Mathematical Cryptography

MATH 490

Start

August 26, 2024

Author

Paul Beggs
BeggsPA@Hendrix.edu

Instructor

Prof. Allie Ray, Ph.D.

End

December 2, 2024

TABLE OF CONTENTS

CHAPTER 1

THE REAL NUMBERS

1.1 Introduction

Before starting the course, it is important to understand that this document is for notetaking, and will therefore be a bit more informal than the actual textbook. The textbook is *An Introduction to Mathematical Cryptography* by Hoffstein, Pipher, and Silverman. The textbook can be located at this link

Definition Caesar Shift Cipher:

An encrypted text (by **shifting**), and you match it up with the alphabet. To encrypt, you write out a sentence, match it with a random assortment of letters by shifting the letters by a predetermined amount.

Definition Code:

Replace words / concepts. Example: Eagle has landed.

Definition Cipher:

Replacing characters or letters. Simply, replacing one letter for another.

Definition Scytale Cipher:

Used by the Spartans in the 5^{th} century B.C.. This is also known as a **Transposition Cipher**.

Definition Transposition Cipher:

Changed order, but the stayed the same.

Definition Plain Text:

Original message that is readable to humans. Abbreviated as [pt].

Definition Cipher Text:

Encrypted message that is unreadable to humans. Abbreviated as [ct].

Definition Encrypting:

From plain text to cipher text. The inverse of encrypting is decrypting; which is going from the Plain Text [pt] to the Cipher Text [ct].

Definition Key:

A secret number or word used in encoding and decoding using a certain algorithm. Example: Caesar shift: $A \to R$ rotated clockwise by 17

Definition Key Space:

The set of all keys, notated $\mathcal{K}$. The cardinality (amount of different keys) is notated with absolute value symbols. (E.g., for the Caesar shift, $|\mathcal{K}| = 26$ because there are 26 letters in the alphabet. Similarly, Scytale $|\mathcal{K}| =$ pt.)

Definition Brute Force Attack:

[During decryption] Trying all possible keys.

1.1.1 Goals of Cryptography

1. Provide confidentiality – You can't read the message.
2. Provide integrity – You can't change the message.
3. Provide authenticity – You can't forge the message.

Generally, these are the people and setting that will be used in examples: Alice and Bob are trying to communicate. Eve is trying to eavesdrop on the conversation.

1.1.2 Simple Substitution Ciphers (Mono-alphabetic Cipher)

Each letter can be replaced with any other letter. For example, you may have a key: $\{a, b, c, \ldots, z\} \to \{q, m, w, \ldots, t\}$. Its cardinality is $|\mathcal{K}| = 26!$.

Definition Cryptanalysis:

Process of decrypting without a key.

Definition Bigrams:

Two letters that are commonly placed together in language. For example, "Th", "is", or "He".

Definition Frequency Analysis:

English language patterns

Note that 13% of letters that are used in the alphabet are (in order from least to greatest): E, T, A, O, N. In brief, the longer the text, the more likely these letters will pop up.

1.2 Divisibility and Greatest Common Denominators

Can assume all the properties of $\mathbb{R}, \mathbb{Z},$ and $\mathbb{N}$. Note that $\mathbb{N}$ does not include 0.

Definition Divides:

Let a and b be integers with $b \neq 0$. We say that b *divides* a or that a is divisible by b, denoted by $b \mid a$, if there exists an integer n such that $a = nb$.

Example 1.1: Divisibility

Let $a = 100$ and $b = 4$. Is $b \mid a$?

Solution. Yes, because $100 = 4 \times 25$.

Example 1.2: Divisibility

Let $a = 100$ and $b = 8$. Is $b \mid a$?

Solution. No, because $100 = 8 \times 12 + 4$.

Proposition 1.4: Let $a, b, c \in \mathbb{Z}$:

1. If $a \mid b$ and $b \mid c$, then $a \mid c$.
2. If $a \mid b$ and $b \mid a$, then $a = \pm 2$.
3. If $a \mid b$ and $a \mid c$, then $a \mid (b + c) and a \mid (b - c)$.

Definition Greatest Common Divisor:

A *common divisor* of two integers a and b is a positive integer d that divides both of them. The *greatest common divisor* of a and b, denoted by $\gcd(a, b)$, is the largest positive integer such that $d \mid a$ and $d \mid b$.

This is less complicated than it sounds: we are simply factoring the integers and finding the largest common divisor between the two numbers.

Definition Divison with Remainder:

Let a, b be positive integers. Then we say that a *divided by* b gives a *quotient* q and a *remainder* r if $a = bq + r$ and $0 \leq r < b$.

Example 1.3: Division with Remainder

Let $a = 24$ and $b = 16$. Find the quotient and remainder.

Solution. $24 = 16(1) + 8$. Therefore, the quotient is 1 and the remainder is 8.

Example 1.4: Euclidean Algorithm

Compute $\gcd(2024, 748)$ using the Euclidean Algorithm.

Solution. Notice how the b and r values on each line become the new a and b values on the subsequent line:

$$\begin{aligned} 2024 &= 2(748) + 528 \\ 748 &= 1(528) + 220 \\ 528 &= 2(220) + 88 \\ 220 &= 2(88) + \boxed{44} \\ 88 &= 2(44) + 0 \end{aligned}$$

Therefore, the greatest common divisor is 44.

Theorem: Euclidean Algorithm

Let $a, b \in \mathbb{Z}^+$ with $a \geq b$. The following algorithm computes $\gcd(a, b)$ in a finite number of steps.

1. Let $r_0 = a, r_1 = b$;
2. Set $i = 1$;
3. Divide r_{i-1} by r_i to get quotient q_i and remainder r_{i+1};
4. If $r_{i+1} = 0$, stop, and $\gcd(a, b) = r_i$;
5. Otherwise, $r_{i+1} > 0$. Set $i = i + 1$, and go back to step 3.
6. Step 3 is executed at most $2\log_2(b) + 2$ times.

Example 1.5: Linear Combinations

Use Example 1.2 in determining the linear combination of 2024 and 748 that equals 44.

Solution. We let $a = 2024$ and $b = 748$. From the equation in Example 1.2, we read the first line:

$$528 = a - 2b.$$

We substitue this into the second line to get

$$b = (a - 2b) \cdot 1 + 220, \quad \text{so} \quad 220 = 2b - a.$$

We next substitute the expressions $528 = a - 2b$ and $220 = 2b - a$ into the third line to get

$$a - 2b = (-a + 3b) \cdot 2 + 88, \quad \text{so} \quad 88 = 3a - 8b.$$

Finally, we substitute the expressions $220 = -a + 3b$ and $88 = 3a - 8b$ into the fourth line to get

$$-a + 3b = (3a - 8b) \cdot 2 + 44, \quad \text{so} \quad 44 = 7a - 19b.$$

In other words,

$$-7 \cdot 2024 + 19 \cdot 748 = 44 = \gcd(2024, 748),$$

so we have found a way to write $\gcd(a, b)$ as a linear combination of a and b using integer coefficients.

Definition Relatively Prime:

Let a and b be *relatively prime* if $\gcd(a, b) = 1$. More generally, any equation $Au + Bv = \gcd(A, B)$ can be reduced to the case of relatively prime numbers by dividing both sides by

$\gcd(A,B)$. Thus, $\frac{A}{\gcd(A,B)}u + \frac{B}{\gcd(A,B)} = 1$ where $a = A/\gcd(A,B)$ and $b = B/\gcd(A,B)$ are relatively prime and satisfy $au + bv = 1$.

Theorem: Extended Euclidean Algorithm

Let $a, b \in \mathbb{Z}^+$ with $a \geq b$. Then the equation $\gcd(a,b) = ua + vb$ always has a solution in integers u and v. If u_0, v_0 is any one solution, then every solution has the form

$$u = u_0 + \frac{b \cdot t}{\gcd(a,b)} \text{ and } v = v_0 - \frac{a \cdot t}{\gcd(a,b)} \text{ for some integer } t \in \mathbb{Z}.$$

See Exercise 1.10 for a detailed example.

Example 1.6: Relative Prime

What are the relative prime numbers of 2024 and 748?

Solution. In Example 1.2, we found that the gcd of 2024 and 748 have greatest common divisor of 44 and satisfy the equation $-7 \cdot 2024 + 19 \cdot 748 = 44$. We can divide both sides by 44 to get $46u + 17v = 1$. Therefore, 46 and 17 are relatively prime and $u = -7$ and $v = 19$ are the coefficents of a linear combination of 46 and 17 that equals 1.

1.3 Modular Arithmetic

Definition Modular Arithmetic:

Let $m \geq 1$ be an integer. We say that the integers a and b are congruent modulo m if their difference is divisible by m: $m \mid (b-a)$ or $m \mid (a-b)$. Notated as $a = b \mod m$

By the definition of division, we can write this as $b - a = mk$ for some $k \in \mathbb{Z}$ and $b = mk + a$ for some $k \in \mathbb{Z}$. For example, $17 \mod 4 \equiv 1$. Or for another example, $-17 \mod 4 \equiv -1 \equiv 3$. For addition, you can go in two separate directions. For the first, sequence of operations, we could add the numbers inside of the parentheses and then take the mod of the number as demonstrated $(26 + 14) \mod 5 \equiv 40 \mod 5 \equiv 0$, or we could take the mod of both numbers inside the parentheses, demonstrated as $26 \mod +14 \mod 5 = 1 + 4 = 0$.

Proposition 1.13: Let $m \in \mathbb{Z}^+$

1. If $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$ then $a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m} \equiv a_2 \pmod{m} + b_2 \pmod{m}$. Also, $a_1 b_1 = a_2 b_2 \pmod{m} = a_2 \pmod{m} b_2 \pmod{m}$
2. Let $a \in \mathbb{Z}$. Then $ab \equiv 1 \pmod{m}$ for some $b \equiv \mathbb{Z} \iff \gcd(a,m) = 1$

Definition Ring:

We write $\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \ldots, m-1\}$ and call $\mathbb{Z}/m\mathbb{Z}$ the *ring of integers modulo* m. We add and multiplying them as integers and then dividing the result by m and taking the remainder in order to obtain an element in $\mathbb{Z}/m\mathbb{Z}$.

Note that we will be finding the more traditional rings that are brought up in Algebra. Thus, for a ring to be a ring, it must have the following properties:

1. **Additive Closure:** For any $a, b \in R$, the sum $a + b$ is also in R.
2. **Associativity of Addition:** For any $a, b, c \in R$, $(a + b) + c = a + (b + c)$.
3. **Commutativity of Addition:** For any $a, b \in R$, $a + b = b + a$.
4. **Additive Identity:** There exists an element $0 \in R$ such that for any $a \in R$, $a + 0 = a$.
5. **Additive Inverses:** For each $a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0$.
6. **Multiplicative Closure:** For any $a, b \in R$, the product $a \cdot b$ is also in R.
7. **Associativity of Multiplication:** For any $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
8. **Distributive Property:** For any $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

Example 1.7: $(\mathbb{Z}_6, \cdot)$

Find the ring of integers modulo 6 bound under multiplication.

Solution. Note that from the following table, 6 only has 2 inverses, 1 and 5. This is because in their respective column, there is a 1 in each row.

a	0	1	2	3	4	5
$a \cdot 0$	0	0	0	0	0	0
$a \cdot 1$	0	1	2	3	4	5
$a \cdot 2$	0	2	4	0	2	4
$a \cdot 3$	0	3	0	3	0	3
$a \cdot 4$	0	4	2	0	4	2
$a \cdot 5$	0	5	4	3	2	1

Definition Unit:

Recall from Proposition 1.13 that a has an inverse modulo m if and only if $\gcd(a, m) = 1$. Numbers that have inverses are called *units*. We denote the set of all units by

$$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^* &= \{a \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\} \\ &= \{a \in \mathbb{Z}/m\mathbb{Z} \mid \text{a has an inverse modulo } m\}\end{aligned}$$

Click this link to be teleported to section 2.5 where we discuss Groups which is relevant to us now.

Definition Euler's Phi Function:

The function $\varphi(m)$ defined by the rule

$$\varphi(m) = |\{0 \leq a < m \mid \gcd(a, m) = 1\}|$$

1.3.1 Modular Arithmetic and Shift Ciphers

Example 1.8: Shift Cipher

Let's say we have a shift cipher with a key of 3. We want to encrypt the message "HELLO". What is the encrypted message?

Solution. By shifting the letters by 3, we get "KHOOR". For the decryption, we would shift the letters by -3 to get the original message.

