

**An Introduction to Mathematical  
Cryptography  
Solution Manual**

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

©2008 by J. Hoffstein, J. Pipher, J.H. Silverman  
July 31, 2008

# Chapter 1

## An Introduction to Cryptography

### Exercises for Chapter 1

Section. Simple substitution ciphers

**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. (For your convenience, there is a cipher wheel that you can print and cut out at [www.math.brown.edu/~jhs/MathCrypto/CipherWheel.pdf](http://www.math.brown.edu/~jhs/MathCrypto/CipherWheel.pdf).)

- (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.

AOLYLHYLUVZLJYLAZILAALYA OHUAOLZLJYLALZAOHALCLYFIVKFNBZZLZ

- (c) Decrypt the following message, which was encrypted by rotating 1 clockwise for the first letter, then 2 clockwise for the second letter, etc.

XJHRFTNZHMZGAHIUETXZJNBWNUTRHEPOMDNBJMAUGORFAOIZOCC

Solution to Exercise 1.1.

- (a) a page of history is worth a volume of logic  
LALRPZQSTDEZCJTDHZCESLGZWFXPZQWZRTN

This quote is in a court decision of Oliver Wendell Holmes, Jr. (1921).

- (b) there are no secrets better than the secrets that everybody guesses  
AOLYLHYLUVZLJYLAZILAALYA OHUAOLZLJYLALZAOHALCLYFIVKFNBZZLZ

There are no secrets better than the secrets that everybody guesses.

This quote is due to George Bernard Shaw, *Mrs. Warren's Profession* (1893)

- (c) whenangrycounttenbeforeyouspeakifveryangryanhundred  
XJHRFTNZHMZGAHIUETXZJNBWNUTRHEPOMDNBJMAUGORFAOIZOCC

When angry, count ten before you speak; if very angry, an hundred.

This quote is due to Thomas Jefferson, *A Decalogue of Canons...* (1825).

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

- (a) LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBVDVWUHH  
(b) UXENRBWXCUXENFQRLQJUCNABFQNWRCJUCNAJCRXWORWMB  
(c) BGUTBMBGZTFHNLXMKTIIPBMAVAXXLXTEPTRLEXTOKHHFYHKMAXFHNLX

Solution to Exercise 1.2.

- (a) ithinkthatishallneverseeabillboardlovelyasatree  
LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBVDVWUHH

I think that I shall never see, a billboard lovely as a tree.

This quote is due to Ogden Nash, *Many Long Years Ago* (1945), Song of the Open Road.

- (b) loveisnotlovewhichalterswhenitalterationfinds  
UXENRBWXCUXENFQRLQJUCNABFQNWRCJUCNAJCRXWORWMB

Love is not love which alters when it alteration finds.

This quote is due to William Shakespeare, Sonnet 116.

- (c) inbaitingamousetrapwithcheesealwaysleaveroomforthemouse  
BGUTBMBGZTFHNLXMKTIIPBMAVAXXLXTEPTRLEXTOKHHFYHKMAXFHNLX

In baiting a mousetrap with cheese, always leave room for the mouse.

This quote is due to H.H. Munro (Saki), *The Square Egg* (1924).

**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.

- (b) Make a decryption table, that is, make a table in which the ciphertext alphabet is in order from A to Z and the plaintext alphabet is mixed up.  
(c) Use your decryption table from (b) to decrypt the following message.

IBXLX JVXIZ SLLDE VAQLL DEVAU QLB

Solution to Exercise 1.3.

- (a)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
S	C	J	A	X	U	F	B	Q	K	T	P	R	W	E	Z	H	V	L	I	G	Y	D	N	M	O

Table 1.1: Simple substitution encryption table for exercise 1.3

t	h	e	g	o	l	d	i	s	h	i	d	d	e	n	i	n	t	h	e	g	a	r	d	e	n
I	B	X	F	E	P	A	Q	L	B	Q	A	A	X	W	Q	W	I	B	X	F	S	V	A	X	W

Breaking it into five letter blocks gives the ciphertext

IBXFE PAQLB QAAXW QWIBX FSVAX W

(b)

d	h	b	w	o	g	u	q	t	c	j	s	y	x	z	l	i	m	a	k	f	r	n	e	v	p
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

(c)

t	h	e	s	e	c	r	e	t	p	a	s	s	w	o	r	d	i	s	s	w	o	r	d	f	i	s	h
I	B	X	L	X	J	V	X	I	Z	S	L	L	D	E	V	A	Q	L	L	D	E	V	A	U	Q	L	B

Putting in word breaks gives the plaintext

The secret password is swordfish.

**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 GKBJS  
 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

The ciphertext contains 316 letters. Here is a frequency table:

	R	J	I	L	Z	T	N	Q	B	G	K	U	M	O	S	H	W	F	E	D	X	V
Freq	33	30	27	25	24	20	19	16	15	15	13	12	12	10	9	8	7	6	5	5	3	2

The most frequent bigrams are: JN (11 times), NR (8 times), TQ (6 times), and LW, RB, RZ, and JL (5 times each).

- (b) “A Botanical Code”

KZRNK GJKIP ZBOOB XLCRG BXFAU GJBNG RIXRU XAFGJ BXRME MNKNG  
BURIX KJRXR SBUER ISATB UIBNN RTBUM NBIGK EBIGR OCUBR GLUBN  
JBGRL SJGLN GJBOR ISLRS BAFFO AZBUN RFAUS AGGBI NGLXM IAZRX  
RMNVL GEANG CJRUE KISRM BOOAZ GLOKW FAUKI NGRIC BEBRI NJAWB  
OBNNO ATBZJ KOBRC JKIRR NGBUE BRINK XKBAF QBROA LNMGR MALUF  
BBG

The ciphertext contains 253 letters. Here is a frequency table:

	B	R	G	N	A	I	U	K	O	J	L	X	M	F	S	E	Z	C	T	W	P	V	Q
Freq	32	28	22	20	16	16	14	13	12	11	10	10	8	8	7	7	6	5	3	2	1	1	1

The most frequent bigrams are: NG and RI (7 times each), BU (6 times), and BR (5 times).

- (c) In order to make this one a bit more challenging, we have removed all occurrences of the word “the” from the plaintext.

“A Brilliant Detective”

GSZES GNUBE SZGUG SNKGX CSUUE QNZOQ EOVJN VXKNG XGAHS AWSZZ  
BOVUE SIXCQ NQESX NGEUG AHZQA QHNSP CIPQA OIDL VJXGAK CGJCG  
SASUB FVQAV CIAWN VWOVP SNSXV JGPCV NODIX GJQAE VOOXC SXXCG  
OGOVA XGNVU BAVKX QZVQD LVJXQ EXCQD VKCQG AMVAX VWXCG OOBX  
VZCSO SPSPN VAXUB DVVAX QJQAJ VSUXC SXXCV OVJCS NSJXV NOJQA  
MVBSZ VOOSH VSAWX QHGMV GWVSX CSXXC VBSNV ZNVVN SAWQZ ORVXJ  
CVOQE JCGUW NVA

The ciphertext contains 313 letters. Here is a frequency table:

	V	S	X	G	A	O	Q	C	N	J	U	Z	E	W	B	P	I	H	K	D	M	L	R	F
Freq	39	29	29	22	21	21	20	20	19	13	11	11	10	8	8	6	5	5	5	4	3	2	1	1

The most frequent bigrams are: XC (10 times), NV (7 times), and CS, OV, QA, and SX (6 times each).

#### Solution to Exercise 1.4.

- (a) The message was encrypted using the table:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
I	E	B	H	R	W	D	N	T	P	X	U	O	Q	L	M	A	G	Z	J	K	V	F	C	S	Y

The plaintext reads:

“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, however, as would appear, to the crude intellect of the sailor, absolutely insoluble without the key.” (*The Gold-Bug*, 1843, Edgar Allan Poe)

- (b) The message was encrypted using the table:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
R	V	C	X	B	F	S	J	K	Q	P	O	E	I	A	W	D	U	N	G	L	T	Z	Y	M	H

The plaintext reads:

“I was, I think, well educated for the standard of the day. My sister and I had a German governess. A very sentimental creature. She taught us the language of flowers—a forgotten study nowadays, but most charming. A yellow tulip, for instance, means Hopeless Love, while a China Aster means I die of Jealousy at your feet.” (*The Four Suspects*, 1933, Agatha Christie)

(c) The message was encrypted using the table:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
S	D	J	W	V	E	H	C	G	L	R	U	Z	A	Q	P	T	N	O	X	I	M	K	Y	B	F

The plaintext reads (all occurrences of the word “the” were omitted from the text before encryption):

I am fairly familiar with all forms of secret writing, and am myself (the) author of a trifling monograph upon (the) subject, in which I analyze one hundred separate ciphers, but I confess that this is entirely new to me. (The) object of those who invented this system has apparently been to conceal that these characters convey a message, and to give (the) idea that they are (the) mere random sketches of children. (*The Adventure of the Dancing Men*, 1903, Sir Arthur Conan Doyle)

**1.5.** Suppose that you have an alphabet of 26 letters.

- How many possible simple substitution ciphers are there?
- A letter in the alphabet is said to be *fixed* if the encryption of the letter is the letter itself. How many simple substitution ciphers are there that leave:
  - no letters fixed?
  - at least one letter fixed?
  - exactly one letter fixed?
  - at least two letters fixed?

(Part (b) is quite challenging! You might try doing the problem first with an alphabet of four or five letters to get an idea of what is going on.)

Solution to Exercise 1.5.

(a) We can assign  $A$  to any of 26 letters, then  $B$  to any of the remaining 25 letters, etc. So there are  $26! = 403291461126605635584000000$  different simple substitution ciphers.

(b) Let  $\mathbf{S}(n, k)$  denote the number of permutations of  $n$  elements that fix at least  $k$  elements. You might guess that since there are  $\binom{n}{k}$  ways to choose  $k$  elements to fix and  $(n - k)!$  permutations of the remaining  $n - k$  elements,

$$\mathbf{S}(n, k) = \binom{n}{k} (n - k)! \quad \leftarrow \text{Incorrect Formula.} \quad (1.1)$$

But this overcounts because any permutation fixing more than  $n - k$  elements will be counted multiple times. We can, however, get a useful formula out of this mistake by modifying it somewhat. If we let  $\mathbf{R}(n, k)$  denote the number of permutations of  $n$  elements that fix *exactly*  $k$  elements, and  $!(n - k)$  (the subfactorial of  $(n - k)$ ) denote the number of permutations of  $n - k$  elements that fix no elements (such permutations are called *derangements*), then the following equation holds:

$$\mathbf{R}(n, k) = \binom{n}{k} !(n - k). \quad (1.2)$$

How can we compute  $!n$ ? One way would be to consider cycle decompositions of permutations of  $n$  elements, since any derangement of  $n$  elements decomposes into a disjoint union of cycles, with the size of the cycles summing to  $n$ . This, however, is only feasible for relatively small  $n$ . It would also be possible to formulate a recurrence relation, but a method following that tack would take several steps. We'll instead use the following fact:

$$!n = n! - \#\{\text{permutations that fix at least 1 element}\}. \quad (1.3)$$

Now if we notice that

$$\begin{aligned} \#\{\text{permutations that fix at least 1 element}\} &= \\ &\#\{\text{permutations that fix element 1}\} \\ &\cup \{\text{permutations that fix element 2}\} \\ &\cup \cdots \cup \{\text{permutations that fix element } n\} \end{aligned} \quad (1.4)$$

and use an analogue of the following formula in probability (often called the *inclusion-exclusion principle*):

$$\begin{aligned} P(E_1 \cup E_2 \cup \cdots \cup E_n) &= \sum_{i=1}^n P(E_i) + \sum_{i_1 < i_2} P(E_{i_1} \cap E_{i_2}) + \cdots \\ &\quad + (-1)^{r+1} \sum_{i_1 < i_2 < \cdots < i_r} P(E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_r}) + \cdots \\ &\quad + (-1)^{n+1} P(E_1 \cap E_2 \cap \cdots \cap E_n) \end{aligned} \quad (1.5)$$

we see that

$$\begin{aligned} !n &= \sum_{i=1}^n \#\{\text{permutations that fix element } i\} \\ &\quad - \sum_{i_1 < i_2} \#\{\text{permutations that fix elements } i_1 \text{ and } i_2\} + \cdots \\ &\quad + (-1)^{r+1} \sum_{i_1 < i_2 < \cdots < i_r} \#\{\text{permutations that fix elements } i_1, i_2, \dots, i_r\} + \cdots \\ &\quad + (-1)^{n+1} \#\{\text{permutations that fix everything}\}. \end{aligned} \quad (1.6)$$

Given  $k$  elements, the number of permutations fixing them is  $(n - k)!$  regardless of which  $k$  elements you fix, and there are  $\binom{n}{k}$  ways to choose  $k$  elements to fix. So the above equation becomes

$$\begin{aligned} !n &= \binom{n}{1}(n-1)! - \binom{n}{2}(n-2)! + \dots \\ &\quad + (-1)^{k+1} \binom{n}{k}(n-k)! + \dots + (-1)^{n+1}(n-n)!. \end{aligned} \quad (1.7)$$

Now noticing that

$$\binom{n}{k}(n-k)! = \frac{n!}{(n-k)!k!}(n-k)! = \frac{n!}{k!}, \quad (1.8)$$

the formula (??) becomes

$$!n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}. \quad (1.9)$$

This sum is somewhat cumbersome to compute when  $n$  is large, but notice that it resembles the series for  $e^{-1}$ . Thus

$$\sum_{k=0}^n \frac{(-1)^k}{k!} = e^{-1} - \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!}.$$

Since the series is alternating and the terms are decreasing in magnitude, each term is larger than the sum of the remaining terms (alternating series test). So

$$\left| \sum_{k=0}^n \frac{(-1)^k}{k!} - e^{-1} \right| < \frac{1}{(n+1)!}.$$

Multiplying by  $n!$  and using (??) yields

$$\left| !n - \frac{n!}{e} \right| < \frac{1}{n+1}.$$

Hence  $!n$  is the closest integer to  $n!/e$ .

Now that we're able to compute  $!n$ , we can compute

$$\mathbf{R}(n, k) = \binom{n}{k} !n - k = \binom{n}{k} \left\lfloor \frac{(n-k)!}{e} \right\rfloor,$$

and then we can compute  $\mathbf{S}(n, k)$  using

$$\mathbf{S}(n, k) = \sum_{j=k}^n \mathbf{R}(n, j) = n! - \sum_{j=0}^{k-1} \mathbf{R}(n, j). \quad (1.10)$$



(b-i) No letters fixed is  $\mathbf{R}(n, 0) = !n$  is the  $n^{\text{th}}$  derangement number. For  $n = 26$  we get

$$\begin{aligned}\mathbf{R}(26, 0) = !26 &= \lfloor 26!/e \rfloor = \lfloor 148362637348470135821287824.964 \rfloor \\ &= 148362637348470135821287825.\end{aligned}$$

(b-ii) At least one letter fixed is  $n!$  minus no letters fixed, so

$$\mathbf{S}(n, 1) = n! - \mathbf{R}(n, 0) = n! - !n = n! - \lfloor n!/e \rfloor.$$

Hence

$$\mathbf{S}(26, 1) = 26! - \lfloor 26!/e \rfloor = 254928823778135499762712175.$$

(b-iii) Exactly 1 letter fixed is

$$\mathbf{R}(n, 1) = n \cdot !(n-1) = n \left\lfloor \frac{(n-1)!}{e} \right\rfloor,$$

so

$$\mathbf{R}(26, 1) = 26 \left\lfloor \frac{25!}{e} \right\rfloor = 148362637348470135821287824.$$

(b-iv) At least two letters fixed is  $n!$  minus zero or one letters fixed, so

$$\begin{aligned}\mathbf{S}(n, 1) &= n! - \mathbf{R}(n, 0) - \mathbf{R}(1, 0) = n! - !n - n \cdot !(n-1) \\ &= n! - \lfloor n!/e \rfloor - n \lfloor (n-1)!/e \rfloor.\end{aligned}$$

Hence

$$\mathbf{S}(26, 1) = 26! - \lfloor 26!/e \rfloor - 26 \cdot \lfloor 25!/e \rfloor = 106566186429665363941424351.$$

#### Section. Divisibility and greatest common divisors

**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 to Exercise 1.6.

(a) By definition we have  $b = aA$  and  $c = bB$  for some integers  $A$  and  $B$ . Multiplying gives  $bc = aAbB$ , and dividing by  $b$  yields  $c = aAB$ . (Note that  $b$  is nonzero, since zero is not allowed to divide anything.) Hence  $c$  is an integer multiple of  $a$ , so  $a \mid c$ .

