long Division). *To give an example of how the previous algorithm works, let us divide the integer polynomial $A(x) = x^5 + 2x^3 - 9 \in \mathbb{Z}[x]$ by the integer polynomial $B(x) = x^2 + 4x - 1 \in \mathbb{Z}[x]$. Since B is not the zero polynomial and the leading coefficient of B is 1, which is invertible as an integer, we can apply algorithm 3. Our goal is to find solutions to equation XXX, that is, we need to find the quotient polynomial $M \in \mathbb{Z}[x]$ and the remainder polynomial $R \in \mathbb{Z}[x]$ such that $x^5 + 2x^3 - 9 = M(x) \cdot (x^2 + 4x - 1) + R$. Using a notation that is mostly used in Commonwealth countries, we compute as follows:*

$$\begin{array}{r}
 X^3 - 4X^2 + 19X - 80 \\
 X^2 + 4X - 1) \overline{X^5 + 2X^3 - 9} \\
 \underline{-X^5 - 4X^4 + X^3} \\
 -4X^4 + 3X^3 \\
 \underline{4X^4 + 16X^3 - 4X^2} \\
 19X^3 - 4X^2 \\
 \underline{-19X^3 - 76X^2 + 19X} \\
 -80X^2 + 19X - 9 \\
 \underline{80X^2 + 320X - 80} \\
 339X - 89
 \end{array} \tag{3.28}$$

We therefore get $M(x) = x^3 - 4x^2 + 19x - 80$ as well as $R(x) = 339x - 89$ and indeed we have $x^5 + 2x^3 - 9 = (x^3 - 4x^2 + 19x - 80) \cdot (x^2 + 4x - 1) + (339x - 89)$, which we can double check invoking Sage:

```

sage: Zx = ZZ['x']
sage: A = Zx([-9, 0, 0, 2, 0, 1])
sage: B = Zx([-1, 4, 1])
sage: M = Zx([-80, 19, -4, 1])
sage: R = Zx([-89, 339])
sage: A == M*B + R
True

```

Example 22. In the previous example, polynomial division gave a non-trivial (non-vanishing, i.e. non-zero) remainder. Of special interest are divisions that don't give a remainder. Such divisors are called *factors of the dividend*.

For example, consider the integer polynomial P_7 from example XXX again. As we have shown, it can be written both as $x^3 - 4x^2 - 11x + 30$ and as $(x-2)(x+3)(x-5)$. From this, we can see that the polynomials $F_1(x) = (x-2)$, $F_2(x) = (x+3)$ and $F_3(x) = (x-5)$ are all factors of $x^3 - 4x^2 - 11x + 30$, since division of P_7 by any of these factors will result in a zero remainder.

Exercise 23. Consider the polynomial expressions $P(x) := -3x^4 + 4x^3 + 2x^2 + 4$ and $Q(x) = x^2 - 4x + 2$. Compute the Euclidean division of P by Q in the following types:

1. $P, Q \in \mathbb{Z}[x]$
2. $P, Q \in \mathbb{Z}_6[x]$
3. $P, Q \in \mathbb{F}_5[x]$

Now consider the result in $\mathbb{Z}[x]$ and in $\mathbb{Z}_6[x]$. How can we compute the result in $\mathbb{Z}_6[x]$ from the result in $\mathbb{Z}[x]$?

Exercise 24. Show that the polynomial $P(x) = 2x^4 - 3x + 4 \in \mathbb{F}_5[x]$ is a factor of the polynomial $Q(x) = x^7 + 4x^6 + 4x^5 + x^3 + 2x^2 + 2x + 3 \in \mathbb{F}_5[x]$, that is show $P|Q$. What is $Q \div P$?

Prime Factors Recall that the fundamental theorem of arithmetics XXX tells us that every number is the product of prime numbers. Something similar holds for polynomials, too.

The polynomial analog to a prime number is a so called an **irreducible polynomial**, which is defined as a polynomial that cannot be factored into the product of two non-constant polynomials using Euclidean division. Irreducible polynomials are for polynomials what prime numbers are for integer: They are the basic building blocks from which all other polynomials can be constructed. To be more precise, let $P \in R[x]$ be any polynomial. Then there are always irreducible polynomials $F_1, F_2, \dots, F_k \in R[x]$, such that

$$P = F_1 \cdot F_2 \cdot \dots \cdot F_k. \quad (3.29)$$

This representation is unique, except for permutations in the factors and is called the **prime factorization** of P .