1.3.2 Fast Powering Algorithm

We can write the algorithm as follows:

1. Write the exponent in binary.
2. Compute the powers of the base in binary. For example,

$$\begin{aligned}k_0 &= a \pmod m \\ k_1 &= k_0^2 \pmod m = a^2 \pmod m \\ k_2 &= k_1^2 \pmod m = (a^2)^2 \pmod m \\ &\vdots \\ k_r &= k_{r-1}^2 \pmod m = (a^{2^{n-1}})^2 \pmod m\end{aligned}$$

3. Multiply the powers of the base that correspond to the 1s in the binary representation of the exponent. Compute $a_b \pmod m$ by using

$$a^b = a^{b_0 \cdot b_{12} + \cdots + b_r 2^r}$$

Example 1.9: Fast Powering Algorithm

Compute $3^{218} \pmod{1000}$.

Solution. The first step is to write 218 in binary: $218 = 11011010$. Then, we can write the powers of 3 in binary:

$$\begin{aligned}
3^1 &= 3 \pmod{1000} = 3 \\
3^2 &= 3^2 \pmod{1000} = 9 \\
3^4 &= 9^2 \pmod{1000} = 81 \\
3^8 &= 81^2 \pmod{1000} = 561 \\
3^{16} &= 561^2 \pmod{1000} = 721 \\
3^{32} &= 721^2 \pmod{1000} = 841 \\
3^{64} &= 841^2 \pmod{1000} = 281 \\
3^{128} &= 281^2 \pmod{1000} = 961
\end{aligned}$$

Now, we can calculate the value of 3^{218} by multiplying the values of 3^{128}, 3^{64}, 3^{16}, 3^8, and 3^2 together:

$$\begin{aligned}
3^{218} &= 3^{128} \times 3^{64} \times 3^{16} \times 3^8 \times 3^2 \\
&= 961 \times 281 \times 721 \times 561 \times 9 \\
&= 489 \pmod{1000}
\end{aligned}$$

1.4 Prime Numbers, Unique Factorization, and Finite Fields

Definition Prime Number:

A prime number is a positive integer greater than 1 whose only divisors are 1 and itself.

Proposition 1.19 Let p be a prime number with $a, b \in \mathbb{Z}$ such that $p \mid ab$. Then $p \mid a$ or $p \mid b$.

Theorem: Fundamental Theorem of Arithmetic

Let $a \geq 2$ be an integer. Then a can be factored as a product of prime numbers

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

Further, other than rearranging the order of the factors, this factorization is unique.

Proposition 1.21: Let p be prime. Then every non-zero element of $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse.

Put another way, $x \in \mathbb{Z}_p$ has a multiplicative inverse if and only if $\gcd(x, p) = 1$ because of Proposition 1.13.

Definition Field:

If p is prime, then $\mathbb{Z}/p\mathbb{Z}$ of integers modulo p with its addition, subtraction, multiplication, and division rules is a *field*. See the definition of Ring for more information on the properties of a field. (Note that a field is a type of ring, called a communicative ring.) We often notate fields as $\mathbb{F}_p$ and $\mathbb{F}_p^*$ as the group of units

---

1.5 Powers and Primitive Roots in Finite Fields

Theorem: Fermat's Little Theorem

Let p be a prime number and a be an integer. Then,

$$a^{p-1} \equiv \begin{cases} 1 \pmod{p} & \text{if } p \nmid a \\ 0 \pmod{p} & \text{if } p \mid a \end{cases}$$

Definition Order:

The *order* of an element $a \pmod{p}$ is the smallest exponent $k \geq 1$ such that $a^k \equiv 1 \pmod{p}$.

Example 1.10: Order

Find the order of 2 modulo 7.

Solution. $2^3 = 8 \pmod 7 = 1$. Thus, the order of 2 modulo 7 is 3.

Example 1.11: Order

Find the order of 5 modulo 7.

Solution. $5^6 = 15625 \pmod 7 = 1$. Thus, the order of 5 modulo 7 is 6.

Theorem: Primitive Root Theorem

Let p be a prime number. Then there exists an integer g such that there exists an $x \in \mathbb{F}_p^*$ whose powers give every element of $\mathbb{F}_p^*$, i.e.,

$$\mathbb{F}_p^* = \{1, g, g^2, g^3 \ldots, g^{p-2}\}.$$

Elements with this property are called the *primitive roots of* $\mathbb{F}_p$ or *generators of* $\mathbb{F}_p^*$. They are elements of order $p - 1$.

Example 1.12: Primitive Root

Find a primitive root modulo 7.

Solution. We can look to the Primitive Root Theorem to see how many primitive roots are 7 has. Because 7 is prime, we know that $\varphi = 6$. Thus, we know that 7 will have 6 primitive roots. Because there are 6 primitive roots in total, and $\mathbb{F}_7^*$ has 7 elements (including 0), we know that 1-6 will be the primitive roots.

1.6 Symmetric and Antisymmetric Ciphers

1.6.1 Symmetric Ciphers

Definition Symmetric Cipher:

A cipher that uses the same key for both encryption and decryption.

Review of Notation

- k implies key;
- $\mathcal{K}$ implies key space;
- m implies plaintext plain text;
- c implies cipher text;

- $\mathcal{M}$ implies all possible messages (message space);
- $\mathcal{C}$ implies all possible cipher texts (cipher space);
- Encryption is a function that is defined as:

$$e : \mathcal{K} \times \mathcal{M} \to \mathcal{C} \text{ such that } d(k(e(k, m))) = m$$

- Decryption is a function that is defined as:

$$d : \mathcal{K} \times \mathcal{C} \to \mathcal{M} \text{ such that } e(k, d(k, c)) = c$$

This brings us to what it means to be a *successful* cipher. Thus, we look to *Kerckhoff's Principle* which states that the security of a cipher should not depend on the secrecy of the algorithm, but rather on the secrecy of the key. Therefore, we have the following properties that are required for each cipher:

1. For all k and m, it is easy to computer $e_k(m)$. (Note that *easy* is relative to the computational power of the adversary. For this course, *easy* denotes a decryption time of less than a second.)
2. For all k and c, it is easy to compute $e_k(c)$.
3. Given one or more ciphertext, $c_1, \ldots c_n$, all encrypted with the same key, it is hard to compute any plaintext, m, such that $d_k(m)$ without knowing the key.

The next traits are desired, but not required:

4. Given one or more PT and CT pair, $(m_1, c_1), \ldots, (m_n, c_n)$ it is decrypt another CT not on this list without knowing the key. An example would be the *enigma cipher* from WW-II.
5. For any PT chosen by the adversary and their CT's, $(c_1, \ldots c_n)$, it should be hard to decrypt any CT not in this list.

Types of Attacks

- *Brute Force Attack*: Trying all possible keys.
- *Known PT Attack*: The adversary knows the plaintext and the corresponding ciphertext.
- *Chosen PT Attack*: The adversary chooses the plaintext and receives the corresponding ciphertext.

Types of Ciphers

1. Multiplication modulo m: $c = m \times k \pmod{m}$.
   - $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{F}_p^*$
   - $k \in \mathbb{F}_p^*$
   - $e_k(m) = k \cdot m \pmod{p}$
   - $d_k(m) = k^{-1} \cdot c \pmod{p}$
   - Example: $\mathbb{F}_{307}, k = 258, m = 444, e_{258}(444) = 258.444 \pmod{1307} = 843$. To find decrypt this message, Eve needs to iterate through $1307 - 1$ different keys. (Easy.)
2. Add (mod m): $c = m + k \pmod{m}$. (Caesar Cipher.)
3. Affine Cipher: Key $= (k_1, k_2) \in \mathbb{Z} \times \mathbb{Z}$.
4. Hill Cipher.
5. Vernam's One-time Pad.

1.6.2 Encoding Schemes

Definition Encoding Scheme:

An *encoding scheme* is a method of converting plaintext into a form that can be transmitted over a channel. An encoding scheme is assumed to be entirely public knowledge and used by everyone for the same purposes. An encryption scheme is designed to hide information from anyone who dopes not know the key. Thus, an encoding scheme, like an encryption scheme, consists of an encoding functions are public knowledge and should be fast and easy to compute.

This section will cover ASCII: We can take strings of 8 bits and convert them into a single character. From 0 to 255, and use them to represent the letters of the alphabet via $\texttt{a} = 00000000, \texttt{b} = 00000001, \texttt{c} = 00000010, \ldots, \texttt{z} = 00011001$. To distinguish between upper and lower case letters, we can use the first bit to represent the case.

CHAPTER 2

DISCRETE LOGARITHMS AND DIFFIE-HELLMAN

2.1 The Birth of Public Key Cryptography

Definition One-way Function:

A *one-way function* that is easy to computer, but whose inverse is difficult.

Definition Trap-door Function:

A *trap-door function* is a one-way function with an extra piece of information that makes f^{-1} easy.

2.2 Discrete Logarithm Problem (DLP)

Definition Discrete Logarithm Problem:

Let g be a primitive root for $\mathbb{F}_p$ and let h be a nonzero element of $\mathbb{F}_p$. The *Discrete Logarithm Problem* is the problem of finding an exponent x such that

$$g^x \equiv h \pmod{p}.$$

The number x is called the *discrete logarithm* of h to the base g and is denoted by $\log_g(h)$.

Remember the rules of logarithms:

$$\begin{aligned} \log_b(a \cdot c) &= \log_b(a) + \log_b(c) \\ \log_b(a^c) &= c \cdot \log_b(a) \\ \log_b(a/c) &= \log_b(a) - \log_b(c) \end{aligned}$$

What is the value of x such that $20^x = 21 \pmod{23}$ $\overset{\text{Brute-f}}{\Longrightarrow}$ $\log_{20} 21 = \boxed{7} \pmod{23}$. (Where 7 is from wolfram.)

Example 2.1: DLP

Find $\log_2(10) \pmod{11}$. In other words, find the value of x such that $2^x \equiv 10 \pmod{11}$.

Solution.

$$\begin{aligned} 2^1 &= 2 \pmod{11} \\ 2^2 &= 4 \pmod{11} \\ 2^3 &= 8 \pmod{11} \\ 2^4 &= 5 \pmod{11} \\ 2^5 &= 10 \pmod{11} \\ \log_2(10) &= \boxed{5} \pmod{11}. \end{aligned}$$

2.3 Diffie-Hellman Key Exchange

D-H gives a way for Alice and Bob to get a secret shared key in an unsecure environment (i.e., when Eve is listening). Now, we will follow the steps of D-H below:

1. Alice and Bob choose large prime p and primitive root g and make public $k_{\text{pub}} = (p, g)$.
2. Alice and Bob each pick their own secret integers, a, b such that $k_{\text{priv } A} = a$ and $k_{\text{priv } B} = b$. Compute $g^a \pmod{p} = A$ and $g^b \pmod{p} = B$.
3. Exchange a and b over an insecure channel.
   i. Note that Eve would have to solve DLP if she obtained a and b where $a = \log_g(A)$ and $b = \log_g(B)$.
   ii. Guidelines $\approx 2^{1000} g \approx p/2$.
4. Alice computes $B^a \pmod{p} = A'$ and Bob computes $A^b \pmod{p} = B'$.

Example 2.2: D-H

Let $p = 23$ and $g = 5$. Alice chooses $a = 6$ and Bob chooses $b = 15$. Compute the shared secret key.

Solution.

$$\begin{aligned} A &= 5^6 \pmod{23} = 8 \\ B &= 5^{15} \pmod{23} = 19 \\ A' &= 19^6 \pmod{23} = 2 \\ B' &= 8^{15} \pmod{23} = 2. \end{aligned}$$

Definition Diffie-Hellman Problem:

Let p be a prime number and g an integer. The *Diffie-Hellman Problem* is the problem of computing the value of $g^{ab} \pmod{p}$ from the known values of $g^a \pmod{p}$ and $g^b \pmod{p}$.

2.4 Elgamal Public Key Cryptosystem

Public parameter creation	
A trusted party chooses and publishes a large prime p and an element g modulo p of large (prime) order.	
Key creation	
Alice	**Bob**
Choose private key $1 \leq a \leq p-1$. Compute $A = g^a \pmod{p}$. Publish the public key A.	
Encryption	
	Choose plaintext m. Choose random element k. Use Alice's public key A to compute $c_1 = g^k \pmod{p}$ and $c_2 = mA^k \pmod{p}$. Send ciphertext c_1, c_2 to Alice.
Decryption	
Compute $(c_1^a)^{-1} \cdot c_2 \pmod{p}$. This quantity is equal to m.	

Table 2.1: Elgamal Key Creation, Encryption, and Decryption

Example 2.3: Elgamal

Let $p = 29$ and $g = 2$. Alice chooses $a = 12$ and Bob chooses $k = 5$ and wants to send secret message $m = 26$. Compute the shared secret key.