(b) By definition we have  $b = aA$  and  $a = bB$  for some integers  $A$  and  $B$ . Multiplying gives  $ab = aAbB$ , and dividing by  $ab$  yields  $1 = AB$ . (Note that  $a$

and  $b$  are nonzero, since zero is not allowed to divide anything.) But the only way for two integers to have product 1 is for  $A = B = \pm 1$ .

(c) By definition we have  $b = au$  and  $c = av$  for some integers  $u$  and  $v$ . Then

$$b \pm c = au \pm av = a(u \pm v),$$

so both  $b + c$  and  $b - c$  are integer multiples of  $a$ . Hence both are divisible by  $a$ .

**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.
- (c) 9829387493 divided by 873485.
- (d) 1498387487 divided by 76348.

*Solution to Exercise 1.7.*

- (a)  $a = 34787$ ,  $b = 353$ ,  $a/b = 98.54674221$ ,  $q = 98$ ,  $r = a - b \cdot q = 193$ .
- (b)  $a = 238792$ ,  $b = 7843$ ,  $a/b = 30.44651281$ ,  $q = 30$ ,  $r = a - b \cdot q = 3502$ .
- (c)  $a = 9829387493$ ,  $b = 873485$ ,  $a/b = 11253.06959249$ ,  $q = 11253$ ,  $r = a - b \cdot q = 60788$ .
- (d)  $a = 1498387487$ ,  $b = 76348$ ,  $a/b = 19625.75950909$ ,  $q = 19625$ ,  $r = a - b \cdot q = 57987$ .

**1.8.** Use a calculator and the method described in Remark 1.9 to compute the following remainders, without bothering to compute the associated quotients.

- (a) The remainder of 78745 divided by 127.
- (b) The remainder of 2837647 divided by 4387.
- (c) The remainder of 8739287463 divided by 18754.
- (d) The remainder of 4536782793 divided by 9784537.

*Solution to Exercise 1.8.*

- (a)  $a = 78745$ ,  $b = 127$ ,  $a/b = 620.03937008$ .

$$r \approx 127 \cdot 0.03937008 \approx 4.99999889, \quad \text{so } r = 5.$$

- (b)  $a = 2837647$ ,  $b = 4387$ ,  $a/b = 646.83086392$ .

$$r \approx 4387 \cdot 0.83086392 \approx 3644.99997317, \quad \text{so } r = 3645.$$

- (c)  $a = 8739287463$ ,  $b = 18754$ ,  $a/b = 465995.91889730$ .

$$r \approx 18754 \cdot 0.91889730 \approx 17232.99996420, \quad \text{so } r = 17233.$$

- (d)  $a = 4536782793$ ,  $b = 9784537$ ,  $a/b = 463.66862254$ .

$$r \approx 9784537 \cdot 0.66862254 \approx 6542161.98166398, \quad \text{so } r = 6542162.$$

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

- (a)  $\gcd(291, 252)$ .
- (b)  $\gcd(16261, 85652)$ .
- (c)  $\gcd(139024789, 93278890)$ .
- (d)  $\gcd(16534528044, 8332745927)$ .

Solution to Exercise 1.9.

- (a)  $\gcd(291, 252) = 3$ .
- (b)  $\gcd(16261, 85652) = 161$ .
- (c)  $\gcd(139024789, 93278890) = 1$ .
- (d)  $\gcd(16534528044, 8332745927) = 43$ .

**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 to Exercise 1.10.

- (a)  $291 \cdot 13 - 252 \cdot 15 = 3$
- (b)  $16261 \cdot 85573 - 85652 \cdot 16246 = 161$
- (c)  $139024789 \cdot 6944509 - 93278890 \cdot 10350240 = 1$
- (d)  $16534528044 \cdot 81440996 - 8332745927 \cdot 161602003 = 43$

**1.11.** Let  $a$  and  $b$  be positive integers.

- (a) Suppose that there are integers  $u$  and  $v$  satisfying  $au + bv = 1$ . Prove that  $\gcd(a, b) = 1$ .
- (b) Suppose that there are integers  $u$  and  $v$  satisfying  $au + bv = 6$ . Is it necessarily true that  $\gcd(a, b) = 6$ ? If not, give a specific counterexample, and describe in general all of the possible values of  $\gcd(a, b)$ ?
- (c) Suppose that  $(u_1, v_1)$  and  $(u_2, v_2)$  are two solutions in integers to the equation  $au + bv = 1$ . Prove that  $a$  divides  $v_2 - v_1$  and that  $b$  divides  $u_2 - u_1$ .
- (d) More generally, let  $g = \gcd(a, b)$  and let  $(u_0, v_0)$  be a solution in integers to  $au + bv = g$ . Prove that every other solution has the form  $u = u_0 + kb/g$  and  $v = v_0 - ka/g$  for some integer  $k$ . (This is the second part of Theorem 1.11.)

Solution to Exercise 1.11.

(a) Let  $g = \gcd(a, b)$ . Then  $a = gA$  and  $b = gB$  for some integers  $A$  and  $B$ . Substituting into the given equation  $au + bv = 1$  yields

$$1 = au + bv = gAu + gBv = g(Au + Bv).$$

Thus  $g$  divides 1, so we must have  $g = 1$ .

(c) No,  $au + bv = 6$  does not imply  $\gcd(a, b) = 6$ . For example, if  $\gcd(a, b) = 1$ , then we can solve  $aU + bV = 1$ , and multiplying this equation by 6 gives  $a(6U) + b(6V) = 6$ . For a specific counterexample, take  $a = 3$  and  $b = 2$ . Then

$$a \cdot 6 + b \cdot (-6) = 6,$$

but  $\gcd(a, b) = 1$ .

In general, if  $au + bv = c$  has a solution, then  $c$  divides  $\gcd(a, b)$ . To see this, let  $g = \gcd(a, b)$  and divide  $c$  by  $g$  with remainder, say

$$c = gq + r \quad \text{with } 0 \leq r < g.$$

We know that we can find a solution to  $g = ax + by$ , so we get

$$au + bv = c = gq + r = (ax + by)q + r.$$

Rearranging this yields

$$a(u - xq) + b(v - yq) = r.$$

In other words, we have a solution to  $aX + bY = r$  with  $0 \leq r < g$ . The left-hand side is divisible by  $g$ . (Remember that  $g = \gcd(a, b)$ , so  $g$  divides both  $a$  and  $b$ .) Hence  $g \mid r$ . But the only  $r$  satisfying  $0 \leq r < g$  and  $g \mid r$  is  $r = 0$ . Therefore  $c = gq$ , which completes the proof that  $\gcd(a, b)$  divides  $c$ .

(d) We are given that

$$au + bv = g \quad \text{and} \quad au_0 + bv_0 = g.$$

Subtracting and rearranging yields

$$a(u - u_0) = -b(v - v_0).$$

Dividing both sides by  $g$  gives

$$\frac{a}{g}(u - u_0) = -\frac{b}{g}(v - v_0).$$

We observe that  $\gcd(a/g, b/g) = 1$ . (To see this, we note that  $(a/g)u_0 + (b/g)v_0 = 1$ , so (a) tells us that  $\gcd(a/g, b/g) = 1$ .) Thus  $a/g$  divides  $(b/g)(v - v_0)$  and is relatively prime to  $(b/g)$ , so it must divide  $v - v_0$ . Hence

$$v - v_0 = \frac{a}{g}x \quad \text{for some integer } x.$$

The same reasoning tells us that

$$u - u_0 = \frac{b}{g}y \quad \text{for some integer } y.$$

Hence

$$u = u_0 + \frac{b}{g}y \quad \text{and} \quad v = v_0 + \frac{a}{g}x.$$

Substituting into the equation  $\frac{a}{g}(u - u_0) = -\frac{b}{g}(v - v_0)$  from above yields

$$\frac{a}{g} \frac{b}{g} y = -\frac{b}{g} \frac{a}{g} x,$$

so  $y = -x$ . If we use the letter  $k$  instead of the letter  $y$ , we have shown that

$$u = u_0 + \frac{b}{g}k \quad \text{and} \quad v = v_0 - \frac{a}{g}k,$$

which is exactly what we were trying to prove.

**1.12.** The method for solving  $au + bv = \gcd(a, b)$  described in Section 1.2 is somewhat inefficient. This exercise describes a method to compute  $u$  and  $v$  that is well suited for computer implementation. In particular, it uses very little storage.

- (a) Show that the following algorithm computes the greatest common divisor  $g$  of the positive integers  $a$  and  $b$ , together with a solution  $(u, v)$  in integers to the equation  $au + bv = \gcd(a, b)$ .
  1. Set  $u = 1$ ,  $g = a$ ,  $x = 0$ , and  $y = b$
  2. If  $y = 0$ , set  $v = (g - au)/b$  and return the values  $(g, u, v)$
  3. Divide  $g$  by  $y$  with remainder,  $g = qy + t$ , with  $0 \leq t < y$
  4. Set  $s = u - qx$
  5. Set  $u = x$  and  $g = y$
  6. Set  $x = s$  and  $y = t$
  7. Go To Step (2)
- (b) Implement the above algorithm on a computer using the computer language of your choice.
- (c) Use your program to compute  $g = \gcd(a, b)$  and integer solutions to the equation  $au + bv = g$  for the following pairs  $(a, b)$ .
  - (i) (527, 1258)
  - (ii) (228, 1056)
  - (iii) (163961, 167181)
  - (iv) (3892394, 239847)
- (d) What happens to your program if  $b = 0$ ? Fix the program so that it deals with this case correctly.
- (e) It is often useful to have a solution with  $u > 0$ . Modify your program so that it returns a solution with  $u > 0$  and  $u$  as small as possible. [*Hint.* If  $(u, v)$  is a solution, then so is  $(u + b/g, v - a/g)$ .] Redo (c) using your modified program.

Solution to Exercise 1.12.

- (a) A solution for this exercise is not currently available.
- (b) A solution for this exercise will not be provided.
- (c) and (e): (i)  $527 \cdot 43 - 1258 \cdot 18 = 17$   
 (ii)  $228 \cdot 51 - 1056 \cdot 11 = 12$   
 (iii)  $163961 \cdot 4517 - 167181 \cdot 4430 = 7$

$$(iv) 3892394 \cdot 59789 - 239847 \cdot 970295 = 1$$

(d) If  $b = 0$ , then there is a “division by zero” error in step 2. So the program should check if  $b = 0$ , if in that case it should return  $(a, 1, 0)$ .

**1.13.** Let  $a_1, a_2, \dots, a_k$  be integers with  $\gcd(a_1, a_2, \dots, a_k) = 1$ , i.e., the largest positive integer dividing all of  $a_1, \dots, a_k$  is 1. Prove that the equation

$$a_1u_1 + a_2u_2 + \dots + a_ku_k = 1$$

has a solution in integers  $u_1, u_2, \dots, u_k$ . (*Hint.* Repeatedly apply the extended Euclidean algorithm, Theorem 1.11. You may find it easier to prove a more general statement in which  $\gcd(a_1, \dots, a_k)$  is allowed to be larger than 1.)

Solution to Exercise 1.13.

We prove more generally that for any integers  $a_1, \dots, a_k$  (not all zero), there is a solution to

$$a_1u_1 + a_2u_2 + \dots + a_ku_k = \gcd(a_1, \dots, a_k).$$

We give the proof using induction on  $k$ . If  $k = 1$  there is nothing to prove, since  $a_1 \cdot 1 = \gcd(a_1)$ . For  $k = 2$ , this is already proven in the extended Euclidean algorithm. So assume now that we know the result for fewer than  $k$  integers, where  $k \geq 3$ , and we want to prove it for  $k$  integers. By the induction hypothesis, we can find a solution to

$$a_1u_1 + a_2u_2 + \dots + a_{k-1}u_{k-1} = \gcd(a_1, \dots, a_{k-1}).$$

To ease notation, we let  $b = \gcd(a_1, \dots, a_{k-1})$ . We apply the extended Euclidean algorithm to the two numbers  $b$  and  $a_k$ , which gives us a solution to

$$bv + a_kw = \gcd(b, a_k).$$

Multiplying the earlier equation by  $v$  and substituting this equation gives

$$\begin{aligned} a_1u_1v + a_2u_2v + \dots + a_{k-1}u_{k-1}v &= \gcd(a_1, \dots, a_{k-1})v \\ &= bv \quad \text{by definition of } b, \\ &= -a_kw + \gcd(b, a_k). \end{aligned}$$

Hence

$$a_1u_1v + a_2u_2v + \dots + a_{k-1}u_{k-1}v + a_kw = \gcd(b, a_k).$$

This completes the proof, since from the definition of  $\gcd$  as the largest integer dividing all of the listed integers, it's clear that

$$\gcd(b, a_k) = \gcd(\gcd(a_1, \dots, a_{k-1}), a_k) = \gcd(a_1, \dots, a_{k-1}, a_k).$$

Section. Modular arithmetic

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

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

Prove that

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

(This is Proposition 1.13(a).)

*Solution to Exercise 1.14.*

**1.15.** Write out the following tables for  $\mathbb{Z}/m\mathbb{Z}$  and  $(\mathbb{Z}/m\mathbb{Z})^*$ , as we did in Figures 1.4 and 1.5.

- (a) Make addition and multiplication tables for  $\mathbb{Z}/3\mathbb{Z}$ .
- (b) Make addition and multiplication tables for  $\mathbb{Z}/6\mathbb{Z}$ .
- (c) Make a multiplication table for the unit group  $(\mathbb{Z}/9\mathbb{Z})^*$ .
- (d) Make a multiplication table for the unit group  $(\mathbb{Z}/16\mathbb{Z})^*$ .

*Solution to Exercise 1.15.*

(a)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(b)

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(c)

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

(d)

·	1	3	5	7	9	11	13	15
1	1	3	5	7	9	11	13	15
3	3	9	15	5	11	1	7	13
5	5	15	9	3	13	7	1	11
7	7	5	3	1	15	13	11	9
9	9	11	13	15	1	3	5	7
11	11	1	7	13	3	9	15	5
13	13	7	1	11	5	15	9	3
15	15	13	11	9	7	5	3	1

**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)  $347 + 513 \equiv \boxed{\phantom{000}} \pmod{763}$ .  
 (b)  $3274 + 1238 + 7231 + 6437 \equiv \boxed{\phantom{0000}} \pmod{9254}$ .  
 (c)  $153 \cdot 287 \equiv \boxed{\phantom{000}} \pmod{353}$ .  
 (d)  $357 \cdot 862 \cdot 193 \equiv \boxed{\phantom{000}} \pmod{943}$ .  
 (e)  $5327 \cdot 6135 \cdot 7139 \cdot 2187 \cdot 5219 \cdot 1873 \equiv \boxed{\phantom{0000}} \pmod{8157}$ .  
 (*Hint.* After each multiplication, reduce modulo 8157 before doing the next multiplication.)  
 (f)  $137^2 \equiv \boxed{\phantom{000}} \pmod{327}$ .  
 (g)  $373^6 \equiv \boxed{\phantom{000}} \pmod{581}$ .  
 (h)  $23^3 \cdot 19^5 \cdot 11^4 \equiv \boxed{\phantom{000}} \pmod{97}$ .

Solution to Exercise 1.16.