Example 23. Consider the polynomial expression $P = x^2 - 3$. When we interpret P as an integer polynomial $P \in \mathbb{Z}[x]$, we find that this polynomial is irreducible, since any factorization other than $1 \cdot (x^2 - 3)$, must look like $(x - a)(x + a)$ for some integer a , but there is no integers a with $a^2 = 3$.

```
sage: Zx = ZZ['x'] 132
sage: p = Zx(x^2-3) 133
sage: p.roots() 134
[] 135
sage: p.factor() 136
x^2 - 3 137
```

On the other hand interpreting P as a polynomial $P \in \mathbb{Z}_6[x]$ in modulo 6 arithmetics, we see that P has two factors $F_1 = (x - 3)$ and $F_2 = (x + 3)$, since $(x - 3)(x + 3) = x^2 - 3x + 3 - 3 \cdot 3 = x^2 - 3$.

Finding prime factors of a polynomial is hard. As we have seen in example XXX, points where a polynomial evaluates to zero, i.e points $x_0 \in R$ with $P(x_0) = 0$ are of special interest, since it can be shown the polynomial $F(x) = (x - x_0)$ is always a factor of P . The converse, however, is not necessarily true, because a polynomial can have irreducible prime factors.

Points where a polynomial evaluates to zero are called the **roots** of the polynomial. To be more precise, let $P \in R[x]$ be a polynomial. Then the set of all roots of P is defined as

$$R_0(P) := \{x_0 \in R \mid P(x_0) = 0\} \quad (3.30)$$

Finding the roots of a polynomial is sometimes called **solving the polynomial**. It is a hard problem and has been the subject of much research throughout history. In fact, it is well known that, for polynomials of degree 5 or higher, there is, in general, no closed expression, from which the roots can be deduced.

It can be shown that if m is the degree of a polynomial P , then P can not have more than m roots. However, in general, polynomials can have less than m roots.

Example 24. Consider our integer polynomial $P_7(x) = x^3 - 4x^2 - 11x + 30$ from example XXX again. We know that its set of roots is given by $R_0(P_7) = \{-3, 2, 5\}$.

On the other hand, we know from example XXX that the integer polynomial $x^2 - 3$ is irreducible. It follows that it has no roots, since every root defines a prime factor.

Example 25. To give another example, consider the integer polynomial $P = x^7 + 3x^6 + 3x^5 + x^4 - x^3 - 3x^2 - 3x - 1$. We can invoke Sage to compute the roots and prime factors of P :

```
sage: Zx = ZZ['x'] 138
sage: p = Zx(x^7 + 3*x^6 + 3*x^5 + x^4 - x^3 - 3*x^2 - 3*x - 1) 139
sage: p.roots() 140
[(1, 1), (-1, 4)] 141
sage: p.factor() 142
(x - 1) * (x + 1)^4 * (x^2 + 1) 143
```

We see that P has the root 1 and that the associated prime factor $(x - 1)$ occurs once in P and that it has the root -1 , where the associated prime factor $(x + 1)$ occurs 4 times in P . This gives the prime factorization

$$P = (x - 1)(x + 1)^4(x^2 + 1)$$

Lange interpolation One particularly useful property of polynomials is that a polynomial of degree m is completely determined on $m + 1$ evaluation points. Seeing this from a different angle, we can (sometimes) uniquely derive a polynomial of degree m from a set

$$S = \{(x_0, y_0), (x_1, y_1), \dots, (x_m, y_m) \mid x_i \neq x_j \text{ for all indices } i \text{ and } j\} \quad (3.31)$$

This "few too many" property of polynomials is used in many places, like for example in erasure codes. It is also of importance in SNARKs and we therefore need to understand a method to actually compute a polynomial from a set of points.

what does this mean?

If the coefficients of the polynomial we want to find have a notion of multiplicative inverse, it is always possible to find such a polynomial. One method for this is called **Lagrange interpolation**. It works as follows: Given a set like 3.31, a polynomial P of degree $m + 1$ with $P(x_i) = y_i$ for all pairs (x_i, y_i) from S is given by the following algorithm:

Algorithm 4 Lagrange Interpolation

Require: R must have multiplicative inverses

Require: $S = \{(x_0, y_0), (x_1, y_1), \dots, (x_m, y_m) \mid x_i, y_i \in R, x_i \neq x_j \text{ for all indices } i \text{ and } j\}$

procedure LAGRANGE-INTERPOLATION(S)

for $j \in (0 \dots m)$ **do**

$$l_j(x) \leftarrow \prod_{i=0; i \neq j}^m \frac{x - x_i}{x_j - x_i} = \frac{(x - x_0)}{(x_j - x_0)} \dots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \dots \frac{(x - x_m)}{(x_j - x_m)}$$

end for

$$P \leftarrow \sum_{j=0}^m y_j \cdot l_j$$

return P

end procedure

Ensure: $P \in R[x]$ with $\deg(P) = m$

Ensure: $P(x_j) = y_j$ for all pairs $(x_j, y_j) \in S$

Example 26. Let us consider the set $S = \{(0, 4), (-2, 1), (2, 3)\}$. Our task is to compute a polynomial of degree 2 in $\mathbb{Q}[x]$ with fractional number coefficients. Since \mathbb{Q} has multiplicative inverses, we can use the Lagrange interpolation algorithm from 4, to compute the polynomial.