Solution. First, we need to calculate Alice's A and Bob's B. Then, we can calculate the ciphertexts c_1 and c_2:

$$\begin{aligned} A &= g^a \pmod{p} && = 2^{12} \pmod{29} = 7 \\ B &= g^k \pmod{p} && = 2^5 \pmod{29} = 3 \\ c_1 &= g^k \pmod{p} && = 2^5 \pmod{29} = 3 \\ c_2 &= m(A^k) \pmod{p} && = 26(7^5 \pmod{29}) = 10 \end{aligned}$$

Now, for Alice to decrypt the message, she must compute $(c_1^a)^{-1} \cdot c_2 \pmod{p}$:

$$(c_1^a)^{-1} \cdot c_2 \pmod{p} = (3^{12})^{-1} \cdot 10 \pmod{29}$$

The order of operations to compute this is as follows:

1. **Compute** $3^{12} \pmod{29} = 16$;
2. **Compute** $16^{-1} \pmod{29} = 20$;
3. **Finish by multiplying** $20 \cdot 10 \pmod{29} = 26$.

Be aware: You should only use this encryption scheme once. If you use it more than once, it is possible for an attacker to decrypt the message. For example, Eve knows $m_1(c_1, c_2) \rightarrow$ Eve finds A by keeping record of the first message, then by solving for d_2 such that c_1, d_2 (where c_1 is the *same* as the first message) and d_2 is the second message. Then, Eve can solve for m_2 by computing $(c_1^d)^{-1} \cdot d_2 \pmod{p}$.

2.5 An Overview of the Theory of Groups

Definition Group:

A set G along with a binary operation (closure) such that for all $a, b \in G$, $a \times b \in G$ (closure), and there exists an $e \in G$ such that $a \times e = a$ and $e \times a = a$ (identity), for all $a \in G$, there exists $a^{-1} \in G$ such that $a \times a^{-1} = a^{-1} \times a = e$ (inverse), and for all $a, b, c \in G$, $(a \times b) \times c = a \times (b \times c)$ (associativity)

For commutativity, for all $a, b \in G$, $a \times b = b \times a$. Some groups have this, some do not.

Example 2.4: Integer Addition as a Group

Lets check to see addition among the integers are a group: $(\mathbb{Z}, +)$

Solution.

1. True. Let $a, b \in \mathbb{Z}$ $a + b \in \mathbb{Z}$.
2. True. $e = 0 \in \mathbb{Z}$, $a + 0 = a$ and $0 + a = a$
3. True. For all $a \in \mathbb{Z}$, $a^{-1} = -a$ because $a + (-a) = 0 = -a + a$
4. True. For all $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$

Therefore, the additive property of the integers are a group. In fact, because $a+b=b+a$ $\mathbb{Z}$ are a commutative group (abelian group).

Example 2.5: Integer Multiplication

Lets check to see multiplication among the integers are a group: $(\mathbb{Z}, +)$

Solution.

1. True. Let $a, b \in \mathbb{Z}$ $ab \in \mathbb{Z}$.
2. True. $e = 1 \in \mathbb{Z}$, $a * 1 = a$ and $1 * a = a$
3. False. Counterexample: consider $2^{-1} = \frac{1}{2}$ because $2(\frac{1}{2}) = 1$ but $\frac{1}{2} \notin \mathbb{Z}$

2.7 A Collision Algorithm for the DLP

Recall that the DLP is the problem of finding x such that $g^x \equiv h \pmod{p}$ for a given value of h.

Remember that to brute force the DLP, it takes $P-1$ steps. Recall $g^{p-1} \pmod{p} \equiv 1$. In computational complexity, **we say that the DLP is $\mathcal{O}(P)$.**

Proposition 2.21:

(Shanks Baby-Step Giant-Step Algorithm) Computational time of $\mathcal{O}(\sqrt{P})$. Below is the algorithm:

1. Let $m = \lceil \sqrt{P} \rceil$.
2. Create two lists:
   (a) Baby steps: $\{g^0, g^1, g^2, \ldots, g^m\}$.
   (b) Giant steps: $\{h, h \cdot g^{-m}, h \cdot g^{-2m}, \ldots, h \cdot g^{-m^2}\}$.
3. Find a match between the two lists: $g^i \equiv hg^{-in} \pmod{p}$
4. $x = i + jm$ is a solution for $g^x \equiv h \pmod{p}$ (another way of saying "$x = i + jm$ is a solution for the DLP").

Example 2.6: Baby-step, Giant-step

Use the Baby-step, Giant-step algorithm to solve for $13^x \equiv 5 \pmod{47}$.

Solution.

1. Let $m = \lceil \sqrt{47} \rceil = 7$.
2. Create the two lists:
   (a) Baby steps: $\{13^0, 13^1, 13^2, \ldots, 13^6\} \pmod{47} \equiv \{1, 13, 28, 35, 32, 40, 3, 39\}$.
   (b) Giant steps: $\{5, 5{\cdot}13^{-7}, 5{\cdot}13^{-14}, \ldots, 5{\cdot}13^{-49}\} \pmod{47} \equiv \{5, 17, 39, 1, 48, 36, 19, 27\}$.
3. Find a match between the two lists: 39 and 39, or 1 and 1.
4. Substitute the following variables: $i = 7$, $j = 2$, $n = 7$ for the equation $x = i + jm \Rightarrow x = 7 + 2(7) = \boxed{21}$. So, $13^{21} \equiv 5 \pmod{47}$.

Example 2.7: (From Book) Baby-step, Giant-step

Solve the discrete logarithm problem with these values: $g = 9704, h = 13896, p = 17389$.

Solution. The number 9704 has order 1242 in $\mathbb{F}^*_{17389}$. Set $n = \lceil \sqrt{1242} \rceil = 36$ and $u = g^{-n} = 9704{-}36 = 2494$. Table 2.4 in the book lists the values of g^k and $h \cdot u^k$ for $k = 1, 2 \ldots$. From the table, we find the collision

$$9704^7 = 14567 = 13896 \cdot 2494^{32} \text{ in } \mathbb{F}_{17389}.$$

Using the fact that $2494 = 9704^{-36}$, we compute

$$13896 = 9704^7 \cdot 2494^{-32} = 9704^7 \cdot (9704^{36})^{32} = 9704^{1159} \text{ in } \mathbb{F}_{17389}.$$

Hence, $x = 1159$ solves the problem $9704^x = 13896$ in $\mathbb{F}_{17389}$.

2.8 Chinese Remainder Theorem (CRT)

Theorem: Chinese Remainder

Let $n_1, n_2, \ldots, n_k$ be pairwise relatively prime integers. This means that $\gcd(m_i, m_j) = 1$ *for all* $i \neq j$. Then, for any integers $a_1, a_2, \ldots, a_k$, the system of congruences

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

has a unique solution $c \pmod{n_1 n_2 \ldots n_k}$.

Example 2.8: CRT

Solve the following system of congruences:

$$x \equiv 6 \pmod 7$$
$$x \equiv 4 \pmod 8$$

Solution. Note that $x \equiv 6 \pmod 7$ means

$$\begin{aligned} x &= 7n + 6 \\ 7n + 6 &\equiv 4 \pmod 8 \\ 7n &\equiv 6 \pmod 8 \\ n &\equiv 6 \cdot 7^{-1} \pmod 8 \\ &\equiv 6 \cdot 7 \pmod 8 \\ &\equiv 2 \pmod 8, \end{aligned}$$

where $2 \pmod{8 = 8m + 2} = n$. We plug this back into the following:

$$\begin{aligned} x &= 7(8m + 2) + 6 \pmod{7 \cdot 8} \\ &= 56m + 14 + 6 \pmod{56} \\ &= 56m + 20 \pmod{56}. \end{aligned}$$

Note that $56m$ is a multiple of 56 and so it will always be equal to 0. Thus, $x = 20 \pmod{56}$.

In general, to solve for CRT such that $x \equiv a_1 \pmod{m_1} \ldots, x \equiv a_k \pmod{m_k}$ we follow the algorithm below:

1. Let $m = m_1 \cdot m_2 \cdots m_k$.
2. Take $n_i = \frac{m}{m_i}$.
3. Check to see if there is a solution, y_i. $y_i = n_i^{-1} \pmod{m_i}$. Note that the inverse exists because m_i and n_i are relatively prime.
4. Compute $x = a_1 n_1 y_1 + a_2 n_2 y_2 + \cdots + a_k n_k y_k \pmod m$.

Example 2.9: CRT with New Algorithm

Solve the following system of congruences: $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$ where $a_1 = 6, m_1 = 7, a_2 = 4, m_2 = 8$.

Solution.

1. Let $m = 7 \cdot 8 = 56$.
2. Compute $n_1 = 8$ and $n_2 = 7$.
3. Compute $y_1 = 8^{-1} \pmod 7 = 1$ and $y_2 = 7^{-1} \pmod 8 = 7$.
4. Compute

$$\begin{aligned} x &= 6 \cdot 8 \cdot 1 + 4 \cdot 7 \cdot 7 \pmod{56} \\ &= 48 + 196 \pmod{56} \\ &= 244 \pmod{56} \\ &= \boxed{20}. \end{aligned}$$

2.9 Pohlig-Hellman Algorithm

This algorithm is used to solve $g^x \equiv h \pmod p$ for p prime and g primitive root. This has computational time of $\mathcal{O}(\sqrt{p-1})$. Order of g is $p-1$ is composite. This is most efficient when $p-1$ has small prime factors. Look below for the algorithm:

1. Factor $p - 1 = n_1^{e_1} \cdot n_2^{e_2} \cdots n_k^{e_k}$. (Note that $\gcd(q_j, q_i) = 1 \; \forall i \neq j$.)
2. For each $1 \leq i \leq k$, let $m_i = \frac{p-1}{n_i^{e_i}}$.
3. Solve $g^{x_i} \equiv h^{m_i} \pmod p$ for x_i. (Note this DLP is easier because order of g_i is way less than the order of g.)
4. Use CRT to find x such that $x \equiv x_1 \pmod{q_1^{e+1}}, \ldots, x_i \pmod{n_i^{e_i}}$.

Example 2.10: Pohlig-Hellman Algorithm

Solve the following DLP: $7^x \equiv 12 \pmod{41}$.

Solution.

1. Factor $41 - 1 = 40 = 2^3 \cdot 5 = 8 \cdot 5$.
2. Find g_1: $g_1 = 7^{40/8} \pmod{41} = 7^5 \pmod{41} = 38$. Find h_1: $h_1 = 12^5 \pmod{41} = 3$.
3. We can brute force solve for x_1 up to 8 steps:

$$\begin{aligned} 38^{x_1} &\equiv 3 \pmod{41} \\ x_1 &= 5 \pmod 8. \end{aligned}$$

Continue for g_2 and h_2:

$$g_2 = 7^{40/5} \pmod{41} = 7^8 \pmod{41} = 37$$
$$h_2 = 12^8 \pmod{41} = 18.$$

Solve for x_2:

$$37^{x_2} \equiv 18 \pmod{41}$$
$$x_2 = 3 \pmod{5}.$$

4. Use CRT to solve for x:

$$x \equiv 5 \pmod{8}$$
$$x \equiv 3 \pmod{5}.$$

This gives us $M = 8 \cdot 5 = 40$ with $n_1 = 40/8 = 5$, $n_2 = 40/5 = 8$, and $y_1 \equiv 5^{-1} \pmod{8 = \equiv 5}$, $y_2 \equiv 8^{-1} \pmod{5} \equiv 2$. Now we can substitute and see that $x = 5 \cdot 5 \cdot 5 + 3 \cdot 8 \cdot 2 \pmod{40} = \boxed{13}$.

CHAPTER 3

INTEGER FACTORIZATION AND RSA

3.1 Euler's Totient Theorem

Remember FLT and DLP? Can we use FLT for non-prime moduli? No, FLT is only true for prime moduli: $2^5 \pmod 6 = 32$. Thus, we need to look to other ways of solving this problem for non-primes.

Theorem: Euler's Totient Theorem for phi

Let n be a positive integer and let a be an integer such that $\gcd(a, n) = 1$. Then,

$$a^{\varphi(n)} \equiv 1 \pmod n.$$

where $\varphi(N) = \#\{0 < x < N \mid \gcd(x, N) = 1\}$

Corollary 1: Euler's Totient Theorem for *phi*

If N is prime, $a^{\varphi(N)} \equiv 1 \pmod N$. For $\varphi(N)$, we can express it as $N - 1$ from FLT.

Proof. If N is prime, then $\gcd(a, N) = 1$. Thus, for all a, such that $0 < a < N$, $\gcd(a, N) = 1$. Thus, $\varphi(N) = N - 1$. □

Corollary 2: Euler's Totient Theorem for *phi*

If p, q are distinct primes, then

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq} \quad \text{for all } a \text{ such that } \gcd(a, pq) = 1.$$

From this, we can state that $N = pq$.

Proof. For this proof, we would show that $\varphi(pq) = \varphi(q) \cdot \varphi(p) = (p - 1)(q - 1)$. □

Example 3.1: ETT for *phi*

Find $a^x \pmod{15}$.