- (a)  $347 + 513 \equiv \boxed{97} \pmod{763}$ .  
 (b)  $3274 + 1238 + 7231 + 6437 \equiv \boxed{8926} \pmod{9254}$ .  
 (c)  $153 \cdot 287 \equiv \boxed{139} \pmod{353}$ .  
 (d)  $357 \cdot 862 \cdot 193 \equiv \boxed{636} \pmod{943}$ .  
 (e)  $5327 \cdot 6135 \cdot 7139 \cdot 2187 \cdot 5219 \cdot 1873 \equiv \boxed{603} \pmod{8157}$ .  
 (f)  $137^2 \equiv \boxed{130} \pmod{327}$ .  
 (g)  $373^6 \equiv \boxed{463} \pmod{581}$ .  
 (h)  $23^3 \cdot 19^5 \cdot 11^4 \equiv \boxed{93} \pmod{97}$ .

**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)  $x + 17 \equiv 23 \pmod{37}$ .  
 (b)  $x + 42 \equiv 19 \pmod{51}$ .  
 (c)  $x^2 \equiv 3 \pmod{11}$ .  
 (d)  $x^2 \equiv 2 \pmod{13}$ .  
 (e)  $x^2 \equiv 1 \pmod{8}$ .



- (f)  $x^3 - x^2 + 2x - 2 \equiv 0 \pmod{11}$ .  
 (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 to Exercise 1.17.*

- (a)  $x \equiv 23 - 17 \equiv \boxed{6} \pmod{37}$ .  
 (b)  $x \equiv 19 - 42 \equiv -23 \equiv \boxed{28} \pmod{51}$ .  
 (c) The squares modulo 11 are  $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 16 \equiv 5$ , etc. The full list is  $\{0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1\}$ . Thus  $5^2 \equiv 2 \pmod{11}$  and  $6^2 \equiv 2 \pmod{11}$ , so there are two solutions,  $\boxed{x = 5 \text{ and } x = 6}$ .  
 (d) The squares modulo 13 are  $\{0, 1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1\}$ . Thus  $x^2 \equiv 2 \pmod{13}$  has  $\boxed{\text{no solutions}}$ .  
 (e) The solutions to  $x^2 \equiv 1 \pmod{8}$  are  $\boxed{x = 1, x = 3, x = 5 \text{ and } x = 7}$ .  
 (f) Plugging  $x = 0, 1, 2, \dots, 10$  into  $x^3 - x^2 + 2x - 2$  and reducing modulo 11, we find the three solutions  $\boxed{x = 1, x = 3, \text{ and } x = 8}$ .  
 (g) One method is to try all values  $x = 0, 1, 2, \dots, 34$ . A faster method is to list the solutions to  $x \equiv 1 \pmod{5}$ , namely  $1, 6, 11, 16, 21, 26, 31, \dots$  and reduce them modulo 7 to see which ones are congruent to 2 modulo 7. Thus working modulo 7,

$$1 \equiv 1, \quad 6 \equiv 6, \quad 11 \equiv 4, \quad 16 \equiv 2, \quad 21 \equiv 0, \quad 26 \equiv 5, \quad 31 \equiv 3.$$

Thus the solution is  $\boxed{x = 16}$ .

**1.18.** Suppose that  $g^a \equiv 1 \pmod{m}$  and that  $g^b \equiv 1 \pmod{m}$ . Prove that

$$g^{\gcd(a,b)} \equiv 1 \pmod{m}.$$

*Solution to Exercise 1.18.*

The extended Euclidean algorithm says that there are integers  $u$  and  $v$  satisfying  $au + bv = \gcd(a, b)$ . Then

$$g^{\gcd(a,b)} \equiv g^{au+bv} \equiv (g^a)^u \cdot (g^b)^v \equiv 1^u \cdot 1^v \equiv 1 \pmod{p}.$$

**1.19.** Prove that if  $a_1$  and  $a_2$  are units modulo  $m$ , then  $a_1 a_2$  is a unit modulo  $m$ .

*Solution to Exercise 1.19.*

By definition of unit, there are numbers  $b_1$  and  $b_2$  so that

$$a_1 b_1 \equiv 1 \pmod{m} \quad \text{and} \quad a_2 b_2 \equiv 1 \pmod{m}.$$

Then

$$(a_1 a_2)(b_1 b_2) \equiv (a_1 b_1)(a_2 b_2) \equiv 1 \cdot 1 \equiv 1 \pmod{m},$$

so  $a_1 a_2$  is a unit. Its inverse is  $b_1 b_2$ .

**1.20.** Prove that  $m$  is prime if and only if  $\phi(m) = m - 1$ , where  $\phi$  is Euler's phi function.

*Solution to Exercise 1.20.*

Suppose first that  $m$  is prime. Let  $k$  be any number between 1 and  $m - 1$  and let  $d = \gcd(k, m)$ . Then  $d \mid m$ , so the fact that  $m$  is prime tells us that either  $d = 1$  or  $d = m$ . But also  $d \mid k$  and  $1 \leq k < m$ , so we have  $d < m$ . Hence  $d = 1$ . This proves that every number  $k$  between 1 and  $m - 1$  satisfies  $\gcd(k, m) = 1$ . Hence

$$\phi(m) = \#\{1 \leq k < m : \gcd(k, m) = 1\} = \#\{1, 2, 3, \dots, m - 1\} = m - 1.$$

Next suppose that  $\phi(m) = m - 1$ . This means that every number  $k$  between 1 and  $m - 1$  satisfies  $\gcd(k, m) = 1$ . Suppose that  $d$  divides  $m$  and that  $d \neq m$ . Then  $1 \leq d \leq m - 1$ , so  $\gcd(d, m) = 1$ . But the fact that  $d$  divides  $m$  implies that  $\gcd(d, m) = d$ . Hence  $d = 1$ . This proves that the only divisors of  $m$  are 1 and  $m$ , so  $m$  is prime.

**1.21.** Let  $m \in \mathbb{Z}$ .

- (a) Suppose that  $m$  is odd. What integer between 1 and  $m - 1$  equals  $2^{-1} \bmod m$ ?
- (b) More generally, suppose that  $m \equiv 1 \pmod{b}$ . What integer between 1 and  $m - 1$  is equal to  $b^{-1} \bmod m$ ?

*Solution to Exercise 1.21.*

- (a) The fact that  $m$  is odd means that  $\left\lfloor \frac{m+1}{2} \right\rfloor$  is an integer, and clearly

$$2 \cdot \frac{m+1}{2} = m+1 \equiv 1 \pmod{m}.$$

- (b) The assumption that  $m \equiv 1 \pmod{b}$  means that  $\frac{m-1}{b}$  is an integer, so we have

$$b \cdot \frac{m-1}{b} = m-1 \equiv -1 \pmod{m}.$$

This is almost what we want, so multiply by  $-1$  to get

$$b \cdot \frac{1-m}{b} = 1-m \equiv 1 \pmod{m}.$$

Unfortunately,  $\frac{1-m}{b}$  is negative, but we can add on multiples of  $m$  without changing its value modulo  $m$ . Thus  $\frac{1-m}{b} + m = \frac{1+(b-1)m}{b}$  is an integer and

$$b \cdot \frac{1+(b-1)m}{b} = 1+(b-1)m \equiv 1 \pmod{m}.$$

Hence  $b^{-1} \bmod m$  is equal to  $\left\lfloor \frac{1+(b-1)m}{b} \right\rfloor$ .

**1.22.** Let  $m$  be an odd integer and let  $a$  be any integer. Prove that  $2m + a^2$  can never be a perfect square. (*Hint.* If a number is a perfect square, what are its possible values modulo 4?)

Solution to Exercise 1.22.

Any number squared is either 0 or 1 modulo 4. But

$$2m + a^2 \equiv 2 + a^2 \equiv \begin{cases} 2 + 0 \equiv 2 & \text{if } a \text{ is even,} \\ 2 + 1 \equiv 3 & \text{if } a \text{ is odd.} \end{cases}$$

Thus  $2m + a^2$  is either 2 or 3 modulo 4, so it can never be a perfect square.

**1.23.** (a) Find a single value  $x$  that simultaneously solves the two congruences

$$x \equiv 3 \pmod{7} \quad \text{and} \quad x \equiv 4 \pmod{9}.$$

(*Hint.* Note that every solution of the first congruence looks like  $x = 3 + 7y$  for some  $y$ . Substitute this into the second congruence and solve for  $y$ ; then use that to get  $x$ .)

(b) Find a single value  $x$  that simultaneously solves the two congruences

$$x \equiv 13 \pmod{71} \quad \text{and} \quad x \equiv 41 \pmod{97}.$$

(c) Find a single value  $x$  that simultaneously solves the three congruences

$$x \equiv 4 \pmod{7}, \quad x \equiv 5 \pmod{8}, \quad \text{and} \quad x \equiv 11 \pmod{15}.$$

(d) Prove that if  $\gcd(m, n) = 1$ , then the pair of congruences

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

has a solution for any choice of  $a$  and  $b$ . Also give an example to show that the condition  $\gcd(m, n) = 1$  is necessary.

Solution to Exercise 1.23.

(a)  $x = 31$  (b)  $x = 5764$  (c)  $x = 221$

(d) The solutions to the first congruence look like  $x = a + my$  for any integer  $y$ . Substituting into the second congruence yields

$$a + my \equiv b \pmod{n},$$

so we want to find a value of  $z$  such that

$$a + my - b = nz.$$

In other words, we need integers  $y$  and  $z$  satisfying

$$my - nz = b - a.$$

We are given that  $\gcd(m, n) = 1$ , so we can find integers  $u$  and  $v$  satisfying  $mu + nv = 1$ . Multiplying this by  $b - a$  gives

$$mu(b - a) + nv(b - a) = b - a,$$

so we can take  $y = u(b - a)$  and  $z = v(b - a)$ . Then we have  $x = a + my = a + mu(b - a)$ .

To summarize, we first solve  $mu + nv = 1$  and then we take

$$x = a + mu(b - a) = a + (1 - nv)(b - a) = b + nv(b - a).$$

The two expressions for  $x$  show that  $x \equiv a \pmod{m}$  and  $x \equiv v \pmod{n}$ .

This exercise is a special case of the Chinese remainder theorem, which is covered in Chapter 2.

**1.24.** Let  $N$ ,  $g$ , and  $A$  be positive integers (note that  $N$  need not be prime). Prove that the following algorithm, which is a low-storage variant of the square-and-multiply algorithm described in Section 1.3.2, returns the value  $g^A \pmod{N}$ . (In Step 4 we use the notation  $\lfloor x \rfloor$  to denote the greatest integer function, i.e., round  $x$  down to the nearest integer.)

**Input.** Positive integers  $N$ ,  $g$ , and  $A$ .

1. Set  $a = g$  and  $b = 1$ .
2. Loop while  $A > 0$ .
  3. If  $A \equiv 1 \pmod{2}$ , set  $b = b \cdot a \pmod{N}$ .
  4. Set  $a = a^2 \pmod{N}$  and  $A = \lfloor A/2 \rfloor$ .
  5. If  $A > 0$ , continue with loop at Step 2.
6. Return the number  $b$ , which equals  $g^A \pmod{N}$ .

Solution to Exercise 1.24.

\*\*\* fill in solution

**1.25.** Use the square-and-multiply algorithm described in Section 1.3.2, or the more efficient version in Exercise 1.24, to compute the following powers.

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

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

(c)  $11^{507} \pmod{1237}$ .

Solution to Exercise 1.25.

$$(a) \quad 183 = 1 + 2 + 2^2 + 2^4 + 2^5 + 2^7, \quad 17^{183} \pmod{256} = \boxed{113}.$$

$$(b) \quad 477 = 1 + 2^2 + 2^3 + 2^4 + 2^6 + 2^7 + 2^8, \quad 2^{477} \pmod{1000} = \boxed{272}$$

$$(c) \quad 507 = 1 + 2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7 + 2^8, \quad 11^{507} \pmod{1237} = \boxed{322}.$$

Section. Prime numbers, unique factorization, and finite fields

**1.26.** Let  $\{p_1, p_2, \dots, p_r\}$  be a set of prime numbers, and let

$$N = p_1 p_2 \cdots p_r + 1.$$

Prove that  $N$  is divisible by some prime not in the original set. Use this fact to deduce that there must be infinitely many prime numbers. (This proof of the infinitude of primes appears in Euclid's *Elements*. Prime numbers have been studied for thousands of years.)

Solution to Exercise 1.26.

Let  $q$  be any prime that divides  $N$ . (Since  $N \geq 2$ , we know that it must be divisible by some prime.) Suppose that  $q$  were equal to some  $p_i$ . Then we would have

$$1 = N - p_1 p_2 \cdots p_r \equiv 0 \pmod{q},$$

since  $q$  would divide both of the terms  $N$  and  $p_1 \cdots p_r$ . But then  $q \mid 1$ , which is impossible. Therefore  $q$  is not equal to any of the  $p_i$ 's.

Next suppose that there were only finitely many primes. That means we can list them, say  $p_1, p_2, \dots, p_r$ . But from the first part of the exercise, we can create a new prime that's not in our list. This contradicts the assumption that there are finitely many primes, and hence proves that there must be infinitely many primes.

**1.27.** Without using the fact that every integer has a unique factorization into primes, prove that if  $\gcd(a, b) = 1$  and if  $a \mid bc$ , then  $a \mid c$ . (*Hint.* Use the fact that it is possible to find a solution to  $au + bv = 1$ .)

Solution to Exercise 1.27.

From the extended Euclidean algorithm, we can solve  $au + bv = 1$ . Multiply by  $c$  to get  $acu + bcv = c$ . We are given that  $a \mid bc$ , so there is an integer  $d$  satisfying  $bc = ad$ . Substituting this gives  $acu + adv = c$ . Thus  $a(cu + dv) = c$ , which shows that  $a \mid c$ .

**1.28.** Compute the following  $\text{ord}_p$  values:

- (a)  $\text{ord}_2(2816)$ .
- (b)  $\text{ord}_7(2222574487)$ .
- (c)  $\text{ord}_p(46375)$  for each of  $p = 3, 5, 7$ , and  $11$ .

Solution to Exercise 1.28.

- (a)  $\text{ord}_2(2816) = 8$ .
- (b)  $\text{ord}_7(2222574487) = 5$ .
- (c) Let  $a = 46375$ . Then  $\text{ord}_3(a) = 0$ ,  $\text{ord}_5(a) = 3$ ,  $\text{ord}_7(a) = 1$ ,  $\text{ord}_{11}(a) = 0$ .

**1.29.** Let  $p$  be a prime number. Prove that  $\text{ord}_p$  has the following properties.

- (a)  $\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b)$ . (Thus  $\text{ord}_p$  resembles the logarithm function, since it converts multiplication into addition!)
- (b)  $\text{ord}_p(a + b) \geq \min\{\text{ord}_p(a), \text{ord}_p(b)\}$ .
- (c) If  $\text{ord}_p(a) \neq \text{ord}_p(b)$ , then  $\text{ord}_p(a + b) = \min\{\text{ord}_p(a), \text{ord}_p(b)\}$ .

A function satisfying properties (a) and (b) is called a *valuation*.

Solution to Exercise 1.29.

(a) By definition of  $\text{ord}_p$ , we have

$$a = p^{\text{ord}_p(a)} A \quad \text{and} \quad b = p^{\text{ord}_p(b)} B \quad \text{with} \quad p \nmid A \quad \text{and} \quad p \nmid B.$$

Then

$$ab = p^{\text{ord}_p(a)} A \cdot p^{\text{ord}_p(b)} B = p^{\text{ord}_p(a) + \text{ord}_p(b)} AB \quad \text{with} \quad p \nmid AB,$$

so by definition,

$$\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b).$$

(b) We continue with the notation from (a) and, without loss of generality, we switch  $a$  and  $b$  if necessary so that  $\text{ord}_p(a) \geq \text{ord}_p(b)$ . Then

$$a + b = p^{\text{ord}_p(a)} A + p^{\text{ord}_p(b)} B = p^{\text{ord}_p(b)} \left( p^{\text{ord}_p(a) - \text{ord}_p(b)} A + B \right).$$

Thus  $p^{\text{ord}_p(b)} \mid a + b$ , so by definition of  $\text{ord}_p$  we have

$$\text{ord}_p(a + b) \geq \text{ord}_p(b).$$

(Note that we've set things up so that  $\text{ord}_p(b) = \min\{\text{ord}_p(a), \text{ord}_p(b)\}$ , so this is the result that we want.)

