



Mathematical Cryptography

MATH 490

Start

AUGUST 26, 2024

Author

Paul Beggs

BeggsPA@Hendrix.edu

Instructor

Prof. Allie Ray, Ph.D.

End

DECEMBER 2, 2024

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.

AOLYLHYLUVZLJYLAZILAALYAOLHUAOLZLJYLALZAOHALCLYFIVKFNBLZZLZ

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) LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBVDVDWUHH

- (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 $a, b, c \in \mathbb{Z}$. 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:

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

- (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 $a | b$ and $b | a$. We know there exists an $n \in \mathbb{Z}$ such that $a \times n = b$. Similarly, $b | a$ 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 $a | b$ and $b | a$, 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, $a \times \text{some integer} = b + c$ and $a \times \text{some integer} = b - c$ 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 :

$$\begin{aligned} 291/252 &= 1 = q_1 \\ 291 - (252 \times 1) &= 39 = r_2 \end{aligned}$$

(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 :

$$\begin{aligned} 252/39 &= 6 = q_2 \\ 252 - (39 \times 6) &= 18 = r_3 \end{aligned}$$

(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 :

$$\begin{aligned} 39/18 &= 2 = q_3 \\ 39 - (18 \times 2) &= 3 = r_4 \end{aligned}$$

(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 :

$$\begin{aligned} 18/3 &= 6 = q_4 \\ 18 - (3 \times 6) &= 0 = r_5 \end{aligned}$$

(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)

$$\begin{aligned} 85652/16261 &= 5 = q_1 \\ 85652 - (16261 \times 5) &= 4347 = r_2 \end{aligned}$$

(2)

$$\begin{aligned} 16261/4347 &= 3 = q_2 \\ 16261 - (4347 \times 3) &= 3220 = r_3 \end{aligned}$$

(3)

$$\begin{aligned} 4347/3220 &= 1 = q_3 \\ 4347 - (3220 \times 1) &= 1127 = r_4 \end{aligned}$$

(4)

$$\begin{aligned} 3220/1127 &= 2 = q_4 \\ 3220 - (1127 \times 2) &= 966 = r_5 \end{aligned}$$

(5)

$$\begin{aligned} 1127/966 &= 1 = q_5 \\ 1127 - (966 \times 1) &= 161 = r_6 \end{aligned}$$

(6)

$$\begin{aligned} 966/161 &= 6 = q_6 \\ 966 - (161 \times 6) &= 0 = r_7 \end{aligned}$$

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	<i>Formula</i>	<i>Evaluation</i>	v_i	<i>Formula</i>	<i>Evaluation</i>
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 $au + bv = 1$. 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 $\gcd(a, b) = 1$. \square



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 $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}$. \square



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)

$$5327 \cdot 6135 \pmod{8157} = 4203$$

$$4203 \cdot 7139 \pmod{8157} = 3771$$

$$3771 \cdot 2187 \pmod{8157} = 450$$

$$450 \cdot 5219 \pmod{8157} = 7491$$

$$7491 \cdot 1873 \pmod{8157} = \boxed{603}$$

(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 $x = 1, x = 2, \dots, x = m - 1$ 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 whose 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_1a_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, $a_1b_1 \equiv 1 \pmod{m}$ and $a_2b_2 \equiv 1 \pmod{m}$ for some $b_1, b_2 \in \mathbb{Z}$. When we multiply the equations together, we get $(a_1b_1)(a_2b_2) \equiv 1 \pmod{m}$ which can be rewritten as $(a_1a_2)(b_1b_2) \equiv 1 \pmod{m}$. We can multiply b_1 and b_2 to get an integer b_3 . Thus, when we multiply a_1a_2 by b_3 and get 1, we have shown that b_3 is a multiplicative inverse, and a_1a_2 is a unit modulo m . \square

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 2×2 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 $a = a^2 \pmod{256} = 17^2 \pmod{256} = 33$. $A = \lfloor 183/2 \rfloor = 91$.
- $A = 91$ 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, $a = a^2 \pmod{1000} = 296^2 \pmod{1000} = 616$
(devil's number!!!). $A = \lfloor 14/2 \rfloor = 7$.
- $A = 7$ 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 SAVAQ

- (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) WNOOA HTUFN EHRHE NESUV ICEME \Rightarrow “When I...”
- (2) WNOOA HTUFN EHRHE NESUV ICEME \Rightarrow “...N The C...”
- (3) WNOOA HTUFN EHRHE NESUV ICEME \Rightarrow “...ourse...”
- (4) WNOOA HTUFN EHRHE NESUV ICEME \Rightarrow “...Of Hum...”
- (5) WNOOA HTUFN EHRHE NESUV ICEME \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 $a^{-1} \pmod{p}$ 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:

$$\begin{aligned}
 a^{p-1} &\equiv 1 \pmod{p} \\
 a^{p-2} &\equiv a^{-1} \pmod{p} \\
 11^{45} &\pmod{47}
 \end{aligned}$$

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 $2^5 \cdot 2^3 \cdot 2^2 \cdot 2^1 \cdot 2^0 \Rightarrow 11^{2^5} \cdot 11^{2^3} \cdot 11^{2^2} \cdot 11^{2^1} \cdot 11^{2^0} \Rightarrow 11^{32} \cdot 11^8 \cdot 11^4 \cdot 11 \equiv 17 \cdot 14 \cdot 25 \cdot 11$. Now, let's find the values of these numbers:

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

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 $345^{2^9} \cdot 345^{2^6} \cdot 345^{2^3} \cdot 345^{2^0}$.

$$345^1 \equiv 345 \pmod{587}$$

$$345^2 \equiv 451 \pmod{587}$$

$$345^4 \equiv 299 \pmod{587}$$

$$345^8 \equiv 177 \pmod{587}$$

$$345^{16} \equiv 218 \pmod{587}$$

$$345^{64} \equiv 529 \pmod{587}$$

$$345^{128} \equiv 429 \pmod{587}$$

$$345^{256} \equiv 310 \pmod{587}$$

$$345^{512} \equiv 419 \pmod{587}$$

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) $p = 7$: $3^1 \equiv 3, 3^2 \equiv 2, \dots, 3^6 \equiv 1$, 3 is a primitive root.
- (iii) $p = 11$: $3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 5, \dots, 3^5 \equiv 1$, 3 is not a primitive root.
- (iv) $p = 17$: $3^1 \equiv 3, 3^2 \equiv 9, \dots, 3^{16} \equiv 1$, 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.

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

6 is a primitive root.

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

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.