Solution. $15 = 3 \cdot 5$ (relatively prime); $\varphi(15) = 2 \cdot 4 = 8$. Thus, $a^8 \equiv 1 \pmod{15}$.

Theorem: Euler's Totient Theorem for pq

Let p and q be distinct primes and let

$$g = \gcd(p-1, q-1).$$

Then,

$$a^{(p-1)(q-1)/g} \equiv 1 \pmod{pq} \quad \text{for all } a \text{ such that } \gcd(a, pq) = 1.$$

In particular, if p and q are distinct primes, then

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq} \quad \text{for all } a \text{ such that } \gcd(a, pq) = 1.$$

Recall that for Diffie Hellman Elgamal we need to find $a^x \pmod{p}$. Now, for RSA, we will be solving $x^e \pmod{N}$ where $N = pq$.

Proposition 3.2:

Let p be prime and let e be defined as $\{e \in \mathbb{Z} \geq 1 \mid \gcd(e, p-q) = 1\}$. (Note this means that $e^{-1} \bmod p-1$ exists) Then, call $d = e^{-1}$ i.e, $d \equiv e^{-1} \pmod{p-1}$. Then, $x^e \equiv c \pmod{p}$ has the unique solution $x = c^d \pmod{p}$.

Example 3.2: RSA

Find x: $x^3 \equiv 2 \pmod{17}$.

Solution.

1. Check with $\gcd(3, 17-1) = \gcd(3, 16)$ and 17 is a prime number. Thus, we can use Proposition 3.2.
2. Let $d \cdot 3 \equiv 1 \pmod{16} \equiv d \equiv 3^{-1} \pmod{16} \equiv 11$ (Found with EEA)
3. Then, $x^3 \equiv 2 \pmod{17} \Rightarrow x \equiv 2^{11} \pmod{17} \equiv 8$.
4. To check: $8^3 = 512 \pmod{17} = 2$ ✓

Proposition 3.5:

Let $p \neq q$ be primes, and let e be defined as $\{e \in \mathbb{Z} \geq 1 \mid \gcd(e, p-q) = 1\}$ Thus, there exists a $d = e^{-1} \pmod{(p-1)(q-1)}$. Then, $x^e \equiv c \pmod{pq}$ has the unique solution $x \equiv c^d \pmod{pq}$.

Example 3.3: RSA

Solve $x^{169} \equiv 1000 \pmod{6887}$

Solution.

1. Check $\gcd(169, (70)(96)) = \gcd(169, 6720) = 1$ where 70 and 96 are from the prime factorization of 6887 such that $(71-1)(97-1)$ are from $(p-1)(q-1)$.
2. Solve for d such that $d169 \equiv \pmod{6720}$. Using EEA, we find that $d \equiv -1511 \pmod{6720} \equiv 5209$.
3. Solve $x \equiv 1000^{5209} \pmod{6887} = 4055$

Exercise 1.1

Build a cipher wheel as illustrated in Figure 1.1, but with an inner wheel that rotates, and use it to complete the following tasks.

(a) Encrypt the following plaintext using a rotation of 11 clockwise.

"A page of history is worth a volume of logic."

(b) Decrypt the following message, which was encrypted with a rotation of 7 clockwise.

`AOLYLHYLUVZLJYLAZILAALYAOHUAOLZLJYLALZAOHALCLYFIVKFNBLZZLZ`

Solution.

(a) `L ALRP ZQ STDEZCJ TD HZCES L GZWFXP ZQ WZRTN`

(b) THERE ARE NO SECRETS BETTER THAN THE SECRETES [sic] THAT EVERY BODY GUESSES
In the encrypted text, "Secrets" is `ZLJYLAZ`. Then, they use an incorrect spelling of the word, `ZLJYLALZ`, of which has an extra 'e' in it. That is what the "[sic]" is for.

Exercise 1.2

Decrypt each of the following Caesar encryptions by trying the various possible shifts until you obtain readable text.

(a) `LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBDVDWUHH`

(b) `UXENRBWXCUXENFQRLQJUCNABFQNWRCJUCNAJCRXWORWMB`

Solution.

(a) I THINK THAT I SHALL NEVER SEE A BILLBOARD LOVELY AS A TREE

(b) LOVE IS NOT LOVE WHICH ALTERS WHEN IT ALTERATION FINDS

Exercise 1.3

For this exercise, use the simple substitution table given in Table 1.11.

(a) Encrypt the plaintext message:

The gold is hidden in the garden

Solution.

(a) `IBX FEPA QL BQAAXW QW IBX FSVAXW`

Exercise 1.4

Each of the following messages has been encrypted using a simple substitution cipher. Decrypt them. For your convenience, we have given you a frequency table and a list of the most common bigrams that appear in the ciphertext. (If you do not want to recopy the ciphertexts by hand, they can be downloaded or printed from the web site listed in the preface.)

(a) "A Piratical Treasure"

```
JNRZR BNIGI BJRGZ IZLQR OTDNJ GRIHT USDKR ZZWLG OIBTM NRGJN
IJTZJ LZISJ NRSBL QVRSI ORIQT QDEKJ JNRQW GLOFN IJTZX QLFQL
WBIMJ ITQXT HHTBL KUHQL JZKMM LZRNT OBIMI EURLW BLQZJ GKBJT
QDIQS LWJNR OLGRI EZJGK ZRBGS MJLDG IMNZT OIHRK MOSOT QHIJL
QBRJN IJJNT ZFIZL WIZTO MURZM RBTRZ ZKBNN LFRVR GIZFL KUHIM
MRIGJ LJNRB GKHRT QJRUU RBJLW JNRZI TULGI EZLUK JRUST QZLUK
EURFT JNLKJ JNRXR S
```

Solution.

(a) THESE CHARACTERS AS ONE MIGHT READILY GUESS FORM A CIPHER THAT IS TO SAY THEY CONVEY A MEANING BUT THEN FROM WHAT IS KNOWN OF CAPTAIN KIDD I COULD NOT SUPPOSE HIM CAPABLE OF CONSTRUCTING ANY OF THE MORE ABSTRUSE CRYPTOGRAPHS I MADE UP MY MIND AT ONCE THAT THIS WAS OF A SIMPLE SPECIES SUCH HOW EVER AS WOULD APPEAR TO THE CRUDE INTELLECT OF THE SAILOR ABSOLUTELY INSOLUBLE WITHOUT THE KEY

Solver.

Exercise 1.5

Suppose that you have an alphabet of 26 letters.

(a) How many possible simple substitution ciphers are there?

(b) A letter in the alphabet is said to be fixed if the encryption of the letter is the letter itself. *Show an example of how the pieces work together*

Solution.

(a) 26!

(b) This is the formula used for solving for derangements (where n is the number of elements in the set, and $!n$ is the number of derangements [Definition: A permutation with no fixed points]): $!n = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$. From Wikipedia. For $n = 2$. We can run through the following:

(1) $i = 0$: $\frac{(-1)^0}{0!} = 1$

(2) $i = 1$: $\frac{(-1)^1}{1!} = -1$

(3) $i = 2$: $\frac{(-1)^2}{2!} = 0.5$

Sum them together: $1 - 1 + 0.5 = 0.5$. Now we can get !2:

$$!2 = 2! \times (1 - 1 + 0.5) = 2 \times 0.5 = 1$$

Exercise 1.6

Let $a, b, c \in Z$. Use the definition of divisibility to directly prove the following properties of divisibility. (This is Proposition 1.4.)

(a) If $a \mid b$ and $b \mid c$. Then $a \mid c$.

(b) If $a \mid b$ and $b \mid a$. Then $a = \pm b$.

(c) If $a \mid b$ and $a \mid c$. Then $a \mid (b + c)$ and $a \mid (b - c)$.

Solution.

(a) Let $a, b, c \in \mathbb{Z}$ such that $a \mid b$ and $b \mid c$. We know there exists an $n \in \mathbb{Z}$ such that $a \times n = b$. Similarly, $b \mid c$ means there exists an $k \in \mathbb{Z}$ such that $b \times k = c$. We

can use the commutative property to show that:

$$\begin{aligned} k(an) &= (b)k \\ ank &= bk \\ bk &= c \\ a(nk) &= c \\ a &\mid c \end{aligned}$$

(b) From the problem statement, we can intuitively ascertain that because both a, b divide each other, then it must be the case that they are the same number. Moreover, because the criteria for dividing is not pertinent to whether the quotient is negative or positive, this number can be positive or negative. Now that we have an idea of what we are trying to accomplish, we can begin the proof: Let $a, b \in \mathbb{Z}$ such that $a \mid b$ and $b \mid a$. We know there exists an $n \in \mathbb{Z}$ such that $a \times n = b$. Similarly, $b \mid a$ means there exists an $k \in \mathbb{Z}$ such that $b \times k = a$. Then, we can utilize substitution to get the following:

$$\begin{aligned} bk &= a \\ (an)k &= a \end{aligned}$$

From here, we know that because a is present on both sides of the equation, we should divide by a to simplify. Thus, consider the following two cases.

- **Case 1:** $a \neq 0$
  Since a is not zero, we can divide both sides by a to get $nk = 1$. Since, $n, k \in \mathbb{Z}$. We do not need to worry about fractional reciprocals. Instead, we know from the identity property of multiplication, that n, k must both be ± 1.
  - n, k **are both** $+1$**:** Then, $a = b \times 1$ and $b = a \times 1$. Which simplifies to $a = b$ in both cases.
  - n, k **are both** -1**:** Then, $a = b \times (-1)$ and $b = a \times (-1)$ Which simplifies to $a = -b$ in both cases.
- **Case 2:** $a = 0$
  If $a = 0$. Then $b = 0 \times n = 0$ and $0 = b \times k = 0$. Therefore, $a = b = 0$. And $a = \pm b$ is still true.

We have shown that in either case if $a \mid b$ and $b \mid a$. Then $a = \pm b$.

(c) Because a needs to be divisible by both b and c. We know that there must exist an $n, k \in \mathbb{Z}$ such that $b = an$ and $c = ak$. Our goal is to get to the form, $a \times$ some integer $= b + c$ and $a \times$ some integer $= b - c$ so we can use the definition of divides to help us out here. Therefore, let us consider both $b + c$ and $b - c$ in two separate cases:

- **Case 1:** $b + c$

$$b + c = (an) + (ak)$$
$$b + c = a(n + k)$$
$$a \mid (b + c)$$

- **Case 2:** $b - c$

$$b - c = (an) - (ak)$$
$$b - c = a(n - k)$$
$$a \mid (b - c)$$

We have shown that if $a \mid b$ and $a \mid c$. Then $a \mid (b + c)$ and $a \mid (b - c)$.

Exercise 1.7

Use a calculator and the method described in Remark 1.9 to compute the following quotients and remainders.

(a) 34787 divided by 353.

(b) 238792 divided by 7843.

Solution.

(a) $a = 34787$ and $b = 353$. Then $a/b \approx 98.54674220$. So $q = 98$ and $r = a - b \cdot q = 34787 - 353 \cdot 98 = 193$.

(b) $a = 238792$ and $b = 7843$. Then $a/b \approx 30.446512$. So $q = 30$ and $r = a - b \cdot q = 238792 - 7843 \cdot 30 = 3502$.

Exercise 1.9

Use the Euclidean algorithm to compute the following greatest common divisors.

(a) $\gcd(291, 252)$.

(b) $\gcd(16261, 85652)$.

Solution.

(a) $\gcd(291, 252)$

(1) $r_0 = 291$. $r_1 = 252$.

(2) $i = 1$.

(3) Divide r_0 by r_1 to get a quotient, q_1 and a remainder, r_2:

$$291/252 = 1 = q_1$$
$$291 - (252 \times 1) = 39 = r_2$$

(4) $r_2 \neq 0$. So, we continue.

(5) $i = 2 + 1 = 3$.

---

(3) Divide r_1 by r_2 to get quotient, q_2 and a remainder, r_3:

$$252/39 = 6 = q_2$$
$$252 - (39 \times 6) = 18 = r_3$$

(4) $r_3 \neq 0$. So, we continue.

(5) $i = 3 + 1 = 4$.

---

(3) Divide r_2 by r_3 to get quotient q_3 and a remainder, r_4:

$$39/18 = 2 = q_3$$
$$39 - (18 \times 2) = 3 = r_4$$

(4) $r_4 \neq 0$. So, we continue.

(5) $i = 3 + 1 = 5$.

---

(3) Divide r_3 by r_4 to get quotient q_4 and a remainder, r_5:

$$18/3 = 6 = q_4$$
$$18 - (3 \times 6) = 0 = r_5$$

(4) $r_4 = 0$. So, we stop.

We have found that the greatest common divisor is 3.