(c) We continue with the notation from (a) and (b), but for this part we are given that  $\text{ord}_p(a) > \text{ord}_p(b)$ . We also know that  $p \nmid B$ , so it follows that

$$p \nmid \left( p^{\text{ord}_p(a) - \text{ord}_p(b)} A + B \right),$$

since the exponent of  $p$  on the first term is positive. Hence  $p^{\text{ord}_p(b)}$  is the largest power of  $p$  dividing  $a + b$ , which proves that

$$\text{ord}_p(a + b) = \text{ord}_p(b).$$

### Section. Powers and primitive roots in finite fields

**1.30.** For each of the following primes  $p$  and numbers  $a$ , compute  $a^{-1} \bmod p$  in two ways: (i) Use the extended Euclidean algorithm. (ii) Use the fast power algorithm and Fermat's little theorem. (See Example 1.28.)

- (a)  $p = 47$  and  $a = 11$ .
- (b)  $p = 587$  and  $a = 345$ .
- (c)  $p = 104801$  and  $a = 78467$ .

Solution to Exercise 1.30.

(a) (i) We use the extended Euclidean algorithm to solve

$$11u + 47v = 1.$$

The solution is  $(u, v) = (-17, 4)$ , so  $11^{-1} \equiv -17 \equiv 30 \pmod{47}$ . (ii) Fermat's little theorem gives

$$11^{-1} \equiv 11^{45} \equiv 30 \pmod{47}.$$

(b) (i) We use the extended Euclidean algorithm to solve

$$345u + 587v = 1.$$

The solution is  $(u, v) = (114, -67)$ , so  $345^{-1} \equiv 114 \pmod{587}$ . (ii) Fermat's little theorem gives

$$345^{-1} \equiv 345^{585} \equiv 114 \pmod{587}.$$

(c) (i) We use the extended Euclidean algorithm to solve

$$78467u + 104801v = 1.$$

The solution is  $(u, v) = (1763, -1320)$ , so  $78467^{-1} \equiv 1763 \pmod{104801}$ . (ii) Fermat's little theorem gives

$$78467^{-1} \equiv 78467^{104799} \equiv 1763 \pmod{104801}.$$

**1.31.** Let  $p$  be a prime and let  $q$  be a prime that divides  $p - 1$ .

- (a) Let  $a \in \mathbb{F}_p^*$  and let  $b = a^{(p-1)/q}$ . Prove that either  $b = 1$  or else  $b$  has order  $q$ . (Recall that the order of  $b$  is the smallest  $k \geq 1$  such that  $b^k = 1$  in  $\mathbb{F}_p^*$ . *Hint.* Use Proposition 1.30.)
- (b) Suppose that we want to find an element of  $\mathbb{F}_p^*$  of order  $q$ . Using (a), we can randomly choose a value of  $a \in \mathbb{F}_p^*$  and check whether  $b = a^{(p-1)/q}$  satisfies  $b \neq 1$ . How likely are we to succeed? In other words, compute the value of the ratio

$$\frac{\#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} \neq 1\}}{\#\mathbb{F}_p^*}.$$

(*Hint.* Use Theorem 1.31.)

Solution to Exercise 1.31.

(a) Let  $k$  be the order of  $b$ , i.e., the smallest exponent such that  $b^k = 1$ . We know that  $b^q = a^{p-1} = 1$  from Fermat's little theorem. Then Proposition 1.30 tells us that  $k$  divides  $q$ , and since  $q$  is prime, it follows that either  $k = q$  or  $k = 1$ . Thus either  $b$  has order  $q$ , or else it has order 1, in which case  $b = b^1 = 1$ .

(b) Let  $g \in \mathbb{F}_p^*$  be a primitive root. Then every  $a \in \mathbb{F}_p^*$  has the form  $g^i$  for some  $0 \leq i < p - 1$ . We'll count the number of  $a$  with  $a^{(p-1)/q} = 1$ . Thus

$$\begin{aligned}\#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} = 1\} &= \#\{0 \leq i < p-1 : (g^i)^{(p-1)/q} = 1\} \\ &= \#\{0 \leq i < p-1 : g^{i(p-1)/q} = 1\}.\end{aligned}$$

Since  $g$  has order  $p-1$ , we have  $g^k = 1$  if and only if  $p-1 \mid k$ . Hence

$$g^{i(p-1)/q} = 1 \iff p-1 \mid i(p-1)/q \iff q \mid i.$$

Hence

$$\#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} = 1\} = \#\{0 \leq i < p-1 : q \mid i\} = \frac{p-1}{q}.$$

It follows that

$$\begin{aligned}\#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} \neq 1\} &= p-1 - \#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} = 1\} \\ &= p-1 - \frac{p-1}{q} = (p-1) \left(1 - \frac{1}{q}\right).\end{aligned}$$

Hence

$$\frac{\#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} \neq 1\}}{\#\mathbb{F}_p^*} = 1 - \frac{1}{q},$$

so if  $q$  is large, we have a very good chance of succeeding on our first try.

**1.32.** 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 1.33.
- (e) Write a computer program to check for primitive roots and use it to find all primitive roots modulo 229. Verify that there are exactly  $\phi(229)$  of them.
- (f) Use your program from (e) to find all primes less than 100 for which 2 is a primitive root.
- (g) Repeat the previous exercise to find all primes less than 100 for which 3 is a primitive root. Ditto to find the primes for which 4 is a primitive root.

Solution to Exercise 1.32.

- (a) (i) No. (ii) Yes. (iii) Yes. (iv) No.
- (b) (i) Yes. (ii) Yes. (iii) No. (iv) Yes.
- (c) In each case, we list the smallest primitive root



(i)  $p = 23, g = 5$ . (ii)  $p = 29, g = 2$ . (iii)  $p = 41, g = 6$ . (iv)  $p = 43, g = 3$ .  
 (d) The primitive roots modulo 11 are  $\{2, 6, 7, 8\}$ . There are  $\phi(10) = 4$  of them.

(e) The primitive roots modulo 229 are

$\{6, 7, 10, 23, 24, 28, 29, 31, 35, 38, 39, 40, 41, 47, 50, 59, 63, 65, 66,$   
 $67, 69, 72, 73, 74, 77, 79, 87, 90, 92, 96, 98, 102, 105, 110, 112, 113,$   
 $116, 117, 119, 124, 127, 131, 133, 137, 139, 142, 150, 152, 155, 156, 157,$   
 $160, 162, 163, 164, 166, 170, 179, 182, 188, 189, 190, 191, 194, 198, 200,$   
 $201, 205, 206, 219, 222, 223\}.$

There are exactly  $\phi(228) = 72$  of them.

(f) 2 is a primitive root modulo  $p$  for  $p \in \{3, 5, 11, 1319, 29, 37, 53, 59, 61, 67, 83\}$  and for no other primes less than 100. It is conjectured that 2 is a primitive root for infinitely many primes (Artin's conjecture).

(g) 3 is a primitive root modulo  $p$  for  $p \in \{5, 7, 17, 19, 29, 31, 43, 53, 79, 89\}$  and for no other primes less than 100. On the other hand, there are no primes for which 4 is a primitive root. This is because  $4 = 2^2$  is a square, so the powers of 4 can hit at most half of the possible nonzero values modulo  $p$ .

**1.33.** Let  $p$  be a prime such that  $q = \frac{1}{2}(p - 1)$  is also prime. Suppose that  $g$  is an integer satisfying

$$g \not\equiv \pm 1 \pmod{p} \quad \text{and} \quad g^q \not\equiv 1 \pmod{p}.$$

Prove that  $g$  is a primitive root modulo  $p$ .

*Solution to Exercise 1.33.*

Let  $n$  be the order of  $g$ , i.e., the smallest power of  $g$  that is congruent to 1. Then  $n$  divides  $p - 1$  from Proposition 1.30. Since  $p - 1 = 2q$  with  $q$  prime, this means that

$$n = 1 \quad \text{or} \quad n = 2 \quad \text{or} \quad n = q \quad \text{or} \quad n = 2q.$$

We are given that  $g \not\equiv \pm 1 \pmod{p}$ , so  $n \neq 1$  and  $n \neq 2$ , and we are also given that  $g^q \not\equiv \pm 1 \pmod{p}$ , so  $n \neq q$ . The only value left is  $n = 2q$ . This proves that  $n = p - 1$ , so  $g$  is a primitive root modulo  $p$ .

**1.34.** This exercise begins the study of squares and square roots modulo  $p$ .

(a) Let  $p$  be an odd prime number and let  $b$  be an integer with  $p \nmid b$ . Prove that either  $b$  has two square roots modulo  $p$  or else  $b$  has no square roots modulo  $p$ . In other words, prove that the congruence

$$X^2 \equiv b \pmod{p}$$

has either two solutions or no solutions in  $\mathbb{Z}/p\mathbb{Z}$ . (What happens for  $p = 2$ ? What happens if  $p \mid b$ ?)

- (b) For each of the following values of  $p$  and  $b$ , find all of the square roots of  $b$  modulo  $p$ .
- (i)  $(p, b) = (7, 2)$                       (ii)  $(p, b) = (11, 5)$   
 (iii)  $(p, b) = (11, 7)$                       (iv)  $(p, b) = (37, 3)$
- (c) How many square roots does 29 have modulo 35? Why doesn't this contradict the assertion in (a)?
- (d) Let  $p$  be an odd prime and let  $g$  be a primitive root modulo  $p$ . Then any number  $a$  is equal to some power of  $g$  modulo  $p$ , say  $a \equiv g^k \pmod{p}$ . Prove that  $a$  has a square root modulo  $p$  if and only if  $k$  is even.

*Solution to Exercise 1.34.*

- (a) If  $X = a_1$  and  $X = a_2$  are square roots of  $b$  modulo  $p$ , then  $p$  divides  $a_1^2 - b$  and  $p$  divides  $a_2^2 - b$ , so  $p$  divides their difference

$$(a_1^2 - b) - (a_2^2 - b) = a_1^2 - a_2^2 = (a_1 - a_2)(a_1 + a_2).$$

It follows that  $p$  divides either  $a_1 - a_2$  or  $a_1 + a_2$ . If the former, then  $a_1 \equiv a_2 \pmod{p}$ , and if the latter, then  $a_1 \equiv -a_2 \pmod{p}$ . Thus there are at most two possibilities.

Further, if there is one solution  $a$  and if  $p \geq 3$ , then  $p - a$  is a second solution different from  $a$ , so if there are any solutions, then there are exactly two solutions. On the other hand, if  $p = 2$ , then  $X^2 \equiv b \pmod{p}$  always has exactly one solution, namely  $X = b$ .

- (b) (i) 3 and 4.  
 (ii) 4 and 7.  
 (iii) None.  
 (iv) 15 and 22.
- (c) 8, 13, 22, and 27 are all solutions to  $X^2 \equiv 29 \pmod{35}$ , so 29 has four square roots modulo 35. This does not contradict (a), since the modulus 35 is not prime.
- (d) Suppose first that  $k$  is even, say  $k = 2j$ . Then

$$a \equiv g^k \equiv g^{2j} \equiv (g^j)^2 \pmod{p},$$

so  $a$  is a square modulo  $p$ .

Next suppose  $a$  is a square, say  $a \equiv b^2 \pmod{p}$ . Since  $g$  is a primitive root, we can write  $b \equiv g^i \pmod{p}$  for some exponent  $i$ . Then

$$g^k \equiv a \equiv b^2 \equiv (g^i)^2 \equiv g^{2i} \pmod{p}.$$

Thus  $g^{k-2i} \equiv 1 \pmod{p}$ , and the fact that  $g$  is a primitive root implies that  $p - 1$  divides  $k - 2i$ . But  $p - 1$  is even, hence 2 divides  $k - 2i$ , so 2 divides  $k$ .

**1.35.** Let  $p \geq 3$  be a prime and suppose that the congruence

$$X^2 \equiv b \pmod{p}$$

has a solution.

- (a) Prove that for every exponent  $e \geq 1$  the congruence

$$X^2 \equiv b \pmod{p^e} \quad (1.11)$$

has a solution. (*Hint.* Use induction on  $e$ . Build a solution modulo  $p^{e+1}$  by suitably modifying a solution modulo  $p^e$ .)

- (b) Let  $X = \alpha$  be a solution to  $X^2 \equiv b \pmod{p}$ . Prove that in (a), we can find a solution  $X = \beta$  to  $X^2 \equiv b \pmod{p^e}$  that also satisfies  $\beta \equiv \alpha \pmod{p}$ .  
 (c) Let  $\beta$  and  $\beta'$  be two solutions as in (b). Prove that  $\beta \equiv \beta' \pmod{p^e}$ .  
 (d) Use Exercise 1.34 to deduce that the congruence (1.14) has either two solutions or no solutions modulo  $p^e$ .

Solution to Exercise 1.35.

We do (a), (b), and (c) simultaneously. We are given that  $X = \alpha$  is a solution to  $X^2 \equiv b \pmod{p}$ . We are going to prove by induction that for every  $e \geq 1$  there is a unique value  $\beta \pmod{p^e}$  satisfying both

$$\beta^2 \equiv b \pmod{p^e} \quad \text{and} \quad \beta \equiv \alpha \pmod{p}.$$

The case  $e = 1$  is given to us, we must take  $\beta = \alpha$ . Now suppose that we have a value of  $\beta$  that works for  $e$ , and we ask for all solutions that work for  $e + 1$ . Note that if  $\gamma$  is a solution for  $e + 1$ , then  $\gamma \pmod{p^e}$  is a solution for  $e$ . So by the uniqueness part of the induction hypothesis, we would need to have  $\gamma \equiv \beta \pmod{p^e}$ . In other words, if there are any solutions  $\gamma$  for  $e + 1$ , then  $\gamma$  is forced to have the form

$$\gamma = \beta + yp^e \quad \text{for some integer } y.$$

What we want to do is show that there is a unique value of  $y$  modulo  $p$  that makes  $\gamma$  into a solution of  $X^2 \equiv b \pmod{p^{e+1}}$ .

We also want to use the fact that  $\beta$  is a solution to  $X^2 \equiv b \pmod{p^e}$ . This means that

$$\beta^2 = b + p^e B \quad \text{for some integer } B.$$

Now we substitute  $\gamma = \beta + yp^e$  into the congruence  $X^2 \equiv b \pmod{p^{e+1}}$  and try to solve for  $y$ . Thus

$$\begin{aligned} (\beta + yp^e)^2 &\equiv b \pmod{p^{e+1}} \\ \beta^2 + 2yp^e + y^2p^{2e} &\equiv b \pmod{p^{e+1}} \\ \beta^2 + 2yp^e &\equiv b \pmod{p^{e+1}} && \text{since } 2e \geq e + 1, \\ b + p^e B + 2yp^e &\equiv b \pmod{p^{e+1}} && \text{since } \beta^2 = b + p^e B, \\ p^e(B + 2y) &\equiv 0 \pmod{p^{e+1}}. \end{aligned}$$

Thus we need to solve

$$B + 2y \equiv 0 \pmod{p}.$$

This has a unique solution for  $y$ . (Note that  $p$  is assumed to be an odd prime. If  $p = 2$ , the argument does not work.) We can even solve explicitly,

$$y \equiv \frac{p-1}{2}B \pmod{p}.$$

This completes the proof that for every  $e \geq 1$  there exists a unique value of  $\beta \pmod{p^e}$  satisfying

$$\beta^2 \equiv b \pmod{p^e} \quad \text{and} \quad \beta \equiv \alpha \pmod{p},$$

which gives all of the statements in (a), (b), and (b).