$$\begin{aligned} l_0(x) &= \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x + 2}{0 + 2} \cdot \frac{x - 2}{0 - 2} = -\frac{(x + 2)(x - 2)}{4} \\ &= -\frac{1}{4}(x^2 - 4) \\ l_1(x) &= \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x - 0}{-2 - 0} \cdot \frac{x - 2}{-2 - 2} = \frac{x(x - 2)}{8} \\ &= \frac{1}{8}(x^2 - 2x) \\ l_2(x) &= \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x - 0}{2 - 0} \cdot \frac{x + 2}{2 + 2} = \frac{x(x + 2)}{8} \\ &= \frac{1}{8}(x^2 + 2x) \\ P(x) &= 4 \cdot \left(-\frac{1}{4}(x^2 - 4)\right) + 1 \cdot \frac{1}{8}(x^2 - 2x) + 3 \cdot \frac{1}{8}(x^2 + 2x) \\ &= -x^2 + 4 + \frac{1}{8}x^2 - \frac{1}{4}x + \frac{3}{8}x^2 + \frac{3}{4}x \\ &= -\frac{1}{2}x^2 + \frac{1}{2}x + 4 \end{aligned}$$

And, indeed, evaluation of P on the x -values of S gives the correct points, since $P(0) = 4$, $P(-2) = 1$ and $P(2) = 3$.

Example 27. To give another example, more relevant to the topics of this book, let us consider the same set $S = \{(0, 4), (-2, 1), (2, 3)\}$ as in the previous example. This time, the task is to compute a polynomial $P \in \mathbb{F}_5[x]$ from this data. Since we know that multiplicative inverses exist in \mathbb{F}_5 , algorithm XXX applies and we can compute a unique polynomial of degree 2 in $\mathbb{F}_5[x]$ from S . We can use the lookup tables XXX for computation in \mathbb{F}_5 and get the following:

$$\begin{aligned}
 l_0(x) &= \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x + 2}{0 + 2} \cdot \frac{x - 2}{0 - 2} = \frac{(x + 2)(x - 2)}{-4} = \frac{(x + 2)(x + 3)}{1} \\
 &= x^2 + 1 \\
 l_1(x) &= \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x - 0}{-2 - 0} \cdot \frac{x - 2}{-2 - 2} = \frac{x}{3} \cdot \frac{x + 3}{1} = 2(x^2 + 3x) \\
 &= 2x^2 + x \\
 l_2(x) &= \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x - 0}{2 - 0} \cdot \frac{x + 2}{2 + 2} = \frac{x(x + 2)}{3} = 2(x^2 + 2x) \\
 &= 2x^2 + 4x \\
 P(x) &= 4 \cdot (x^2 + 1) + 1 \cdot (2x^2 + x) + 3 \cdot (2x^2 + 4x) \\
 &= 4x^2 + 4 + 2x^2 + x + x^2 + 2x \\
 &= 2x^2 + 3x + 4
 \end{aligned}$$

And, indeed, evaluation of P on the x -values of S gives the correct points, since $P(0) = 4$, $P(-2) = 1$ and $P(2) = 3$.

Exercise 25. Consider example XXX and example XXX again. Why is it not possible to apply algorithm XXX if we consider S as a set of integers, nor as a set in \mathbb{Z}_6 ?

Bibliography

Jens Groth. On the size of pairing-based non-interactive arguments. *IACR Cryptol. ePrint Arch.*, 2016:260, 2016. URL <http://eprint.iacr.org/2016/260>.

David Fifield. The equivalence of the computational diffie–hellman and discrete logarithm problems in certain groups, 2012. URL <https://web.stanford.edu/class/cs259c/finalpapers/dlp-cdh.pdf>.

Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In Joan Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91*, pages 129–140, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg. ISBN 978-3-540-46766-3. URL <https://fmouhart.epheme.re/Crypto-1617/TD08.pdf>.

Martin Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. Mimc: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. Cryptology ePrint Archive, Report 2016/492, 2016. <https://ia.cr/2016/492>.