(b) *To cut back on paper, I am going to avoid reiterating the steps of 4 and 5. If there is a continuation in the enumeration process, then $r_i \neq 0$. And the process needs to continue*: $\gcd(16261, 85652) \Rightarrow \gcd(85652, 16261)$.

(1)

$$85652/16261 = 5 = q_1$$
$$85652 - (16261 \times 5) = 4347 = r_2$$

(2)

$$16261/4347 = 3 = q_2$$
$$16261 - (4347 \times 3) = 3220 = r_3$$

(3)

$$4347/3220 = 1 = q_3$$
$$4347 - (3220 \times 1) = 1127 = r_4$$

(4)

$$3220/1127 = 2 = q_4$$
$$3220 - (1127 \times 2) = 966 = r_5$$

(5)

$$1127/966 = 1 = q_5$$
$$1127 - (966 \times 1) = 161 = r_6$$

(6)

$$966/161 = 6 = q_6$$
$$966 - (161 \times 6) = 0 = r_7$$

We have found that $\gcd(85652, 16261) = 161$.

Exercise 1.10

For each of the $\gcd(a, b)$ values in Exercise 1.9, use the extended Euclidean algorithm (Theorem 1.11) to find integers u and v such that $au + bv = \gcd(a, b)$.

Solution.

(a) We need to solve for the various u_i and v_i. We will start at $i = 2$.

i	u_i	*Formula*	*Evaluation*	v_i	*Formula*	*Evaluation*
2	1	$u_0 - q_1 \times u_1$	$1 - 1 \times 0$	-1	$v_0 - q_1 \times v_1$	$0 - 1 \times 1$
3	-6	$u_1 - q_2 \times u_2$	$0 - 6 \times 1$	7	$v_1 - q_2 \times v_2$	$1 - 6 \times (-1)$
4	13	$u_2 - q_3 \times u_3$	$1 - 2 \times (-6)$	-15	$v_2 - q_3 \times v_3$	$-1 - 2 \times 7$

Thus, we can now fill out the table in full:

i	r_i	q_i	r_{i+1}	u_i	v_i
0	291	–	–	1	0
1	252	1	39	0	1
2	39	6	18	1	-1
3	18	2	3	-6	7
4	3	6	0	13	-15

Now, we need to solve: $au + bv = \gcd(a, b) \Rightarrow 291(13) + 252(-15) = 3$. 3 matches the gcd that we found in Exercise 1.9, so this is the correct solution.

(b)

i	r_i	q_i	r_{i+1}	u_i	v_i
0	85652	–	–	1	0
1	16261	5	4347	0	1
2	4347	3	3220	1	-5
3	3220	1	1127	-3	16
4	1127	2	966	4	-21
5	966	1	161	-11	58
6	161	6	0	15	-79

$85652(15) + 16261(-79) = 161$.

Exercise 1.11

Let a and b be positive integers.

(a) Suppose that there are integers u and v satisfying $au + bv = 1$. Prove that $\gcd(a, b) = 1$.

Proof. (a) Suppose there are integers a, b, u, v such that $av + bv = 1$. Assume $d \in \mathbb{Z}$ such that $d = \gcd(a, b)$. Since d divides both a and b by definition of common divisor, it must also divide av and bv by definition of divisibility. Moreover, because $au + bv = 1$ and d is a common divisor of both av and bv. It must also divide 1 by Proposition 1.4 (c). Then, the only positive integer that divides 1 is 1 itself, so it must be the case that $d = 1$. Therefore, since $d = 1$ and $\gcd(a, b) = d$. It follows that $\gcd(a, b) = 1$. □

Exercise 1.14

Let $m \geq 1$ be an integer and suppose that

$$a_1 \equiv a_2 \pmod{m} \text{ and } b_1 \equiv b_2 \pmod{m}.$$

Prove that

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m} \text{ and } a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}.$$

(This is Proposition 1.13(a).)

Proof. Let $m \geq 1$ be an integer and suppose that $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$. From the definition of modulo, we know the difference of $a_1 - a_2$ and $b_1 - b_2$ is divisible by m.

- **Addition:** We want to show that $a_1 + b_1 \equiv a_2 + b_2$. So, our goal is to achieve $m \mid ((a_1+b_1)-(a_2+b_2))$. Thus, consider $(a_1+b_1)-(a_2+b_2)$. We can distribute the minus sign to get $(a_1 - a_2) + (b_1 - b_2)$. From Proposition 1.4 (c), because we know that $m \mid (a_1 - a_2)$ and $m \mid (b_1 - b_2)$. We can write this as $m \mid ((a_1 - a_2) + (b_1 - b_2))$ which implies $m \mid ((a_1 + b_1) - (a_2 + b_2))$. This shows $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$.
- **Subtraction:** Similarly to addition, we want to show $a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$. Thus, consider $(a_1 - b_1) - (a_2 - b_2)$ which implies $(a_1 - a_2) - (b_1 - b_2)$. From Proposition 1.4 (c), because we know that $m \mid (a_1 - a_2)$ and $m \mid (b_1 - b_2)$. We can write this as $m \mid ((a_1 - a_2) - (b_1 - b_2))$ which implies $m \mid ((a_1 - b_1) - (a_2 - b_2))$. So $a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$.

Therefore we have shown $a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}$

- **Product** We want to show that $a_1 \cdot a_2 \equiv a_2 \cdot b_2 \pmod{m}$. Thus, consider $a_1 \cdot b_1 - a_2 \cdot b_2$:

$$\begin{aligned} a_1 \cdot b_1 - a_2 \cdot b_2 &= a_1 \cdot b_1 - a_1 \cdot b_2 + a_1 \cdot b_2 - a_2 \cdot b_2 \\ &= a_1 \cdot (b_1 - b_2) + b_2 \cdot (a_1 - a_2) \end{aligned}$$

  Because $m \mid (b_1 - b_2)$ and $m \mid (a_1 - a_2)$. We know from the definition of division that when we multiply those numbers by an integer like a_1 and b_2. m still divides the expression. Hence, $m \mid (a_1 \cdot (b_1 - b_2))$ and $m \mid (b_2 \cdot (a_1 - a_2))$. Therefore, $m \mid (a_1 \cdot b_1 - a_2 \cdot b_2)$ and $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}$. □

Exercise 1.16

Do the following modular computations. In each case, fill in the box with an integer between 0 and $m-1$. Where m is the modulus.

(a) $347 + 513 \equiv \boxed{} \pmod{763}$.

(c) $153 \cdot 287 \equiv \boxed{} \pmod{353}$

(e) $5327 \cdot 6135 \cdot 7139 \cdot 2187 \cdot 5219 \cdot 1873 \equiv \boxed{} \pmod{8157}$ (*Hint:* After each multiplication, reduce modulo 8157 before doing the next multiplication.)

(g) $373^6 \equiv \boxed{} \pmod{581}$.

Solution.

(a) $347 + 513 \pmod{763} = 97$

(c) $153 \cdot 287 \pmod{353} = 139$

(e)

$$\begin{aligned} 5327 \cdot 6135 \pmod{8157} &= 4203 \\ 4203 \cdot 7139 \pmod{8157} &= 3771 \\ 3771 \cdot 2187 \pmod{8157} &= 450 \\ 450 \cdot 5219 \pmod{8157} &= 7491 \\ 7491 \cdot 1873 \pmod{8157} &= \boxed{603} \end{aligned}$$

(g) $373^6 \pmod{581} = 463$

Exercise 1.17

Find all values of x between 0 and $m-1$ that are solutions of the following congruences. (*Hint:* If you can't figure out a clever way to find the solution(s), you can just substitute each value $x = 1$. $x = 2, \ldots$. $x = m - 1$ and see which ones work.)

(a) $x + 17 \equiv 23 \pmod{37}$.

(c) $x^2 \equiv 3 \pmod{11}$

(g) $x \equiv 1 \pmod{5}$ and also, $x \equiv 2 \pmod{7}$. (Find all solutions modulo 35, that is, find the solutions satisfying $0 \leq x \leq 34$.

Solution.

(a) $x = 6$

(c) We know that x cannot be any number who's square does not exceed 11 because

we cannot square a number to get 3 (other than $\sqrt{3}$. But these are only the integers, so we cannot use that). Hence, $x \neq 1, 2, 3$ because we know that the results of these, $1^2 = 1$. $2^2 = 4$. $3^2 = 9$ are not equivalent to 3. Let's try some more values: $x = 4$: $4^2 = 16 \pmod{11} = 5 \not\equiv 3$; $x = 5$: $5^2 = 25 \pmod{11} = 3 \equiv 3$; $x = 6$: $6^2 = 36 \pmod{11} = 3 \equiv 3$; $x = 7$: $7^2 = 49 \pmod{11} = 5 \not\equiv 3$; $x = 8$: $8^2 = 64 \pmod{11} = 9 \not\equiv 3$; $x = 9$: $9^2 = 81 \pmod{11} = 4 \not\equiv 3$; $x = 10$: $10^2 = 100 \pmod{11} = 1 \not\equiv 3$.

Thus, we have it that $x = 5, 6$.

(g) Because we have $x \equiv 1 \pmod{5}$. Verifying correct x's are straightforward. All we need to check for is if a multiple of $5 + 1$ satisfies $x \equiv 2 \pmod{7}$. Thus, the only solution is $x = 16$

Exercise 1.19

Prove that if a_1 and a_2 are units modulo m. Then $a_1 a_2$ is a unit modulo m.

Proof. Suppose a_1 and a_2 are units modulo m. This means $a \in \mathbb{Z}/m\mathbb{Z}$: $gcd(a, m) = 1$. In other words, $a_1 b_1 \equiv 1 \pmod{m}$ and $a_2 b_2 \equiv 1 \pmod{m}$ for some $b_1, b_2 \in \mathbb{Z}$. When we multiply the equations together, we get $(a_1 b_1)(a_2 b_2) \equiv 1 \pmod{m}$ which can be rewritten as $(a_1 a_2)(b_1 b_2) \equiv 1 \pmod{m}$. We can multiply b_1 and b_2 to get an integer b_3. Thus, when we multiply $a_1 a_2$ by b_3 and get 1. We have shown that b_3 is a multiplicative inverse, and $a_1 a_2$ is a unit modulo m. □

Exercise (Additional)

Decide whether each of the following is a group:

(a) `All 2x2 matrices with real number entries` with operation matrix addition

(b) `All 2x2 matrices with real number entries` with operation matrix multiplication

Solution.

(a) **Matrix Addition: ✓**

(1) **Closure:** For addition to work between matrices, they must be of dimension $2 \times 2 + 2 \times 2$. Therefore, the dimensions do not change, and it is closed.

(2) **Associativity:** 2×2 matrix addition is associative, as it inherits this property from the properties of matrices.

(3) **Identity Element:** We can add a matrix Z that consists of only 0s to a matrix A. And matrix A will remain unchanged.

(4) **Inverse Element:** True. Consider the matrices, $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. And $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

When we add these two together we get $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. This shows that 2×2 matrices have additive inverses.

(b) **Matrix Multiplication: ✗**

(1) **Closure:** The dimensions will stay the same during multiplication because it is an $n \times n$ matrix.

(2) **Associativity:** 2×2 matrix multiplication is associative, as it inherits this property from the properties of matrices.

(3) **Identity Element:** True. Consider the identity matrix, $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. When we multiply a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ by I. We get

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

(4) **Inverse Element:** False. Matrices with a non-zero determinant fail this criteria. Consider the matrix $B = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$. The determinant would be $\det((1)(4) - (2)(3) = -2$. Therefore, this matrix would not have an inverse.

Exercise (Additional)

Is `All 2x2 matrices with real number entries` a ring with operations matrix addition and matrix multiplication? Justify your answer.

Solution. ✓

(1) **Additive Closure:** True. (See the previous exercise (a), (1)).

(2) **Additive Associativity:** True. Inherited from the properties of matrices.

(3) **Additive Identity:** True. (See the previous exercise (a), (3)).

(4) **Additive Inverse:** True. You can take the difference between a matrix and its inverted duplicate (e.g., $-[A]$) and get 0.

(5) **Multiplicative Closure:** True. (See the previous exercise (b), (4)).

(6) **Distributive Property:** True. While this will pose an error on a calculator, you can do the equivalent: $[A]([B] + [C]) = [A][B] + [A][C]$. This is true because you are still taking the summation of each a_{ij}. b_{ij} and c_{ij}.

Exercise 1.26

Use the square-and-multiply algorithm described in Section 1.3.2, or the more efficient version in Exercise 1.25, to compute the following powers.

(a) $17^{183} \pmod{256}$.

(b) $2^{477} \pmod{1000}$

$\pmod{256}$

Solution.