(d) From the earlier exercise we know that  $X^2 \equiv b \pmod{p}$  has either 0 or 2 solutions. If it has no solutions, there certainly aren't any solutions to  $X^2 \equiv b \pmod{p^e}$  for  $e \geq 2$ , since any such solution could always be reduced modulo  $p$ . On the other hand, if  $X^2 \equiv b \pmod{p}$  has two solutions, then (a), (b), and (c) together imply that there are also two solutions to  $X^2 \equiv b \pmod{p^e}$  for each  $e \geq 1$ , since the solutions to  $X^2 \equiv b \pmod{p}$  are matched up one-to-one with the solutions to  $X^2 \equiv b \pmod{p^e}$ .

This exercise is a very special case of Hensel's lemma.

**1.36.** Compute the value of

$$2^{(p-1)/2} \pmod{p}$$

for every prime  $3 \leq p < 20$ . Make a conjecture as to the possible values of  $2^{(p-1)/2} \pmod{p}$  when  $p$  is prime and prove that your conjecture is correct.

Solution to Exercise 1.36.

$p = 3$	$2^1 = 2 \equiv 2$
$p = 5$	$2^2 = 4 \equiv 4$
$p = 7$	$2^3 = 8 \equiv 1$
$p = 11$	$2^5 = 32 \equiv 10$
$p = 13$	$2^6 = 64 \equiv 12$
$p = 17$	$2^8 = 256 \equiv 1$
$p = 19$	$2^9 = 512 \equiv 18$

**Conjecture:**  $2^{(p-1)/2}$  is congruent to either 1 or  $p-1$  modulo  $p$ .

**Proof:** Let  $a = 2^{(p-1)/2}$ . Then  $a^2 \equiv 2^{p-1} \equiv 1 \pmod{p}$  by Fermat's little theorem. Therefore  $a \equiv \pm 1 \pmod{p}$ . To see this last fact, note that  $p \mid (a^2 - 1)$ , so  $p \mid (a-1)(a+1)$ , so since  $p$  is prime, it divides one of  $a-1$  or  $a+1$ , which is just another way of saying that  $a \equiv \pm 1 \pmod{p}$ .

Section. Cryptography by hand

**1.37.** Write a 2 to 5 page paper on one of the following topics, including both cryptographic information and placing events in their historical context:

- (a) Cryptography in the Arab world to the 15th century.
- (b) European cryptography in the 15th and early 16th centuries.
- (c) Cryptography and cryptanalysis in Elizabethan England.
- (d) Cryptography and cryptanalysis in the 19th century.
- (e) Cryptography and cryptanalysis during World War I.
- (f) Cryptography and cryptanalysis during World War II.

(Most of these topics are too broad for a short term paper, so you should choose a particular aspect on which to concentrate.)

Solution to Exercise 1.37.

*A solution for this exercise will not be provided.*

**1.38.** A **homophonic cipher** is a substitution cipher in which there may be more than one ciphertext symbol for each plaintext letter. Here is an example of a homophonic cipher, where the more common letters have several possible replacements.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
!	4	#	\$	1	%	&	*	(	)	3	2	=	+	[	9	]	{	}	:	;	7	<	>	5	?
♡	○	*	ℵ	6	↗	▷	◇	∧		↘	△	▽	8	♣		Ω	√	⊗	♠						♠
Θ				∞		↑	‡						•	⊙				◁	⊕	⇐					♠
↙				↓														⇒	↖						

Decrypt the following message.

( % △ ♠ ⇒ ‡ # 4 ∞ : ◇ 6 ↗ ⊙ [ ℵ 8 % 2 [ 7 ↓ ♣ ↘ ♡ 5 ⊙ ▽

Solution to Exercise 1.38.

( % △ ♠ ⇒ ‡ # 4 ∞ : ◇ 6 ↗ ⊙ [ ℵ 8  
 I f m u s i c b e t h e f o o d o  
 % 2 [ 7 ↓ ♣ ↘ ♡ 5 ⊙ ▽  
 f l o v e p l a y o n

From Shakespeare's *Twelfth Night*: If music be the food of love, play on...

**1.39.** 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.<sup>1</sup> 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

<sup>1</sup>If the number of letters in the message is not an even multiple of 25, then extra random letters are appended to the end of the message.

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 to Exercise 1.39.*

- (a) Ciphertext: FCNER OODNS URSYA REEEG SAVAO

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

- (b) Plaintext: When in the course of human events it becomes necessary...

Hopefully everyone recognizes the first few words of the American Declaration of Independence.

W	H	E	N	I
N	T	H	E	C
O	U	R	S	E
O	F	H	U	M
A	N	E	V	E

(c) Plaintext: We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator...

Another excerpt from the Declaration of Independence. It was encrypted using a 15-by-4 rectangle.

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

#### Section. Symmetric ciphers and asymmetric ciphers

**1.40.** Encode the following phrase (including capitalization, spacing and punctuation) into a string of bits using the ASCII encoding scheme given in Table 1.10.

Bad day, Dad.

*Solution to Exercise 1.40.*

B	a	d	d	a	y	,
66	97	100	32	100	97	121
01000010	01100001	01100100	00100000	01100100	01100001	01111001
	D	a	d	.		
32	68	97	100	46		
00100000	01000100	01100001	01100100	00101110		

Thus the phrase “Bad day, Dad.” becomes the ASCII list of bits

```
0100001001100001011001000010000001100100011000010111
1001001011000010000001000100011000010110010000101110
```

**1.41.** Consider the affine cipher with key  $k = (k_1, k_2)$  whose encryption and decryption functions are given by (1.11) on page 43.

- Let  $p = 541$  and let the key be  $k = (34, 71)$ . Encrypt the message  $m = 204$ . Decrypt the ciphertext  $c = 431$ .
- Assuming that  $p$  is public knowledge, explain why the affine cipher is vulnerable to a chosen plaintext attack. (See Property 4 on page 38.) How many plaintext/ciphertext pairs are likely to be needed in order to recover the private key?
- Alice and Bob decide to use the prime  $p = 601$  for their affine cipher. The value of  $p$  is public knowledge, and Eve intercepts the ciphertexts  $c_1 = 324$  and  $c_2 = 381$  and also manages to find out that the corresponding plaintexts are  $m_1 = 387$  and  $m_2 = 491$ . Determine the private key and then use it to encrypt the message  $m_3 = 173$ .
- Suppose now that  $p$  is not public knowledge. Is the affine cipher still vulnerable to a chosen plaintext attack? If so, how many plaintext/ciphertext pairs are likely to be needed in order to recover the private key?

*Solution to Exercise 1.41.*

(a) The encryption of  $m = 204$  is  $c \equiv 34 \cdot 204 + 71 \equiv 7007 \equiv 515 \pmod{541}$ . The inverse of  $k_1$  is  $34^{-1} \equiv 366 \pmod{541}$ . The decryption of  $c = 431$  is  $m \equiv 366(431 - 71) \equiv 297 \pmod{541}$ .

(b) Given two plaintext/ciphertext pairs, one can solve the two linear congruences

$$c_1 \equiv k_1 \cdot m_1 + k_2 \pmod{p} \quad \text{and} \quad c_2 \equiv k_1 \cdot m_2 + k_2 \pmod{p}$$

for the two unknowns  $k_1$  and  $k_2$ .

(c) Eve knows that

$$324 \equiv k_1 \cdot 387 + k_2 \pmod{601} \quad \text{and} \quad 381 \equiv k_1 \cdot 491 + k_2 \pmod{601}$$

She subtracts the first equation from the second to get

$$57 \equiv k_1 \cdot 104 \pmod{601}.$$

She computes  $104^{-1} \equiv 549 \pmod{601}$ , and hence

$$k_1 \equiv 57 \cdot 104^{-1} \equiv 41 \pmod{601}.$$

Then she uses either of the above congruences to recover  $k_2$ ,

$$k_2 \equiv 324 - k_1 \cdot 387 \equiv 83 \pmod{601}.$$

Eve now knows Alice and Bob's private key, so she can encrypt a message,

$$c_3 \equiv k_1 \cdot m_3 + k_2 \equiv 41 \cdot 173 + 83 \equiv 565 \pmod{601}.$$

(d) Yes. Suppose that we have three plaintext/ciphertext pairs,

$$(m_1, c_1), (m_2, c_2), (m_3, c_3).$$

This gives us a system of three congruences

$$c_1 \equiv k_1 m_1 + k_2 \pmod{p}$$

$$c_2 \equiv k_1 m_2 + k_2 \pmod{p}$$

$$c_3 \equiv k_1 m_3 + k_2 \pmod{p}$$

We can write this in suggestive matrix and vector notation at

$$\begin{pmatrix} c_1 & m_1 & 1 \\ c_2 & m_2 & 1 \\ c_3 & m_3 & 1 \end{pmatrix} \begin{pmatrix} 1 & -k_1 & -k_2 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \pmod{p}.$$

Using linear algebra modulo  $p$ , this implies that the determinant of the matrix satisfies



$$\det \begin{pmatrix} c_1 & m_1 & 1 \\ c_2 & m_2 & 1 \\ c_3 & m_3 & 1 \end{pmatrix} \equiv 0 \pmod{p}.$$

Thus three plaintext/ciphertext pairs allows Eve to compute a number, namely

$$D = \det \begin{pmatrix} c_1 & m_1 & 1 \\ c_2 & m_2 & 1 \\ c_3 & m_3 & 1 \end{pmatrix}$$

that is divisible by the secret prime  $p$ . If Eve can factor  $D$ , then at worst she has a few possible values of  $p$  to check. So three pairs may be enough to break the cipher.

More generally, if Eve has  $n$  different pairs, she can compute determinant values  $D_1, \dots, D_{n-2}$  by using different pairs in the last row of the matrix (keeping the first two rows the same). This gives her a bunch of numbers that are divisible by  $p$ , and within a short time she will almost certain find that  $\gcd(D_1, \dots, D_{n-2})$  is equal to  $p$ .

**1.42.** Consider the Hill cipher defined by (1.11),

$$e_k(m) \equiv k_1 \cdot m + k_2 \pmod{p} \quad \text{and} \quad d_k(c) \equiv k_1^{-1} \cdot (c - k_2) \pmod{p},$$

where  $m$ ,  $c$ , and  $k_2$  are column vectors of dimension  $n$ , and  $k_1$  is an  $n$ -by- $n$  matrix.

- (a) We use the vector Hill cipher with  $p = 7$  and the key  $k_1 = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$  and  $k_2 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}$ .
  - (i) Encrypt the message  $m = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ .
  - (ii) What is the matrix  $k_1^{-1}$  used for decryption?
  - (iii) Decrypt the message  $c = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$ .
- (b) Explain why the Hill cipher is vulnerable to a chosen plaintext attack.
- (c) The following plaintext/ciphertext pairs were generated using a Hill cipher with the prime  $p = 11$ . Find the keys  $k_1$  and  $k_2$ .

$$m_1 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}, \quad c_1 = \begin{pmatrix} 1 \\ 8 \end{pmatrix}, \quad m_2 = \begin{pmatrix} 8 \\ 10 \end{pmatrix}, \quad c_2 = \begin{pmatrix} 8 \\ 5 \end{pmatrix}, \quad m_3 = \begin{pmatrix} 7 \\ 1 \end{pmatrix}, \quad c_3 = \begin{pmatrix} 8 \\ 7 \end{pmatrix}.$$

- (d) Explain how any simple substitution cipher that involves a permutation of the alphabet can be thought of as a special case of a Hill cipher.

Solution to Exercise 1.42.

- (a-i)  $e_k(m) = \begin{pmatrix} 5 \\ 3 \end{pmatrix}$ .
- (a-ii)  $k_1^{-1} = \begin{pmatrix} 3 & 6 \\ 4 & 5 \end{pmatrix}$ .
- (a-iii)  $d_k(c) = \begin{pmatrix} 0 \\ 4 \end{pmatrix}$ .
- (b) Each known plaintext/ciphertext pair gives a congruence of the form  $c \equiv k_1 \cdot m + k_2 \pmod{p}$ . Writing this out gives  $n$  linear equations for the  $n^2 + n$  unknown entries of  $k_1$  and  $k_2$ . Hence  $n+1$  plaintext/ciphertext pairs probably gives enough equations to solve for the keys  $k_1$  and  $k_2$ .

(c) We let  $k_1 = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$  and  $k_2 = \begin{pmatrix} u \\ v \end{pmatrix}$ . Then the congruence  $c_1 = k_1 m_1 + k_2 \pmod{11}$  becomes the matrix equation

$$\begin{pmatrix} 1 \\ 8 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 5 \\ 4 \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 5x + 4y + u \\ 5z + 4w + v \end{pmatrix} \pmod{11}.$$

So this gives the two congruences

$$5x + 4y + u \equiv 1 \pmod{11} \quad \text{and} \quad 5z + 4w + v \equiv 8 \pmod{11}.$$

Similarly, the congruence  $c_2 = k_1 m_2 + k_2 \pmod{11}$  gives

$$8x + 10y + u \equiv 8 \pmod{11} \quad \text{and} \quad 8z + 10w + v \equiv 5 \pmod{11}.$$

and  $c_3 = k_1 m_3 + k_2 \pmod{11}$  gives

$$7x + y + u \equiv 8 \pmod{11} \quad \text{and} \quad 7z + w + v \equiv 7 \pmod{11}.$$

This gives us 6 equations for the 6 unknowns  $x, y, z, w, u, v$ . Further, three of the equations only involve  $x, y, u$  and the other three only involve  $z, w, v$ , so it's really two sets of 3-by-3 equations to solve:

$$\begin{array}{ll} 5x + 4y + u = 1 & 5z + 4w + v = 8 \\ 8x + 10y + u = 8 & 8z + 10w + v = 5 \\ 7x + y + u = 8 & 7z + w + v = 7. \end{array}$$

(All equations are modulo 11.) These are easily solved using basic linear algebra methods, and we find that

$$(x, y, u) = (3, 7, 2) \quad \text{and} \quad (z, w, v) = (4, 3, 9).$$

Hence

$$k_1 = \begin{pmatrix} 3 & 7 \\ 4 & 3 \end{pmatrix} \quad \text{and} \quad k_2 = \begin{pmatrix} 2 \\ 9 \end{pmatrix}.$$

(d) We work with vectors of dimension 26. Let  $\mathbf{e}_1, \dots, \mathbf{e}_{26}$  be the usual basis vectors for  $\mathbb{R}^{26}$ , i.e.,  $\mathbf{e}_i$  has a 1 in the  $i^{\text{th}}$  place and 0's elsewhere. For the plaintext, we use  $\mathbf{e}_1$  to represent (a), we use  $\mathbf{e}_2$  to represent (b), and so on. We view the simple substitution cipher as a function that takes each plaintext letter and assigns it to a ciphertext letter. Equivalently, it takes each  $\mathbf{e}_i$  and assigns it to some  $\mathbf{e}_{\pi(i)}$ , where  $\pi$  is a one-to-one function

$$\pi : \{1, 2, \dots, 26\} \longrightarrow \{1, 2, \dots, 26\}.$$

In the Hill cipher, we now take  $k_1$  to be the matrix whose  $ij^{\text{th}}$  entry is 1 if  $e(i) = j$ , and otherwise it is 0. We also take  $k_2 = 0$ . Then  $k_1 \cdot \mathbf{e}_i = \mathbf{e}_{\pi(i)}$ , so the encryption of the plaintext  $\mathbf{e}_i$  is equal to  $\mathbf{e}_{\pi(i)}$ , as desired.

**1.43.** Let  $N$  be a large integer and let  $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{Z}/N\mathbb{Z}$ . For each of the functions

$$e : \mathcal{K} \times \mathcal{M} \longrightarrow \mathcal{C}$$

listed in (a), (b), and (c), answer the following questions:

- Is  $e$  an encryption function?
- If  $e$  is an encryption function, what is its associated decryption function  $d$ ?
- If  $e$  is not an encryption function, can you make it into an encryption function by using some smaller, yet reasonably large, set of keys?