(a) $a = 17$, $b = 1$, $A = 183$, and $N = 256$. We will now begin the loop because $A > 0$

- $A = 183$ is odd. Therefore, $b = b \cdot a \pmod{256} = 1 \cdot 17 \pmod{256} = 17$; and $a = a^2 \pmod{256} = 17^2 \pmod{256} = 33$. $A = \lfloor 182/2 \rfloor = 91$.
- $A = 91$ is odd. Therefore, $b = b \cdot a \pmod{256} = 17 \cdot 33 \pmod{256} = 49$; and $a = a^2 \pmod{256} = 33^2 \pmod{256} = 65$. $A = \lfloor 91/2 \rfloor = 45$.
- $A = 45$ is odd. Therefore, $b = b \cdot a \pmod{256} = 49 \cdot 65 \pmod{256} = 113$; and $a = a^2 \pmod{256} = 65^2 \pmod{256} = 129$. $A = \lfloor 45/2 \rfloor = 22$.
- $A = 22$ is even. Therefore, $a = a^2 \pmod{256} = 129^2 \pmod{256} = 1$. $A = \lfloor 22/2 \rfloor = 11$.
- $A = 11$ is odd. Therefore, $b = b \cdot a \pmod{256} = 113 \cdot 1 \pmod{256} = 113$; and $a = a^2 \pmod{256} = 1^2 \pmod{256} = 1$. $A = \lfloor 11/2 \rfloor = 5$.
- $A = 5$ is odd. Therefore, $b = b \cdot a \pmod{256} = 113 \cdot 1 \pmod{256} = 113$; and $a = a^2 \pmod{256} = 1^2 \pmod{256} = 1$. $A = \lfloor 5/2 \rfloor = 2$.
- $A = 2$ is even. Therefore, $a = a^2 \pmod{256} = 1^2 \pmod{256} = 1$. $A = \lfloor 2/2 \rfloor = 1$.
- $A = 1$ is odd. Therefore, $b = b \cdot a \pmod{256} = 113 \cdot 1 \pmod{256} = 113$; and $a = a^2 \pmod{256} = 1^2 \pmod{256} = 1$. $A = \lfloor 1/2 \rfloor = 0$.

Since $A = 0$, we can report the value of b, which is 113. Hence, $17^183 \pmod{256} = 113$.

(b) $a = 2$, $b = 1$, $A = 477$, $N = 1000$. We will now begin the loop because $A > 0$

- $A = 477$ is odd. Therefore, $b = b \cdot a \pmod{1000} = 1 \cdot 2 \pmod{1000} = 2$; and $a = a^2 \pmod{1000} = 2^2 \pmod{1000} = 4$. $A = \lfloor 477/2 \rfloor = 238$.

- $A = 238$ is even. Therefore, $a = a^2 \pmod{1000} = 4^2 \pmod{1000} = 16$. $A = \lfloor 238/2 \rfloor = 119$.
- $A = 119$ is odd. Therefore, $b = b \cdot a \pmod{1000} = 2 \cdot 16 \pmod{1000} = 32$; and $a = a^2 \pmod{1000} = 16^2 \pmod{1000} = 256$. $A = \lfloor 119/2 \rfloor = 59$.
- $A = 59$ is odd. Therefore, $b = b \cdot a \pmod{1000} = 32 \cdot 256 \pmod{1000} = 192$; and $a = a^2 \pmod{1000} = 256^2 \pmod{1000} = 536$. $A = \lfloor 59/2 \rfloor = 29$.
- $A = 29$ is odd. Therefore, $b = b \cdot a \pmod{1000} = 192 \cdot 536 \pmod{1000} = 912$; and $a = a^2 \pmod{1000} = 536^2 \pmod{1000} = 296$. $A = \lfloor 29/2 \rfloor = 14$.
- $A = 14$ is even. Therefore, $a = a^2 \pmod{1000} = 296^2 \pmod{1000} = 616$. $A = \lfloor 14/2 \rfloor = 7$.
- $A = 7$ is odd. Therefore, $b = b \cdot a \pmod{1000} = 912 \cdot 616 \pmod{1000} = 792$; and $a = a^2 \pmod{1000} = 616^2 \pmod{1000} = 456$. $A = \lfloor 7/2 \rfloor = 3$.
- $A = 3$ is odd. Therefore, $b = b \cdot a \pmod{1000} = 792 \cdot 456 \pmod{1000} = 152$; and $a = a^2 \pmod{1000} = 456^2 \pmod{1000} = 936$. $A = \lfloor 3/2 \rfloor = 1$.
- $A = 1$ is odd. Therefore, $b = b \cdot a \pmod{1000} = 152 \cdot 936 \pmod{1000} = 272$; and $a = a^2 \pmod{1000} = 936^2 \pmod{1000} = 96$. $A = \lfloor 1/2 \rfloor = 0$.

Since $A = 0$, we can report the value of b, which is 272. Hence, $2^{477} \pmod{1000} = 272$.

Exercise 1.41

A *transposition cipher* is a cipher in which the letters of the plaintext remain the same, but their order is rearranged. Here is a simple example in which the message is encrypted in blocks of 25 letters at a time. Take the given 25 letters and arrange them in a 5-by-5 block by writing the message horizontally on the lines. For example, the first 25 letters of the message

```
Now is the time for all good men to come to the aid...
```

is written as

```
N O W I S
T H E T I
M E F O R
A L L G O
O D M E N
```

Now the ciphertext is formed by reading the letters down the columns, which gives the ciphertext

```
NTMAO OHELD WEFLM ITOGE SIRON.
```

(a) Use this transposition cipher to encrypt the first 25 letters of the message

```
Four score and seven years ago our fathers...
```

(b) The following message was encrypted using this transposition cipher. Decrypt it.

```
WNOOA HTUFN EHRHE NESUV ICEME.
```

(c) There are many variations on this type of cipher. We can form the letters into a rectangle instead of a square, and we can use various patterns to place the letters into the rectangle and to read them back out. Try to decrypt the following ciphertext, in which the letters were placed horizontally into a rectangle of some size and then read off vertically by columns.

```
WHNCE STRHT TEOOH ALBAT DETET SADHE
LEELL QSFMU EEEAT VNLRI ATUDR HTEEA
```

(For convenience, we've written the ciphertext in 5 letter blocks, but that doesn't necessarily mean that the rectangle has a side of length 5.)

Solution.

(a) The first 25 letters of the sentence given is, "Four score and seven year ago". Written in block form:

```
F O U R S
C O R E A
N D S E V
E N Y E A
R S A G O
```

Now the ciphertext is formed by reading the letters down the columns, which gives the ciphertext

```
FCNER OODNS URSYA REEEG SAVAO
```

(b) To create a transposition cipher, we can read the sentence from the starting letter of each word from the sentence, and move inward. For example,

(1) $\boxed{W}$NOOA $\boxed{H}$TUFN $\boxed{E}$HRHE $\boxed{N}$ESUV $\boxed{I}$CEME $\Rightarrow$ "When I..."

(2) W$\boxed{N}$OOA H$\boxed{T}$UFN E$\boxed{H}$RHE N$\boxed{E}$SUV I$\boxed{C}$EME $\Rightarrow$ "...N The C..."

(3) WN$\boxed{O}$OA HT$\boxed{U}$FN EH$\boxed{R}$HE NE$\boxed{S}$UV IC$\boxed{E}$ME $\Rightarrow$ "...ourse..."

(4) WNO$\boxed{O}$A HTU$\boxed{F}$N EHR$\boxed{H}$E NES$\boxed{U}$V ICE$\boxed{M}$E $\Rightarrow$ "...Of Hum..."

(5) WNOO$\boxed{A}$ HTUF$\boxed{N}$ EHRH$\boxed{E}$ NESU$\boxed{V}$ ICEM$\boxed{E}$ $\Rightarrow$ "...an Eve."

Putting it all together, we get, "When in the course of human eve..." (Declaration of Independence)

(c) This cipher is going to be a little difficult as we have to go through a couple of cases to see which pattern makes the most sense. If we consider the number of letters, 60, we can start at the lowest divisor, 2, and work our way up through the other divisors (this way, we won't start with extremely long ciphers that will each take up a whole page on their lonesome). Thus,

- Reading by 2s (to get a 2×30 matrix)

  ```
  W N E T H T O H L A D T A H L E
  H C S R T E O A B T E S D E E L
  ```

  Clearly, even though we do not have all the letters, there are no words being formed. Let's move on.

- Reading by 3s (to get a 3×20 matrix)

  ```
  W C T T O A A E T D L L S U E V R T R E
  H E R T O L T T S H E L F E A N I U H E
  N S H E H B D E A E E Q M E T L A D T A
  ```

  There are no words here.

- 4×15 matrix

```
W E H O L D T H E S E T R U T
H S T O B E S E L F E V I D E
N T T H A T A L L M E N A R E
C R E A T E D E Q U A L T H A
```

There we finally have our transcription! "We hold these truths to be self evident that all men are created equal tha..." (Declaration of Independence again).

Exercise Additional Problem

Write down the steps for an algorithm to encrypt a plaintext using a transposition/S-cytale cipher using n columns. *Hint: This should involve some modular arithmetic.*

Solution.

(1) Remove all spaces from the plaintext message.

(2) Let i be the length of the message after removing spaces.

(3) Find the number of rows m required for the transposition cipher matrix:

$$m = \left\lceil \frac{i}{n} \right\rceil$$

(4) Create an $m \times n$ matrix to hold the characters.

(5) For each character in the message, place it into the matrix. Let the index of the current character in the message be k, where $0 \leq k < i$. Calculate the row and column for this character as follows:

$$\text{row} = \left\lfloor \frac{k}{n} \right\rfloor$$

$$\text{column} = k \pmod{n}$$

(6) Once all characters are placed into the matrix, read the matrix column by column to form the ciphertext. For each column j, loop through the rows and append each character to the ciphertext in the following order:

$$\text{character index} = j + n \times \text{row}$$

(7) If there are empty cells (i.e., n does not divide the message length i), fill these cells with random characters or leave them blank.

(8) Concatenate the characters column by column to form the final ciphertext.

Exercise 1.32

For each of the following primes p and numbers a, compute $a^{-1} \mod p$ in two ways: (i) the extended Euclidean algorithm. (ii) Use the fast power algorithm and Fermat's little theorem. (See Example 1.27.)

(a) $p = 47$ and $a = 11$.

(b) $p = 587$ and $a = 345$.

Solution.

(a) (i) For the extended Euclidean algorithm, we can start by filling out this table:

i	r_i	q_i	r_{i+1}	u_i	v_i
0	47	–	–	1	0
1	11	4	3	0	1
2	3	3	2	1	$0 - 4 \cdot 1 = -4$
3	2	1	1	$0 - 3 \cdot 1 = -4$	$1 - 3 \cdot -4 = 13$
4	1	2	0	$1 - 1 \times -4 = 4$	$-4 - 1 \cdot 13 = -17$

Thus, to find $a^{-1} \pmod p$, we need an x such that $11x \equiv 1 \pmod{47}$. From our table, we know that number to be -17 because $1 = 4 \times 47 - 17 \times 11$. Then, as a positive number mod 47, we get $x \equiv -17 \equiv 30 \pmod{47}$.

(ii) For Fermat's Little Theorem:

$$a^{p-1} \equiv 1 \pmod p$$
$$a^{p-2} \equiv a^{-1} \pmod p$$
$$11^{45} \pmod{47}$$

By the fast power algorithm, we need to find the binary representation of 45. Thus, $45 \pmod 2 = 1$, $22 \pmod 2 = 0$, $11 \pmod 2 = 1$, $5 \pmod 2 = 1$, $2 \pmod 2 = 0$, $1 \pmod 2 = 1$. From this, we have the binary representation of 45_{10} as 101101_2. Hence, we will need to calculate $2^5 \cdot 2^3 \cdot 2^2 \cdot 2^1 \cdot 2^0 \Rightarrow 11^{2^5} \cdot 11^{2^3} \cdot 11^{2^0} \Rightarrow 11^{32} \cdot 11^8 \cdot 11^4 \cdot 11 \equiv 17 \cdot 14 \cdot 25 \cdot 11$. Now, lets find the values of these numbers:

$$11^1 \equiv 11 \pmod{47}$$
$$11^2 \equiv 27 \pmod{47}$$
$$11^4 \equiv 25 \pmod{47}$$
$$11^8 \equiv 14 \pmod{47}$$
$$11^{16} \equiv 8 \pmod{47}$$
$$11^{32} \equiv 17 \pmod{47}$$

Now, we can calculate $11^{45} = 11^{32} \cdot 11^8 \cdot 11^4 \cdot 11 \equiv 17 \cdot 14 \cdot 25 \cdot 11 \pmod{47}$.

Further multiplying we get $17 \cdot 14 \pmod{47} \equiv 3$. Then, $3 \cdot 25 \pmod{47} \equiv 28$. And finally, $28 \cdot 11 \pmod{47} \equiv 30$. Thus confirming our previous answer in (i).