(a)  $e_k(m) \equiv k - m \pmod{N}$ .

(b)  $e_k(m) \equiv k \cdot m \pmod{N}$ .

(c)  $e_k(m) \equiv (k + m)^2 \pmod{N}$ .

Solution to Exercise 1.43.

(a) Yes,  $e$  is an encryption function. The decryption function  $d_k(c) = k - c$  is the same as  $e$ !

(b) No,  $e$  is not an encryption function, it is not one-to-one. However, if we restrict the keys to  $\mathcal{K} = (\mathbb{Z}/N\mathbb{Z})^*$  (i.e.,  $\gcd(k, N) = 1$ ), then  $e$  is an encryption function, with decryption function  $d_k(c) \equiv k^{-1}c \pmod{N}$ .

(c) No,  $e$  is not an encryption function, it is not one-to-one, and no subset of keys will make it one-to-one. However, one might define a decryption “function” by  $d_k(c) \equiv \sqrt{c} - k \pmod{N}$ . Assuming that one knows how to compute square roots modulo  $N$ , this gives two possible decryptions, since it’s really  $\pm\sqrt{c}$ . In practice, one might be able to use some property of valid messages to figure out which one is correct.

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

(b) Convert the decimal integer  $m = 37853$  into a binary number.

(c) Convert the decimal integer  $m = 9487428$  into a binary number.

(d) Use exclusive or (XOR) to “add” the bit strings  $11001010 \oplus 10011010$ .

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

Solution to Exercise 1.44.

(a)  $2^{11} + 2^{10} + 2^8 + 2^6 + 2^5 + 2^2 + 2^0 = \boxed{3429}$

(b)  $37853 = 2^{15} + 2^{12} + 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + 2^3 + 2^2 + 2^0$ , so the binary form of 37853 is  $\boxed{1001001111011101}$ .

(c)  $9487428 = 2^{23} + 2^{20} + 2^{15} + 2^{14} + 2^{10} + 2^6 + 2^2$ , so the binary form of 9487428 is  $\boxed{100100001100010001000100}$ .

(d)  $11001010 \oplus 10011010 = \boxed{01010000}$ .

(e)

$$\begin{aligned}
8734 &= '10001000011110', \\
5177 &= '01010000111001', \\
8734 \oplus 5177 &= 10001000011110 \oplus 01010000111001 = 11011000100111, \\
'11011000100111' &= \boxed{13863}.
\end{aligned}$$

**1.45.** Alice and Bob choose a key space  $\mathcal{K}$  containing  $2^{56}$  keys. Eve builds a special-purpose computer that can check 10,000,000,000 keys per second.

- (a) How many days does it take Eve to check half of the keys in  $\mathcal{K}$ ?
- (b) Alice and Bob replace their key space with a larger set containing  $2^B$  different keys. How large should Alice and Bob choose  $B$  in order to force Eve's computer to spend 100 years checking half the keys? (Use the approximation that there are 365.25 days in a year.)

For many years the United States government recommended a symmetric cipher called DES that used 56 bit keys. During the 1990s, people built special purpose computers demonstrating that 56 bits provided insufficient security. A new symmetric cipher called AES, with 128 bit keys, was developed to replace DES. See Section 8.10 for further information about DES and AES.

*Solution to Exercise 1.45.*

(a)

$$\begin{aligned}
(2^{56} \text{ keys}) \cdot \left( \frac{1 \text{ second}}{10,000,000,000 \text{ keys}} \right) \cdot \left( \frac{1 \text{ minute}}{60 \text{ seconds}} \right) \\
\cdot \left( \frac{1 \text{ hour}}{60 \text{ minutes}} \right) \cdot \left( \frac{1 \text{ day}}{24 \text{ hours}} \right) \approx 83.4 \text{ days}.
\end{aligned}$$

It thus takes about 83.4 days to check all the keys, so about  $\boxed{41.7 \text{ days}}$  to check half the keys.

(b)

$$\begin{aligned}
&\left( \frac{10,000,000,000 \text{ keys}}{1 \text{ second}} \right) \cdot \left( \frac{60 \text{ seconds}}{1 \text{ minute}} \right) \cdot \left( \frac{60 \text{ minutes}}{1 \text{ hour}} \right) \\
&\cdot \left( \frac{24 \text{ hours}}{1 \text{ day}} \right) \cdot \left( \frac{365.25 \text{ days}}{1 \text{ year}} \right) \cdot (100 \text{ years}) \\
&= 315576000000000000 \text{ keys} \approx 2^{64.775} \text{ keys}.
\end{aligned}$$

Thus it takes Eve's computer 100 years to check  $2^{64.775}$  keys. The problem says that this should be half the keys, so Alice and Bob should have at least  $2^{65.775}$  different keys. In practice, it is easiest to choose an integral power of 2, so Alice and Bob's key space should contain (at least)  $2^{66}$  keys.

Comparing (a) and (b), notice that by increasing the keylength from 56 bits to 66 bits, Alice and Bob's security goes from 42 days to 100 years. Thus even a

small increase in the keylength results in an enormous increase in the breaking time by exhaustive search. This reflects the fact that exponential functions grow extremely rapidly.

**1.46.** Explain why the cipher

$$e_k(m) = k \oplus m \quad \text{and} \quad d_k(c) = k \oplus c$$

defined by XOR of bit strings is not secure against a chosen plaintext attack. Demonstrate your attack by finding the private key used to encrypt the 16-bit ciphertext  $c = 1001010001010111$  if you know that the corresponding plaintext is  $m = 0010010000101100$ .

*Solution to Exercise 1.46.*

If you know  $m$  and  $c$ , since they are related by  $c = k \oplus m$ , it follows that  $c \oplus m = k \oplus m \oplus m = k$ . For the example,

$$k = c \oplus m = 1001010001010111 \oplus 0010010000101100 = \boxed{1011000001111011}.$$

**1.47.** Alice and Bob create a symmetric cipher as follows. Their private key  $k$  is a large integer and their messages (plaintexts) are  $d$ -digit integers

$$\mathcal{M} = \{m \in \mathbb{Z} : 0 \leq m < 10^d\}.$$

To encrypt a message, Alice computes  $\sqrt{k}$  to  $d$  decimal places, throws away the part to the left of the decimal point, and keeps the remaining  $d$  digits. Let  $\alpha$  be this  $d$ -digit number. (For example, if  $k = 23$  and  $d = 6$ , then  $\sqrt{87} = 9.32737905\dots$  and  $\alpha = 327379$ .)

Alice encrypts a message  $m$  as

$$c \equiv m + \alpha \pmod{10^d}.$$

Since Bob knows  $k$ , he can also find  $\alpha$ , and then he decrypts  $c$  by computing  $m \equiv c - \alpha \pmod{10^d}$ .

- (a) Alice and Bob choose the secret key  $k = 11$  and use it to encrypt 6-digit integers (i.e.,  $d = 6$ ). Bob wants to send Alice the message  $m = 328973$ . What is the ciphertext that he sends?
- (b) Alice and Bob use the secret key  $k = 23$  and use it to encrypt 8-digit integers. Alice receives the ciphertext  $c = 78183903$ . What is the plaintext  $m$ ?
- (c) Show that the number  $\alpha$  used for encryption and decryption is given by the formula

$$\alpha = \left\lfloor 10^d \left( \sqrt{k} - \lfloor \sqrt{k} \rfloor \right) \right\rfloor,$$

where  $\lfloor t \rfloor$  denotes the greatest integer that is less than or equal to  $t$ .

- (d) (Challenge Problem) If Eve steals a plaintext/ciphertext pair  $(m, c)$ , then it is clear that she can recover the number  $\alpha$ , since  $\alpha \equiv c - m \pmod{10^d}$ . If  $10^d$  is large compared to  $k$ , can she also recover the number  $k$ ? This might be useful, for example, if Alice and Bob use some of the other digits of  $\sqrt{k}$  to encrypt subsequent messages.

Solution to Exercise 1.47.

(a)  $\sqrt{11} = 3.3166247903\dots$ , so  $\alpha = 316624$  and the ciphertext is  $c = 328973 + 316624 = \boxed{645597}$ .

(b)  $\sqrt{23} = 4.7958315233127195\dots$ , so  $\alpha = 79583152$  and the plaintext is

$$c = 78183903 - 79583152 = -1399249 \equiv \boxed{98600751} \pmod{10^8}.$$

(c) The quantity  $x - \lfloor x \rfloor$  gives the fractional part of  $x$ , i.e., the part to the right of the decimal point. The remaining part of the formula simply shifts the digits  $d$  places to the left and then discards everything after the decimal point.

(d) The answer is yes, Eve should be able to recover  $k$ , but probably not using the tools that we've developed so far. Let  $\beta = \alpha/10^d$ . Then

$$\sqrt{k} = L + \beta \quad \text{for some } L \in \mathbb{Z}.$$

There are two unknowns here,  $k$  and  $L$ , and all that Eve knows is that they are both integers. Squaring both sides gives

$$k = L^2 + 2L\beta + \beta^2.$$

Thus there are integers  $A$  and  $B$  satisfying

$$\beta^2 + A\beta + B = 0,$$

namely  $A = 2L$  and  $B = L^2 - k$ . Of course, Eve doesn't know  $A$  or  $B$ , either. However, there are algorithms based on lattice reduction that are very good at finding the smallest (quadratic) polynomial with integer coefficients satisfied by a given decimal number. Using these algorithms, Eve should be able to find  $A$  and  $B$ , from which it is easy to recover  $k$  as  $k = \frac{1}{4}A^2 - B$ .

**1.48.** Bob and Alice use a cryptosystem in which their private key is a (large) prime  $k$  and their plaintexts and ciphertexts are integers. Bob encrypts a message  $m$  by computing the product  $c = km$ . Eve intercepts the following two ciphertexts:

$$c_1 = 12849217045006222, \quad c_2 = 6485880443666222.$$

Use the gcd method described in Section 1.7.4 to find Bob and Alice's private key.

Solution to Exercise 1.48.

We compute

$$\gcd(c_1, c_2) = 174385766.$$

This factors as  $174385766 = 2 \cdot 87192883$  and  $87192883$  is prime, so it is Bob and Alice's key.



## Chapter 2

# Discrete Logarithms and Diffie–Hellman

### Exercises for Chapter 2

Section. Diffie–Hellman and RSA

**2.1.** Write a one page essay giving arguments, both pro and con, for the following assertion:

If the government is able to convince a court that there is a valid reason for their request, then they should have access to an individual’s private keys (even without the individual’s knowledge), in the same way that the government is allowed to conduct court authorized secret wiretaps in cases of suspected criminal activity or threats to national security.

Based on your arguments, would you support or oppose the government being given this power? How about without court oversight? The idea that all private keys should be stored at a secure central location and be accessible to government agencies (with or without suitably stringent legal conditions) is called *key escrow*.

Solution to Exercise 2.1.

*A solution for this exercise will not be provided.*

**2.2.** Research and write a one to two page essay on the classification of cryptographic algorithms as munitions under ITAR (International Traffic in Arms Regulations). How does that act define “export”? What are the potential fines and jail terms for those convicted of violating the Arms Export Control Act? Would teaching non-classified cryptographic algorithms to a college class that includes non-US citizens be considered a form of export? How has US government policy changed from the early 1990s to the present?



Solution to Exercise 2.2.

Some historical material:

Press Release

Law Professor Sues Federal Government Over Computer Privacy Issues

Federal Civil Rights Action Seeks Injunction Against State Department  
And National Security Agency

Cleveland Scholar Attacks Prohibition On Discussing Cryptographic Software  
With Foreign Students And Colleagues

For Immediate Release

Cleveland, Wednesday, August 7, 1996

A Case Western Reserve University law professor filed suit today in federal court, challenging government regulations which restrict his ability to teach a course in computer law. Peter Junger, a twenty-five year veteran of the law school faculty, will file a federal civil rights action this afternoon in the United States District Court in Cleveland. The suit names the Department of State and the secretive National Security Agency, which administer federal regulations limiting Professor Junger's ability to teach.

The case involves the International Traffic in Arms Regulations, or ITAR, federal regulations which restrict the export of military technology. Under the ITAR, cryptographic computer software, which encodes text to preserve the privacy of messages on the Internet, is considered a "munition" and subject to strict export control. The regulations raise significant First Amendment questions by defining "export" to include discussing technical information about non-classified software with foreign nationals, such as students registered for Professor Junger's course.

In recent months, the State Department has sent a series of letters threatening possible criminal action to a Florida man who posted a simple cryptographic algorithm to the "sci.crypt" Usenet Newsgroup, an Internet site popular with cryptography enthusiasts. These and similar incidents have caused Professor Junger to limit his discussions of cryptographic material with foreign colleagues, for fear of violating the ITAR. Penalties for unlicensed disclosure of cryptographic information are severe: federal law provides ten year prison terms and One Million Dollar fines for those convicted of violating the Arms Export Control Act, the legislation under which the ITAR was promulgated.

---

Statement by Ambassador David Aaron

US Envoy for Cryptography

RSA Data Security Conference, January 28, 1997

International Views of Key Recovery

These concerns are being heard in Washington. The Administration has taken the following steps - many based on the direct recommendations of industry representatives:

First, at the end of last year, jurisdiction for licenses of encryption exports was transferred from the Department of State to the Department of Commerce. Commercial encryption is no longer treated as a munition and thereby

subject to various foreign policy embargoes. We hope this will both speed up and simplify the tasks of obtaining licenses.

Second, and very important, the Administration will license the export of encryption products, of any algorithm and any key length, if they incorporate key recovery.

Third, the Administration will also permit the export, over the next two years, of 56-bit DES and equivalent encryption products without key recovery provided exporters make commitments to develop key recovery products. I am pleased to report that already at least 4 vendors have formally filed key recovery commitments and several more companies are in the initial stages of dialogue with the Department of Commerce.

And last, a point which is often lost in the debate, domestic use of key recovery will be voluntary as announced by the Vice President last October. All Americans will remain free to use any encryption system in the United States.

In 1992, the Software Publishers Association and the State Department reached an agreement which allows the export of programs containing RSA Data Security's RC2 and RC4 algorithms, but only when the key size is set to 40 bits or less. 40 bits is not very secure, and application of a distributed attack using standard workstations in a good-size lab can break these in at most a few days. This theory was demonstrated quite visibly in mid-1995 when two independent groups broke 40-bit keys used in the export version of the Netscape browser.

Section. The discrete logarithm problem

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

- (a) Suppose that  $x = a$  and  $x = b$  are both integer solutions to the congruence  $g^x \equiv h \pmod{p}$ . Prove that  $a \equiv b \pmod{p-1}$ . Explain why this implies that the map (2.1) on page 63 is well-defined.
- (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 to Exercise 2.3.*

(a) We are given that  $g^a \equiv g^b \pmod{p}$ , since they are both congruent to  $h$ . Hence  $g^{a-b} \equiv 1 \pmod{p}$ . But  $g$  is a primitive root, so its order is  $p-1$ , which implies that  $p-1$  divides  $a-b$ . Hence  $a \equiv b \pmod{p-1}$ . This means the  $\log_g(h)$  is well-defined up to adding or subtracting multiples of  $p-1$ , so the map (2.1) on page 63 is well-defined.

(b) We have

$$\begin{aligned} g^{\log_g(h_1) + \log_g(h_2)} &= g^{\log_g(h_1)} \cdot g^{\log_g(h_2)} \\ &\equiv h_1 \cdot h_2 \pmod{p} \\ &\equiv g^{\log_g(h_1 h_2)} \pmod{p}. \end{aligned}$$

Hence  $\log_g(h_1) + \log_g(h_2) = \log_g(h_1 h_2)$ , or more precisely, they are congruent modulo  $p - 1$ .