(b) (i) For the extended Euclidean algorithm:

i	r_i	q_i	r_{i+1}	u_i	v_i
0	587	–	–	1	0
1	345	1	242	0	1
2	242	1	103	1	$0 - 1 \cdot 1 = -1$
3	103	2	36	$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot -1 = 2$
4	36	2	31	$1 - 2 \cdot -1 = 3$	$-1 - 2 \cdot 2 = -5$
5	31	1	5	$-1 - 2 \cdot 3 = -7$	$2 - 2 \cdot -5 = 12$
6	5	6	1	$3 - 1 \cdot -7 = 10$	$-5 - 1 \cdot 12 = -17$
7	1	5	0	$10 - 6 \cdot 10 = -67$	$12 - 6 \cdot -17 = 114$

Thus, the inverse of 345 (mod 587) is 114.

(ii) The binary expression for 585_{10} is 1001001001_2 (I just used my calculator this time and kept dividing ans by 2 while keeping track of the odd vs even quotients). This leaves us with $345^{2^9} \cdot 345^{2^6} \cdot 345^{2^3} \cdot 345^{2^0}$.

$$
\begin{aligned}
345^1 &\equiv 345 \pmod{587} \\
345^2 &\equiv 451 \pmod{587} \\
345^4 &\equiv 299 \pmod{587} \\
345^8 &\equiv 177 \pmod{587} \\
345^{16} &\equiv 218 \pmod{587} \\
345^{64} &\equiv 529 \pmod{587} \\
345^{128} &\equiv 429 \pmod{587} \\
345^{256} &\equiv 310 \pmod{587} \\
345^{512} &\equiv 419 \pmod{587}
\end{aligned}
$$

Now we can multiply and solve: $345^{2^9} \cdot 345^{2^6} \cdot 345^{2^3} \cdot 345^{2^0} \Rightarrow 419 \cdot 529 \cdot 177 \cdot 345 \pmod{587} = 114$. Therefore, the inverse of 345 (mod 587) is 114.

Exercise 1.34

Recall that g is called a primitive root modulo p if the powers of g give all nonzero elements of $\mathbb{F}_p$.

(a) For which of the following primes is 2 a primitive root modulo p?

(i) $p = 7$ (ii) $p = 13$ (iii) $p = 19$ (iv) $p = 23$

(b) For which of the following primes is 3 a primitive root modulo p?

(i) $p = 5$ (ii) $p = 7$ (iii) $p = 11$ (iv) $p = 17$

(c) Find a primitive root for each of the following primes.

(i) $p = 23$ (ii) $p = 29$ (iii) $p = 41$ (iv) $p = 43$

(d) Find all primitive roots modulo 11. Verify that there are exactly $\phi(10)$ of them, as asserted in Remark 1.32.

Solution.

(a) (i) $p = 7$: $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1 \pmod 7$. Because 2 does not cover every nonzero elements of $\mathbb{F}_p$, 2 is not a primitive root.

(ii) $p = 13$: $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 3$, $2^5 \equiv 6$, $2^6 \equiv 12$, $2^7 \equiv 11$, $2^8 \equiv 9$, $2^9 \equiv 5$, $2^{10} \equiv 10$, $2^{11} \equiv 7$, $2^{12} \equiv 1$, 2 is a primitive root.

(iii) $p = 19$: $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 16$, $2^5 \equiv 13$, $2^6 \equiv 7$, $2^7 \equiv 14$, $2^8 \equiv 9$, $2^9 \equiv 18$, $2^{10} \equiv 17$, $2^{11} \equiv 15$, $2^{12} \equiv 11$, $2^{13} \equiv 3$, $2^{14} \equiv 6$, $2^{15} \equiv 12$, $2^{16} \equiv 5$, $2^{17} \equiv 10$, $2^{18} \equiv 1$, 2 is a primitive root.

(iv) $p = 23$: $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 16$, $2^5 \equiv 9$, $2^6 \equiv 18$, $2^7 \equiv 13$, $2^8 \equiv 3$, $2^9 \equiv 6$, $2^{10} \equiv 12$, $2^{11} \equiv 1$, 2 is not a primitive root.

(b) (i) $p = 5$: $3^1 \equiv 3, 3^2 \equiv 4, 3^3 \equiv 2, 3^4 \equiv 1$, 3 is a primitive root.

(ii) $p = 7$: $3^1 \equiv 3, 3^2 \equiv 2, \ldots, 3^6 \equiv 1$, 3 is a primitive root.

(iii) $p = 11$: $3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 5, \ldots, 3^5 \equiv 1$, 3 is not a primitive root.

(iv) $p = 17$: $3^1 \equiv 3, 3^2 \equiv 9, \ldots, 3^{16} \equiv 1$, 3 is a primitive root.

(c) (i) $p = 23$: $5^1 \equiv 5$, $5^2 \equiv 2$, $5^3 \equiv 10$, $5^4 \equiv 4$, $5^5 \equiv 20$, $5^6 \equiv 8$, $5^7 \equiv 17$, $5^8 \equiv 16$, $5^9 \equiv 11$, $5^{10} \equiv 9$, $5^{11} \equiv 22$, $5^{12} \equiv 18$, $5^{13} \equiv 21$, $5^{14} \equiv 13$, $5^{15} \equiv 19$, $5^{16} \equiv 3$, $5^{17} \equiv 15$, $5^{18} \equiv 6$, $5^{19} \equiv 7$, $5^{20} \equiv 12$, $5^{21} \equiv 14$, $5^{22} \equiv 1$,
5 is a primitive root.

(ii) $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 16$, $2^5 \equiv 3$, $2^6 \equiv 6$, $2^7 \equiv 12$, $2^8 \equiv 24$, $2^9 \equiv 19$, $2^{10} \equiv 9$, $2^{11} \equiv 18$, $2^{12} \equiv 7$, $2^{13} \equiv 14$, $2^{14} \equiv 28$, $2^{15} \equiv 27$, $2^{16} \equiv 25$, $2^{17} \equiv 21$,

$2^{18} \equiv 13$, $2^{19} \equiv 26$, $2^{20} \equiv 23$, $2^{21} \equiv 17$, $2^{22} \equiv 5$, $2^{23} \equiv 10$, $2^{24} \equiv 20$, $2^{25} \equiv 11$, $2^{26} \equiv 22$, $2^{27} \equiv 15$, $2^{28} \equiv 1$,
2 is a primitive root.

(iii) $6^1 \equiv 6$ $6^2 \equiv 36$, $6^3 \equiv 11$, $6^4 \equiv 25$, $6^5 \equiv 27$, $6^6 \equiv 39$, $6^7 \equiv 29$, $6^8 \equiv 10$, $6^9 \equiv 19$, $6^{10} \equiv 32$, $6^{11} \equiv 28$, $6^{12} \equiv 4$, $6^{13} \equiv 24$, $6^{14} \equiv 21$, $6^{15} \equiv 3$, $6^{16} \equiv 18$, $6^{17} \equiv 26$, $6^{18} \equiv 33$, $6^{19} \equiv 34$, $6^{20} \equiv 40$, $6^{21} \equiv 35$, $6^{22} \equiv 5$, $6^{23} \equiv 30$, $6^{24} \equiv 16$, $6^{25} \equiv 14$, $6^{26} \equiv 2$, $6^{27} \equiv 12$, $6^{28} \equiv 31$, $6^{29} \equiv 22$, $6^{30} \equiv 9$, $6^{31} \equiv 13$, $6^{32} \equiv 37$, $6^{33} \equiv 17$, $6^{34} \equiv 20$, $6^{35} \equiv 38$, $6^{36} \equiv 23$, $6^{37} \equiv 15$, $6^{38} \equiv 8$, $6^{39} \equiv 7$, $6^{40} \equiv 1$,
6 is a primitive root.

(iv) $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 27$, $3^4 \equiv 38$, $3^5 \equiv 28$, $3^6 \equiv 41$, $3^7 \equiv 37$, $3^8 \equiv 25$, $3^9 \equiv 32$, $3^{10} \equiv 10$, $3^{11} \equiv 30$, $3^{12} \equiv 4$, $3^{13} \equiv 12$, $3^{14} \equiv 36$, $3^{15} \equiv 22$, $3^{16} \equiv 23$, $3^{17} \equiv 26$, $3^{18} \equiv 35$, $3^{19} \equiv 19$, $3^{20} \equiv 14$, $3^{21} \equiv 42$, $3^{22} \equiv 40$, $3^{23} \equiv 34$, $3^{24} \equiv 16$, $3^{25} \equiv 5$, $3^{26} \equiv 15$, $3^{27} \equiv 2$, $3^{28} \equiv 6$, $3^{29} \equiv 18$, $3^{30} \equiv 11$, $3^{31} \equiv 33$, $3^{32} \equiv 13$, $3^{33} \equiv 39$, $3^{34} \equiv 31$, $3^{35} \equiv 7$, $3^{36} \equiv 21$, $3^{37} \equiv 20$, $3^{38} \equiv 17$, $3^{39} \equiv 8$, $3^{40} \equiv 24$, $3^{41} \equiv 29$, $3^{42} \equiv 1$,
3 is a primitive root.

(d) The primitive roots modulo 11 are 2, 6, 7, 8. To check:
$2^1 \equiv 11 = 2$, $2^2 \equiv 11 = 4$, $2^3 \equiv 11 = 8$, $2^4 \equiv 11 = 5$, $2^5 \equiv 11 = 10$, $2^6 \equiv 11 = 9$, $2^7 \equiv 11 = 7$, $2^8 \equiv 11 = 3$, $2^9 \equiv 11 = 6$, $2^{10} \equiv 11 = 1$,

2 is a primitive root.

$6^1 \equiv 11 = 6$, $6^2 \equiv 11 = 3$, $6^3 \equiv 11 = 7$, $6^4 \equiv 11 = 9$, $6^5 \equiv 11 = 10$, $6^6 \equiv 11 = 5$, $6^7 \equiv 11 = 8$, $6^8 \equiv 11 = 4$, $6^9 \equiv 11 = 2$, $6^{10} \equiv 11 = 1$,

6 is a primitive root.

$7^1 \equiv 11 = 7$, $7^2 \equiv 11 = 5$, $7^3 \equiv 11 = 2$, $7^4 \equiv 11 = 3$, $7^5 \equiv 11 = 10$, $7^6 \equiv 11 = 4$, $7^7 \equiv 11 = 6$, $7^8 \equiv 11 = 9$, $7^9 \equiv 11 = 8$, $7^{10} \equiv 11 = 1$,

7 is a primitive root.

$8^1 \equiv 11 = 8$, $8^2 \equiv 11 = 9$, $8^3 \equiv 11 = 6$, $8^4 \equiv 11 = 4$, $8^5 \equiv 11 = 10$, $8^6 \equiv 11 = 3$, $8^7 \equiv 11 = 2$, $8^8 \equiv 11 = 5$, $8^9 \equiv 11 = 7$, $8^{10} \equiv 11 = 1$,

8 is a primitive root.

Exercise 2.3

Let g be a primitive root for $\mathbb{F}_p$.

(b) Prove that $\log_g(h_1 h_2) = \log_g(h_1) + \log_g(h_2)$ for all $h_1, h_2 \in \mathbb{F}_p^*$.

(c) Prove that $\log_g(h^n) = n \log_g(h)$ for all $h \in \mathbb{F}_p^*$ and $n \in \mathbb{Z}$.

Solution.

(b) *Proof.* We know that $g^x \equiv h \pmod{p}$, which means that $x = \log_g(h)$. Similarly, if $g^{x_1} \equiv h_1 \pmod{p}$ and $g^{x_2} \equiv h_2 \pmod{p}$, then $x_1 = \log_g(h_1)$ and $x_2 = \log(h_2)$. Now, we can substitute these values into the first equation to get $g^{x_1+x_2} \equiv h_1 h_2 \pmod{p} \equiv g^{\log_g(h_1)+\log_g(h_2)} \pmod{p}$. Then, from the properties of exponents, we can rewrite this equation as $h_1 \cdot h_2 \pmod{p} \equiv g^{\log_g(h_1 h_2)} \pmod{p}$. Therefore, $\log_g(h_1 \cdot h_2) = \log_g(h_1) + \log_g(h_2)$.

(c) *Proof* Following a similar process to (b), we start with $g^{n \log_g(h)}$. Then, by using the properties of logarithms, we can rewrite this as $g^{\log_g(h^n)}$. Then, because $g^{\log_g}$ cancel out, we see that $g^{\log_g(h^n)} = h^n$. Putting everything together, we have

$$\begin{aligned} g^{\log_g(h^n)} &\equiv h^n \pmod{p} \\ \log_g(h^n) &\equiv n \log_g(h) \pmod{p}. \end{aligned}$$

Exercise 2.4

Compute the following discrete logarithms.

(a) $\log_2(13)$ for the prime 23, i.e., $p = 23$, $g = 2$, and you must solve the congruence $2^x \equiv 13 \pmod{23}$.

(b) $\log_{10}(22)$ for the prime $p = 47$.

(c) $\log_{627}(608)$ for the prime $p = 941$. (Hint: Look in the second column of Table 2.1 on page 66.)

Solution.

(a) We use Wolfram Alpha to solve for x in the equation $2^x \equiv 13 \pmod{23}$: $x = 7$.

(b) Solving for x we get $x = 11$.

(c) $x = 18$.

Exercise 2.6

Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for a Diffie-Hellman key exchange. Alice sends Bob the value $A = 974$. Bob asks for your assistance, so you tell him to use the secret exponent $b = 871$.

(a) What value B should Bob send to Alice, and what is their secret shared value?

(b) Can you figure out Alice's secret exponent?

Added (a) and (b) for clarity in Exercise 2.6.

Solution.

(a) Bob sends $B = g^b = 2^{871} \equiv 805 \pmod{1373}$. Their shared secret value is $974^{871} \equiv 397 \pmod{1373}$ (via Wolfram Alpha).

(b) To get Alice's secret exponent, we need to solve a by brute force. Thus, we need to solve the equation $2^a \equiv 974 \pmod{1373}$. We find that $a = 587$.

Exercise 2.7

Let p be a prime and let g be an integer. The *Decision Diffie-Hellman Problem* is as follows. Suppose that you are given three numbers A, B, and C, and suppose that A and B are equal to

$$A \equiv g^a \pmod{p} \quad \text{and} \quad B \equiv g^b \pmod{p},$$

but that you do not necessarily know the values of the exponents a and b. Determine whether C is equal to $g^{ab} \pmod{p}$. Notice that this is different from the Diffie-Hellman problem described on page 69. The Diffie-Hellman problem asks you to actually compute the value of g^{ab}.

(a) Prove that an algorithm that solves the Diffie-Hellman problem can be used to solve the decision Diffie-Hellman problem.

(b) Do you think that the decision Diffie-Hellman problem is hard or easy? Why? See Exercise 6.40 for a related example in which the decision problem is easy, but it is believed that the associated computational problem is hard.

Solution.

(a) Since we know that $A = g^a \pmod{p}$ and $B = g^b \pmod{p}$, then we just have to compare C to $g^{ab} \pmod{p}$. If $C = g^{ab} \pmod{p}$, then the algorithm solves the decision Diffie-Hellman problem.

(b) Because we only know A and B it makes determining C hard because we only know g^{a+b} and *not* g^{ab}. Thus, the decision Diffie-Hellman problem is hard because

it is difficult to determine whether $C = g^{ab} \pmod{p}$ without knowing a and b.

Exercise 2.8

Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for communications using the Elgamal public key cryptosystem.

(a) Alice chooses $a = 947$ as her private key. What is the value of her public key A?

(b) Bob chooses $b = 716$ as his private key, so his public key is

$$B \equiv 2^{716} \equiv 469 \pmod{1373}.$$

Alice encrypts the message $m = 583$ using the random element $k = 877$. What is the ciphertext (c_1, c_2) that Alice sends to Bob?

(c) Alice decides to choose a new private key $a = 299$ with associated public key

$$A \equiv 2^{299} \equiv 34 \pmod{1373}.$$

Bob encrypts a message using Alice's public key and sends her the ciphertext $(c_1, c_2) = (661, 1325)$. Decrypt the message.

(d) Now Bob chooses a new private key and publishes the associated public key $B = 893$. Alice encrypts a message using this public key and sends the ciphertext $(c_1, c_2) = (693, 793)$ to Bob. Eve intercepts the transmission. Help Eve by solving the discrete logarithm problem $2^b \equiv 893 \pmod{1373}$ and using the value of b to decrypt the message.

Solution.

(a) $p = 1373,\ g = 2,\ a = 947 \Rightarrow A \equiv 2^{947} \pmod{1373} \equiv 177.$

(b) $c_1 \equiv 2^{877} \pmod{1373} \equiv 719,\ c_2 \equiv 583 \cdot 469^{877} \pmod{1373} \equiv 623.$ Alice sends "$(719, 623)$" to Bob.

(c) To decrypt, we can use the EEA to find the inverse of $661^{299} \pmod{1373} \equiv 645^{-1} \equiv 794$. From here, we solve for the message: $1325 \cdot 794 \pmod{1373} \equiv 332$.

(d) Solving for b in $2^b \equiv 893 \pmod{1373}$ gives $b = 219$. Now we can decrypt:

$$(c_1^a)^{-1} \cdot c_2 \equiv (693^{219})^{-1} \equiv 431^{-1} \cdot 793 \equiv 532 \cdot 793 \equiv 365 \pmod{1373}.$$

Alice's private message to Bob is $m = 365$.

Exercise 1.46

(a) Convert the 12-bit binary number 110101100101 into a decimal integer between 0 and $2^{12} - 1$.

(e) Convert the decimal numbers 8734 and 5177 into binary numbers, combine them using XOR, and convert the result back into a decimal number.

For this exercise, I will be using these python functions that I wrote:

```
def compute_binary(num):
    binary_representation = []
    while num != 0:
        result = num % 2
        num = num // 2
        binary_representation.append(result)
    binary_str = ''.join(map(str, binary_representation))
    print(binary_str)

def compute_decimal_int(binary_str):
    int_representation = int(binary_str, 2)
    print(int_representation)
```

Solution.

(a) 3429

(e) Note the added 0 for the second binary number so the two numbers add properly.

$$\begin{aligned} 8734 &= 10001000011110 \\ 5177 &= 01010000111001 \\ 8734 \oplus 5177 &= 11011001010111 \\ 13863 &= 11011001010111 \end{aligned}$$

Exercise 2.17

Use Shanks's babystep-giantstep method to solve the following discrete logarithm problems.

(a) $11^x = 21$ in $\mathbb{F}_{71}$.

Solution.

(a) 1. Let $m = \lceil \sqrt{70} \rceil = 9$

2. Create two lists:

- **Baby steps:**

$$\{11^0, 11^1, \ldots, 11^9\} \pmod{71} \equiv \{1, \boxed{11}, 50, 53, 15, 23, 40, 14, 12\}$$

- **Giant steps:**

$$\{21, 21 \cdot 11^{-9}, 21 \cdot 11^{-18}, \ldots\} \pmod{71} \equiv \{21, 5, 35, 32, \boxed{11} \ldots\}$$

3. Find a match between the two lists: $\boxed{11}$
4. Substitute values for $i + jm = 1 + 4(9) = 37$. So, $11^{37} \equiv 21 \pmod{71}$

Exercise 2.18

Solve each of the following simultaneous systems of congruences (or explain why no solution exists).

(b) $x \equiv 137 \pmod{423}$ and $x \equiv 87 \pmod{191}$.

(d) $x \equiv 5 \pmod{9}$, $x \equiv 6 \pmod{10}$, and $x \equiv 7 \pmod{11}$.

Solution.

(b)
1. Let $m = 423 \cdot 191 = 80793$.
2. Compute $n_1 = \frac{m}{m_1} = \frac{80793}{423} = 191$, and $n_2 = \frac{80793}{191} = 423$
3. Compute $y_1 = 191^{-1} \pmod{423} \equiv 392$ and $y_2 = 423^{-1} \pmod{191} \equiv 14$.
4. Compute $x = (137)(191)(392) + (87)(423)(14) \pmod{80793} \equiv 27209$

(d)
1. Let $m = 9 \cdot 10 \cdot 11 = 990$.
2. Compute $n_1 = \frac{990}{9} = 110$, $n_2 = \frac{990}{10} = 99$, and $n_3 = \frac{990}{11} = 90$.
3. Compute $y_1 = 110^{-1} \pmod{9} \equiv 5$, $y_2 = 99^{-1} \pmod{10} \equiv 9$, and $y_3 = 90^{-1} \pmod{11} \equiv 6$
4. Compute $x = (5)(110)(5) + (6)(99)(9) + (7)(90)(6) \pmod{990} = 986$

Exercise 2.20

Let a, b, m, n be integers with $\gcd(m, n) = 1$. Let

$$c \equiv (b - a) \cdot m^{-1} \pmod{n}.$$

Prove that $x = a + cm$ is a solution to

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}, \tag{2.24}$$

and that every solution to (2.24) has the form $x = a + cm + ymn$ for some $y \in \mathbb{Z}$.

Proof. Let $a, b, m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. Let $c \equiv (b - a)m^{-1} \pmod{n}$. Review the following:

$$\begin{aligned} x &\equiv a \pmod{m} \\ a + cm &\equiv a \pmod{m} \\ a &\equiv a \pmod{m} - cm. \end{aligned}$$

Then, because cm is a multiple of m, when we take the mod of $a - cm \pmod{m}$, we will always get a. Hence, $a \equiv a \pmod{m}$. For the other equation, we will be using the def of c in our proof:

$$\begin{aligned} a + cm &\equiv b \pmod{n} \\ cm &\equiv b - a \pmod{n} \\ c &\equiv (b - a)m^{-1} \pmod{n}. \end{aligned}$$

So, now when we multiply by m on both sides, we get $cm \equiv b - a \pmod{n}$. Rearranging, we see $cm + a \equiv b \pmod{n}$, so x is a solution.

For the second half of the proof, suppose we have x' as the solution for $x' \equiv a \pmod{m}$ and $x' \equiv b \pmod{n}$. We want to show that $x' = x$. Thus, we subtract x from x' and get the following:

$$x' - x \equiv a - a = 0 \pmod{m}, \text{ which implies } x' - x = km \text{ for some } k \in \mathbb{Z}.$$

This is the outcome because we know that for anything to be equal to 0 in modulus, the number itself must be a multiple of the modulus, m. We can follow the same logic for b, and see that $x' - x \equiv b - b = lm$ for some $l \in \mathbb{Z}$. Since $\gcd(m, n) = 1$, $x' - x$ must be a multiple of m and n, meaning $x' - x = ymn$ for some $y \in \mathbb{Z}$. Therefore, $x' = x + ymn, = a + cm + ymn$. □

Exercise 2.28

Use the Pohlig-Hellman algorithm (Theorem 2.31) to solve the discrete logarithm problem $g^x = a$ in $\mathbb{F}_p$ in each of the following cases.

(a) $p = 433$, $g = 7$, $a = 166$.

Solution. We start by writing the given information into an equation that we can work with. Thus, $7^x \equiv 166 \pmod{433}$. Since 433 is prime, $\varphi(433) = 432$, which we can factor

to $16 \cdot 27$. Let $x = a_0 + 16a_1$:

$$(7^{a_0+16a_1})^{27} \equiv 166^{27} \pmod{433} \tag{3.1}$$
$$(7^{27a_0+432a_1}) \equiv \tag{3.2}$$
$$(7^{27a_0} \cdot 7^{432a_1}) \equiv \tag{3.3}$$
$$(7^{27})^{a_0}(7^{a_1})^{432} \equiv \tag{3.4}$$
$$(265)^{a_0} \equiv 250 \pmod{433} \tag{3.5}$$

For (3.1), we got the expression by substituting x for $a_0 + 16a_1$ for the exponent in $g^x \equiv \ldots$. From there, (3.2) — (3.4) is simple algebra. Then for (3.5), because 7^{a_1} is congruent to 1, $(7^{a_1})^{432} = 1$. Additionally, we take $7^{27} \pmod{432}$ to get 265^{a_0}. Then, we do the same thing for the other side of the equation. Now, we can brute force this by setting $a_1 = \{0, 1, 2, 3, \ldots, 27\}$. We find that when $a_0 = 15$, $265^{a_0} \equiv 250 \pmod{433}$. Seeing that we have a_0, we need to find b_0:

$$(7^{b_0+27b_1})^{16} \equiv 166^{16} \pmod{433}$$
$$374^{b_0} \equiv 335 \pmod{433}$$

Thus, through brute force, we find that $b_0 = 20$. We can take our a_0 and b_0 to solve for x_1, x_2:

$$x_1 = a_0 + 16a_1$$
$$x_1 = 15 \pmod{16}$$

and

$$x_2 = b_0 + 27b_1$$
$$x_2 = 20 \pmod{27}$$

At this point, we can solve the CRT.

1. Let $m = 16 \cdot 27 = 432$.
2. Compute $n_1 = \frac{432}{16} = 27$ and $n_2 = \frac{432}{27} = 16$.
3. Compute $y_1 = 27^{-1} \pmod{16} \equiv 3$ and $y_2 = 16^{-1} \pmod{27} \equiv 22$.
4. Compute $x = (27)(15)(3) + (20)(16)(22) \pmod{432} = 47$

I relied on this video heavily.