(c) We have

$$g^{n \log_g(h)} = \left(g^{\log_g(h)}\right)^n \equiv h^n \equiv g^{\log_g(h^n)} \pmod{p}.$$

Hence  $n \log_g(h) \equiv \log_g(h^n) \pmod{p-1}$ .

**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 64.)

*Solution to Exercise 2.4.*

- (a)  $\log_2(13) = 7$  in  $\mathbb{F}_{23}$ , since  $2^{13} = 128 \equiv 13 \pmod{23}$ .
- (b)  $\log_{10}(22) = 11$  in  $\mathbb{F}_{47}$ .
- (c) The table shows that  $627^{18} \equiv 608 \pmod{941}$ , so  $\log_{627}(608) = 18$  in  $\mathbb{F}_{941}$ .

**2.5.** Let  $p$  be an odd prime and let  $g$  be a primitive root modulo  $p$ . Prove that  $a$  has a square root modulo  $p$  if and only if its discrete logarithm  $\log_g(a)$  modulo  $p$  is even.

*Solution to Exercise 2.5.*

This solution is taken from the proof of Proposition 3.60.

Let  $m = \log_g(a)$ , so  $a = g^m$ . If  $m = 2k$  is even, then  $g^m = g^{2k} = (g^k)^2$  is a square.

On the other hand, let  $m$  be odd, say  $m = 2k + 1$ , and suppose that  $g^m$  is a square modulo  $p$ , say  $g^m \equiv c^2 \pmod{p}$ . Fermat's little theorem (Theorem 1.25) tells us that

$$c^{p-1} \equiv 1 \pmod{p}.$$

However,  $c^{p-1} \pmod{p}$  is also equal to

$$c^{p-1} \equiv (c^2)^{\frac{p-1}{2}} \equiv (g^m)^{\frac{p-1}{2}} \equiv (g^{2k+1})^{\frac{p-1}{2}} \equiv g^{k(p-1)} \cdot g^{\frac{p-1}{2}} \pmod{p}.$$

Another application of Fermat's little theorem tells us that

$$g^{k(p-1)} \equiv (g^{p-1})^k \equiv 1^k \equiv 1 \pmod{p},$$

so we find that

$$g^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

This contradicts the fact that  $g$  is a primitive root, which proves that every odd power of  $g$  is not a square modulo  $p$ .

Section. Diffie–Hellman key exchange

**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 your assistance, so you tell him to use the secret exponent  $b = 871$ . What value  $B$  should Bob send to Alice, and what is their secret shared value? Can you figure out Alice’s secret exponent?

*Solution to Exercise 2.6.*

Bob sends  $B = g^b = 2^{871} \equiv 805 \pmod{1373}$  to Alice. Their shared value is  $A^b = 974^{871} \equiv 397 \pmod{1373}$ . There is no really easy way to determine Alice’s secret exponent, but with a computer or even a programmable calculator, it does not take long to compute all of the powers of 2 modulo 1373. (Using the babystep–giantstep method is even faster, you only need to make two lists of length approximately  $\sqrt{1373} = 37.04\dots$ . If you do this, you will find that  $2^{587} \equiv 974 \pmod{1373}$ , so Alice’s secret exponent is 587.

**2.7.** Let  $p$  be a prime and let  $g$  be an integer. The *Diffie–Hellman Decision 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 67. 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 Diffie–Hellman decision problem.
- (b) Do you think that the Diffie–Hellman decision problem is hard or easy? Why?

See Exercise 5.35 for a related example in which the decision problem is easy, but it is believed that the associated computational problem is hard.

*Solution to Exercise 2.7.*

(a) This is obvious. If you can compute  $g^{ab}$  from  $g$ ,  $g^a$ , and  $g^b$ , then you can simply compare the value of  $g^{ab}$  with the value of  $C$  and check if they are equal.

(b) No one currently knows how to solve the Diffie–Hellman decision problem without solving the Diffie–Hellman computational problem.

Section. The ElGamal public key cryptosystem

**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 ephemeral key  $k = 877$ . 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 to Exercise 2.8.

- (a)  $A \equiv 2^{947} \equiv 177 \pmod{1373}$ , so Alice's public key is  $A = 177$ .
- (b)  $c_1 \equiv 2^{877} \equiv 719 \pmod{1373}$  and  $c_2 \equiv 583 \cdot 469^{877} \equiv 623 \pmod{1373}$ . Alice sends the ciphertext  $(c_1, c_2) = (719, 623)$  to Bob.
- (c)  $(c_1^a)^{-1} \cdot c_2 \equiv (661^{299})^{-1} \cdot 1325 \equiv 645^{-1} \cdot 1325 \equiv 794 \cdot 1325 \equiv 332 \pmod{1373}$ . Thus the plaintext is  $m = 332$ . It turns out that the ephemeral key is  $k = 566$ , but Alice does not know this value.
- (d) The solution to  $2^b \equiv 893 \pmod{1373}$  is  $b = 219$ , which is Bob's private key. It is now easy to decrypt,

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

Thus Alice's message to Bob is  $m = 365$ . (The ephemeral key was  $k = 932$ .)

**2.9.** Suppose that an oracle offers to solve the Diffie–Hellman problem for you. (See page 67 for a description of the Diffie–Hellman problem.) Explain how you can use the oracle to decrypt messages that have been encrypted using the ElGamal public key cryptosystem.

Solution to Exercise 2.9.

In the ElGamal PKC, you know Alice's public key  $A \equiv g^a \pmod{p}$  and you know the ciphertext consisting of the two quantities  $c_1 \equiv g^k \pmod{p}$  and  $c_2 \equiv m \cdot A^k \pmod{p}$ , where  $k$  is Bob's secret ephemeral key. You thus know the values of  $g^a$  and  $g^k$ , so the Diffie–Hellman problem oracle will take those values and tell you the value of  $g^{ak} \pmod{p}$ . But  $g^{ak} \equiv A^k \pmod{p}$ , so you can recover Bob's plaintext message by computing  $(g^{ak})^{-1} \cdot c_2 \equiv m \pmod{p}$ .

**2.10.** The exercise describes a public key cryptosystem that requires Bob and Alice to exchange several messages. We illustrate the system with an example.

Bob and Alice fix a publicly known prime  $p = 32611$ , and all of the other numbers used are private. Alice takes her message  $m = 11111$ , chooses a random exponent  $a = 3589$ , and sends the number  $u = m^a \pmod{p} = 15950$  to Bob. Bob chooses a random exponent  $b = 4037$  and sends  $v = u^b \pmod{p} = 15422$  back to Alice. Alice then computes  $w = v^{15619} \equiv 27257 \pmod{32611}$  and

sends  $w = 27257$  to Bob. Finally, Bob computes  $w^{31883} \pmod{32611}$  and recovers the value 11111 of Alice's message.

- Explain why this algorithm works. In particular, Alice uses the numbers  $a = 3589$  and  $15619$  as exponents. How are they related? Similarly, how are Bob's exponents  $b = 4037$  and  $31883$  related?
- Formulate a general version of this cryptosystem, i.e., using variables, and show that it works in general.
- What is the disadvantage of this cryptosystem over ElGamal? (*Hint.* How many times must Alice and Bob exchange data?)
- Are there any advantages of this cryptosystem over ElGamal? In particular, can Eve break it if she can solve the discrete logarithm problem? Can Eve break it if she can solve the Diffie–Hellman problem?

*Solution to Exercise 2.10.*

- Alice's and Bob's exponents satisfy

$$3589 \cdot 15619 \equiv 1 \pmod{32610} \quad \text{and} \quad 4037 \cdot 31883 \equiv 1 \pmod{32610}$$

The reason why the algorithm works is discussed in the answer to (b).

- In the general formulation, a public prime  $p$  is fixed. Alice chooses a plaintext  $m \pmod{p}$  and a random exponent  $a$  satisfying  $\gcd(a, p-1) = 1$ . She sends

$$u \equiv m^a \pmod{p}$$

to Bob. Bob chooses a random exponent  $b$  satisfying  $\gcd(b, p-1) = 1$ , computes

$$v \equiv u^b \pmod{p},$$

and sends  $v$  to Alice. Alice now computes the inverse of  $a$  modulo  $p-1$ , i.e., she solves  $ax \equiv 1 \pmod{p-1}$  for  $x$ . Let  $a' = a^{-1} \pmod{p-1}$ . Alice computes

$$w \equiv v^{a'} \pmod{p}$$

and sends it to Bob. Finally, Bob computes the inverse  $b' = b^{-1} \pmod{p-1}$  and then  $w^{b'} \pmod{p}$  is equal to  $m$ .

To see that this last assertion is true, we compute

$$w^{b'} \equiv v^{a'b'} \equiv u^{ba'b'} \equiv m^{aba'b'} \pmod{p}.$$

We know that

$$aa' \equiv 1 \pmod{1} \pmod{p-1} \quad \text{and} \quad bb' \equiv 1 \pmod{1} \pmod{p-1},$$

so the exponent  $aba'b'$  is congruent to 1 modulo  $p-1$ . Then Fermat's little theorem tells us that  $m^{aba'b'} \equiv m \pmod{p}$ .

- ElGamal only requires Alice to send Bob a single message. This new cryptosystem requires Alice to send Bob two messages and for Bob to send a

message back to Alice. So this new system is much more interactive and requires a lot more communication than does ElGamal.

(d) The advantage of this new system is that Alice and Bob reveal somewhat less information than in ElGamal. Of course, if Eve can solve the DLP, then since she knows  $u$ ,  $v$  and  $w$ , she can solve

$$w \equiv v^x \pmod{p}$$

to recover  $x = a'$ , and then she can recover  $m$ , because

$$u^{a'} \equiv m^{aa'} \equiv m \pmod{p}.$$

However, there does not appear to be an easy way for Eve to break the system if she knows how to solve the Diffie–Hellman Problem. Thus this new cryptosystem is potentially more secure than ElGamal, if it turns out that the DHP is easier to solve than the DLP.

**Section. An overview of the theory of groups**

**2.11.** The group  $\mathcal{S}_3$  consists of the following six distinct elements

$$e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau,$$

where  $e$  is the identity element and multiplication is performed using the rules

$$\sigma^3 = e, \quad \tau^2 = 1, \quad \tau\sigma = \sigma^2\tau.$$

Compute the following values in the group  $\mathcal{S}_3$ :

- (a)  $\tau\sigma^2$       (b)  $\tau(\sigma\tau)$       (c)  $(\sigma\tau)(\sigma\tau)$       (d)  $(\sigma\tau)(\sigma^2\tau)$ .

Is  $\mathcal{S}_3$  a commutative group?

*Solution to Exercise 2.11.*

$$(a) \tau\sigma^2 = (\tau\sigma)\sigma = (\sigma^2\tau)\sigma = \sigma^2(\tau\sigma) = \sigma^2(\sigma^2\tau) = \sigma^4\tau = (\sigma^3)\sigma\tau = \sigma\tau.$$

$$(b) \tau(\sigma\tau) = (\tau\sigma)\tau = (\sigma^2\tau)\tau = \sigma^2\tau^2 = \sigma^2.$$

$$(c) (\sigma\tau)(\sigma\tau) = \sigma(\tau\sigma)\tau = \sigma(\sigma^2\tau)\tau = \sigma^3\tau^2 = e.$$

$$(d) (\sigma\tau)(\sigma^2\tau) = \sigma(\tau\sigma)\sigma\tau = \sigma(\sigma^2\tau)\sigma\tau = \sigma^3(\tau\sigma)\tau = e(\sigma^2\tau)\tau = \sigma^2\tau^2 = \sigma^2.$$

No,  $\mathcal{S}_3$  is not a commutative group. For example  $\tau\sigma = \sigma^2\tau$ , which is different from  $\sigma\tau$ .

**2.12.** Let  $G$  be a group, let  $d \geq 1$  be an integer, and define a subset of  $G$  by

$$G[d] = \{g \in G : g^d = e\}.$$

- (a) Prove that if  $g$  is in  $G[d]$ , then  $g^{-1}$  is in  $G[d]$ .  
 (b) Suppose that  $G$  is commutative. Prove that if  $g_1$  and  $g_2$  are in  $G[d]$ , then their product  $g_1 \star g_2$  is in  $G[d]$ .  
 (c) Deduce that if  $G$  is commutative, then  $G[d]$  is a group.  
 (d) Show by an example that if  $G$  is not a commutative group, then  $G[d]$  need not be a group. (*Hint.* Use Exercise 2.11.)

Solution to Exercise 2.12.

(a) For any element  $h$  of  $G$  and any positive integer  $n$ , we have

$$(h^{-1})^n \star h^n = (h^{-1} \star h^{-1} \star \cdots \star h^{-1}) \star (h \star h \star \cdots \star h) = e,$$

since there are  $n$  copies of  $h^{-1}$  to cancel the  $n$  copies of  $h$ . Thus  $(h^{-1})^n$  is the inverse of  $h^n$ , which we can write succinctly as  $(h^{-1})^n = (h^n)^{-1}$ . We apply this with  $h = g$  and  $n = d$  and use the assumption that  $g^d = e$  to conclude that

$$(g^{-1})^d = (g^d)^{-1} = e^{-1} = e.$$

Hence  $g^{-1}$  is in  $G[d]$ .

(b) We are given that  $g_1^d = e$  and  $g_2^d = e$ . We use the commutativity to compute

$$(g_1 g_2)^d = g_1 g_2 g_1 g_2 \cdots g_1 g_2 = g_1^d g_2^d = ee = e.$$

Therefore  $g_1 g_2 \in G[d]$ .

(c) From (a) and (b), if we start with two elements in  $G[d]$ , their product and their inverses are in  $G[d]$ . Also clearly  $e$  is in  $G[d]$ . This gives the first two axioms, and the third (associativity) is automatic, since it's true for all elements in  $G$ .

(d) Using the group  $\mathcal{S}_3$  in Exercise 2.11, we have  $\tau^2 = e$  and  $(\sigma\tau)^2 = e$ . (The first is true from the description of the group, and the second is true from part (c) of the exercise.) However,  $(\sigma\tau)\tau = \sigma\tau^2 = \sigma$  does not satisfy  $\sigma^2 = e$ . To see why, note that  $\sigma^3 = e$ , so if also  $\sigma^2 = e$ , then we would have  $e = \sigma^3 = (\sigma^2)\sigma = e\sigma = \sigma$ , which is not true.

An alternative solution is to use the group of 2-by-2 matrices with integer coefficients. The matrix  $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  satisfies  $A^2 = I$  and the matrix  $B = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$  satisfies  $B^2 = I$ , but  $AB = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$  actually has order 3, i.e.,  $(AB)^3 = I$ .

**2.13.** Let  $G$  and  $H$  be groups. A function  $\phi : G \rightarrow H$  is called a (group) *homomorphism* if it satisfies

$$\phi(g_1 \star g_2) = \phi(g_1) \star \phi(g_2) \quad \text{for all } g_1, g_2 \in G.$$

(Note that the product  $g_1 \star g_2$  uses the group law in the group  $G$ , while the product  $\phi(g_1) \star \phi(g_2)$  uses the group law in the group  $H$ .)

(a) Let  $e_G$  be the identity element of  $G$ , let  $e_H$  be the identity element of  $H$ , and let  $g \in G$ . Prove that

$$\phi(e_G) = e_H \quad \text{and} \quad \phi(g^{-1}) = \phi(g)^{-1}.$$

(b) Let  $G$  be a commutative group. Prove that the map  $\phi : G \rightarrow G$  defined by  $\phi(g) = g^2$  is a homomorphism. Give an example of a noncommutative group for which this map is not a homomorphism.

(c) Same question as (b) for the map  $\phi(g) = g^{-1}$ .

Solution to Exercise 2.13.

A solution for this exercise is not currently available.



**2.14.** Prove that each of the following maps is a group homomorphism.

- (a) The map  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$  that sends  $a \in \mathbb{Z}$  to  $a \bmod N$  in  $\mathbb{Z}/N\mathbb{Z}$ .
- (b) The map  $\phi : \mathbb{R}^* \rightarrow \text{GL}_2(\mathbb{R})$  defined by  $\phi(a) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ .
- (c) The discrete logarithm map  $\log_g : \mathbb{F}_p^* \rightarrow \mathbb{Z}/(p-1)\mathbb{Z}$ , where  $g$  is a primitive root modulo  $p$ .

*Solution to Exercise 2.14.*

*A solution for this exercise is not currently available.*

- 2.15.** (a) Prove that  $\text{GL}_2(\mathbb{F}_p)$  is a group.  
 (b) Show that  $\text{GL}_2(\mathbb{F}_p)$  is a noncommutative group for every prime  $p$ .  
 (c) Describe  $\text{GL}_2(\mathbb{F}_2)$  completely. That is, list its elements and describe the multiplication table.  
 (d) How many elements are there in the group  $\text{GL}_2(\mathbb{F}_p)$ ?  
 (e) How many elements are there in the group  $\text{GL}_n(\mathbb{F}_p)$ ?

*Solution to Exercise 2.15.*

(a) The identity element is the usual matrix  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . The definition of  $\text{GL}_2(\mathbb{F}_p)$  ensures that every element has an inverse. Finally, the associative law is true because it's true in general for matrix multiplication. (But feel free to write it out explicitly for the product of three 2-by-2 matrices.)

(b) Here's an example of noncommuting matrices:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

(If  $p = 2$ , then  $2 = 0$ , but they are still different matrices.)

(c) The group  $\text{GL}_2(\mathbb{F}_2)$  has 6 elements:

$$\begin{array}{lll} e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \alpha = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} & \beta = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \\ \gamma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \delta = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & \epsilon = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \end{array}$$

They satisfy many relations, for example  $\beta = \alpha^2$  and  $\epsilon = \alpha^2\gamma$ . In fact, we can get all 6 elements as

$$e, \alpha, \alpha^2, \gamma, \alpha\gamma, \alpha^2\gamma,$$

and the group operation is determined by the rules

$$\alpha^3 = e, \quad \gamma^2 = e, \quad \gamma\alpha = \alpha^2\gamma.$$

Comparing with Exercise 2.11 we see that  $\text{GL}_2(\mathbb{F}_2)$  is the same as the group  $\mathcal{S}_3$  described in that exercise, we've just named the generating elements  $\alpha$  and  $\gamma$  instead of  $\sigma$  and  $\tau$ .

(d) Let  $\alpha$  be a matrix in  $\text{GL}_2(\mathbb{F}_p)$ . The first row can be any vector except for the 0 vector, so there are  $p^2 - 1$  possibilities for the first row. The second row

can be any vector that is not a scalar multiple of the first row. There are  $p$  possible scalar multiples of the first row, so there are  $p^2 - p$  possibilities for the second row. Hence

$$\# \text{GL}_2(\mathbb{F}_p) = (p^1 - 1)(p^2 - p) = (p - 1)^2 p(p + 1).$$

(e) Using the same reasoning as in (d), there are  $p^n - 1$  allowable first rows, then  $p^n - p$  allowable second rows, then  $p^n - p^2$  allowable third rows (since we have to disallow all linear combinations of the first two rows), etc. Hence

$$\# \text{GL}_n(\mathbb{F}_p) = \prod_{i=0}^{n-1} (p^n - p^i).$$

Section. How hard is the discrete logarithm problem?

**2.16.** Verify the following assertions from Example 2.17.

- |   |  |
|---|--|
| (a) $x^2 + \sqrt{x} = \mathcal{O}(x^2)$ .   | (d) $(\ln k)^{375} = \mathcal{O}(k^{0.001})$ . |
| (b) $5 + 6x^2 - 37x^5 = \mathcal{O}(x^5)$ . | (e) $k^2 2^k = \mathcal{O}(e^{2k})$ .          |
| (c) $k^{300} = \mathcal{O}(2^k)$ .          | (f) $N^{10} 2^N = \mathcal{O}(e^N)$ .          |

Solution to Exercise 2.16.

*A solution for this exercise is not currently available.*

Section. A Collision Algorithm for the DLP

**2.17.** Use Shanks's babystep-giantstep method to solve the following discrete logarithm problems. (For (b) and (c), you may want to write a computer program implementing Shanks's algorithm.)

- (a)  $11^x = 21$  in  $\mathbb{F}_{71}$ .  
 (b)  $156^x = 116$  in  $\mathbb{F}_{593}$ .  
 (c)  $650^x = 2213$  in  $\mathbb{F}_{3571}$ .

Solution to Exercise 2.17.

(a) The number 11 has order 70 in  $\mathbb{F}_{71}$ . Set  $N = \lceil \sqrt{70} \rceil = 9$  and  $H = h^{-N} = 11^{-9} = 7$ . From Table ?? we see that

$$11^1 = 21 \cdot 7^4 = 11 \quad \text{in } \mathbb{F}_{71}.$$

Hence

$$21 = 11^1 \cdot 7^{-4} = 11^1 \cdot (11^9)^4 = 11^{37} \quad \text{in } \mathbb{F}_{71},$$

so the solution is  $\boxed{x=37}$ .

(b) The number 156 has order 148 in  $\mathbb{F}_{593}$ . Set  $N = \lceil \sqrt{148} \rceil = 13$  and  $H = h^{-N} = 156^{-13} = 297$ . From Table ?? we see that

$$156^7 = 116 \cdot 297^4 = 452 \quad \text{in } \mathbb{F}_{593}.$$

$k$	$h^k$	$a \cdot H^k$
1	11	5
2	50	35
3	53	32
4	15	11

Table 2.1: Solve  $11^x \equiv 21 \pmod{71}$  with babystep–giantstep

$k$	$h^k$	$a \cdot H^k$
1	156	58
2	23	29
3	30	311
4	529	452
5	97	226
6	307	113
7	452	353

Table 2.2: Solve  $156^x \equiv 116 \pmod{593}$  via babystep–giantstep

Hence

$$116 = 156^7 \cdot 297^{-4} = 156^7 \cdot (156^{13})^4 = 156^{59} \quad \text{in } \mathbb{F}_{593},$$

so the solution is  $\boxed{x=59}$ .

(c) The number  $h = 650$  has order 510 in  $\mathbb{F}_{3571}$ . Set  $N = \lceil \sqrt{510} \rceil = 23$  and  $H = h^{-N} = 650^{-23} = 1925$ . Table ?? lists the values of  $h^k$  and  $a \cdot H^k$  for  $k = 1, 2, \dots$ . From the table we see that

$$650^{20} = 2213 \cdot 1925^{13} = 3011 \quad \text{in } \mathbb{F}_{3571}.$$

Using the fact that  $1925 = 650^{-23}$ , we compute

$$2213 = 650^{20} \cdot 1925^{-13} = 650^{20} \cdot (650^{23})^{13} = 650^{319} \quad \text{in } \mathbb{F}_{3571},$$

so the solution is  $\boxed{x=319}$ .

Section. The Chinese remainder theorem

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

$k$	$h^k$	$a \cdot H^k$
1	650	3393
2	1122	166
3	816	1731
4	1892	432
5	1376	3128

$k$	$h^k$	$a \cdot H^k$
6	1650	694
7	1200	396
8	1522	1677
9	133	41
10	746	363

$k$	$h^k$	$a \cdot H^k$
11	2815	2430
12	1398	3311
13	1666	<b>3011</b>
14	887	442
15	1619	952

$k$	$h^k$	$a \cdot H^k$
16	2476	677
17	2450	3381
18	3405	2063
19	2801	323
20	<b>3011</b>	421

Table 2.3: Solve  $650^x \equiv 2213 \pmod{3571}$  using babystep–giantstep

- (a)  $x \equiv 3 \pmod{7}$  and  $x \equiv 4 \pmod{9}$ .  
 (b)  $x \equiv 137 \pmod{423}$  and  $x \equiv 87 \pmod{191}$ .  
 (c)  $x \equiv 133 \pmod{451}$  and  $x \equiv 237 \pmod{697}$ .  
 (d)  $x \equiv 5 \pmod{9}$ ,  $x \equiv 6 \pmod{10}$ , and  $x \equiv 7 \pmod{11}$ .  
 (e)  $x \equiv 37 \pmod{43}$ ,  $x \equiv 22 \pmod{49}$ , and  $x \equiv 18 \pmod{71}$ .

Solution to Exercise 2.18.

- (a)  $x \equiv 31 \pmod{63}$ .  
 (b)  $x \equiv 27209 \pmod{80793}$ .  
 (c) No solution, since  $\gcd(451, 697) = 41$  and 133 and 237 are not congruent to one another modulo 41.  
 (d)  $x \equiv 986 \pmod{990}$ .  
 (e)  $x \equiv 11733 \pmod{149597}$ .

**2.19.** Solve the 1700-year-old Chinese remainder problem from the *Sun Tzu Suan Ching* stated on page 82.

Solution to Exercise 2.19.

In the modern notation, the solution in the *Sun Tzu Suan Ching* uses the fact that:

$$\begin{array}{lll} 70 \equiv 1 \pmod{3} & \equiv 0 \pmod{5} & \equiv 0 \pmod{7}, \\ 21 \equiv 0 \pmod{3} & \equiv 1 \pmod{5} & \equiv 0 \pmod{7}, \\ 15 \equiv 0 \pmod{3} & \equiv 0 \pmod{5} & \equiv 1 \pmod{7}. \end{array}$$

Hence  $(2 * 70) + (3 * 21) + (2 * 15) = 233$  satisfies the desired congruences. Since any multiple of 105 is divisible by 3, 5 and 7, we can subtract  $2 * 105$  from 233 to get 23 as the smallest positive solution.

Problem 26 is the only problem in the *Sun Tzu Suan Ching* that illustrates the Chinese remainder theorem. Thus it is not known if the author had developed a general method to solve such problems.

**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  $x = a + \text{cm}$  is a solution to

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}, \quad (2.1)$$

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

Solution to Exercise 2.20.

A solution for this exercise is not currently available.

**2.21.** Let  $x = c$  and  $x = c'$  be two solutions of the system of simultaneous congruences (2.7) in the Chinese remainder theorem (Theorem 2.25). Prove that

$$c \equiv c' \pmod{m_1 m_2 \cdots m_k}.$$

Solution to Exercise 2.21.

*A solution for this exercise is not currently available.*

**2.22.** For those who have studied ring theory, this exercise sketches a short, albeit nonconstructive, proof of the Chinese remainder theorem. Let  $m_1, \dots, m_k$  be integers and let  $m = m_1 m_2 \cdots m_k$  be their product.

(a) Prove that the map

$$\begin{aligned} \frac{\mathbb{Z}}{m\mathbb{Z}} &\longrightarrow \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times \frac{\mathbb{Z}}{m_k\mathbb{Z}} \\ a \bmod m &\longrightarrow (a \bmod m_1, a \bmod m_2, \dots, a \bmod m_k) \end{aligned} \quad (2.2)$$

is a well-defined homomorphism of rings. (*Hint.* First define a homomorphism from  $\mathbb{Z}$  to the right-hand side of (2.25), and then show that  $m\mathbb{Z}$  is in the kernel.)

- (b) Assume that  $m_1, \dots, m_k$  are pairwise relatively prime. Prove that the map given by (2.25) is one-to-one. (*Hint.* What is the kernel?)
- (c) Continuing with the assumption that the numbers  $m_1, \dots, m_k$  are pairwise relatively prime, prove that the map (2.25) is onto. (*Hint.* Use (b) and count the size of both sides.)
- (d) Explain why the Chinese remainder theorem (Theorem 2.25) is equivalent to the assertion that (b) and (c) are true.

Solution to Exercise 2.22.

*A solution for this exercise is not currently available.*

**2.23.** Use the method described in Section 2.8.1 to find square roots modulo the following composite moduli.

- (a) Find a square root of 340 modulo 437. (Note that  $437 = 19 \cdot 23$ .)
- (b) Find a square root of 253 modulo 3143.
- (c) Find four square roots of 2833 modulo 4189. (The modulus factors as  $4189 = 59 \cdot 71$ . Note that your four square roots should be distinct modulo 4189.)
- (d) Find eight square roots of 813 modulo 868.

Solution to Exercise 2.23.

- (a) The square roots of 340 modulo 437 are 146, 215, 222, and 291.
- (b) The square roots of 253 modulo 3143 are 489, 1387, 1756, 2654. (Note  $3143 = 7 \cdot 449$  and 449 is prime.)
- (c) The square roots of 2833 modulo 4189 are 1002, 1712, 2477, and 3187.
- (d) We factor  $868 = 4 \cdot 7 \cdot 31$ . The eight square roots of 813 modulo 868 are 41, 83, 351, 393, 475, 517, 785, and 827.

**2.24.** Let  $p$  be an odd prime and let  $b$  be a square root of  $a$  modulo  $p$ . This exercise investigates the square root of  $a$  modulo powers of  $p$ .

- (a) Prove that for some choice of  $k$ , the number  $b + kp$  is a square root of  $a$  modulo  $p^2$ , i.e.,  $(b + kp)^2 \equiv a \pmod{p^2}$ .

- (b) The number  $b = 537$  is a square root of  $a = 476$  modulo the prime  $p = 1291$ . Use the idea in (a) to compute a square root of 476 modulo  $p^2$ .
- (c) Suppose that  $b$  is a square root of  $a$  modulo  $p^n$ . Prove that for some choice of  $j$ , the number  $b + jp^n$  is a square root of  $a$  modulo  $p^{n+1}$ .
- (d) Explain why (c) implies the following statement: If  $p$  is an odd prime and if  $a$  has a square root modulo  $p$ , then  $a$  has a square root modulo  $p^n$  for every power of  $p$ . Is this true if  $p = 2$ ?
- (e) Use the method in (c) to compute the square root of 3 modulo  $13^3$ , given that  $9^2 \equiv 3 \pmod{13}$ .

Solution to Exercise 2.24.

- (a),(c),(d) *A solution for this exercise is not currently available.*
- (b)  $(b + k \cdot p)^2 \equiv a \pmod{p^2}$  gives  $1074k + 223 \equiv 0 \pmod{p}$ , and hence  $k \equiv 239 \pmod{p}$ . This gives 309086 as the square root of  $a$  modulo  $p^2$ .
- (e) 9863 is the square root of 3 modulo  $13^3$ .

**2.25.** Suppose  $n = pq$  with  $p$  and  $q$  both primes.

- (a) Suppose that  $\gcd(a, pq) = 1$ . Prove that if the equation  $x^2 \equiv a \pmod{n}$  has any solutions, then it has four solutions.
- (b) Suppose you had a machine that could find all four solutions for some given  $a$ . How could you use this machine to factor  $n$ ?

Solution to Exercise 2.25.

*A solution for this exercise is not currently available.*

Section. The Pohlig–Hellman algorithm

**2.26.** Let  $\mathbb{F}_p$  be a finite field and let  $N \mid p - 1$ . Prove that  $\mathbb{F}_p^*$  has an element of order  $N$ . This is true in particular for any prime power that divides  $p - 1$ . (*Hint.* Use the fact that  $\mathbb{F}_p^*$  has a primitive root.)

Solution to Exercise 2.26.

Let  $g$  be a primitive root. Then  $g$  has order  $p - 1$ , so  $h = g^{(p-1)/N}$  has order  $N$ .

**2.27.** Write out your own proof that the Pohlig–Hellman algorithm works in the particular case that  $p - 1 = q_1 \cdot q_2$  is a product of two distinct primes. This provides a good opportunity for you to understand how the proof works and to get a feel for how it was discovered.

Solution to Exercise 2.27.

*A solution for this exercise will not be provided.*

**2.28.** Use the Pohlig–Hellman algorithm (Theorem 2.32) to solve the discrete logarithm problem

$$g^x = a \quad \text{in } \mathbb{F}_p$$

in each of the following cases.

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

- (b)  $p = 746497$ ,  $g = 10$ ,  $a = 243278$ .  
 (c)  $p = 41022299$ ,  $g = 2$ ,  $a = 39183497$ . (*Hint.*  $p = 2 \cdot 29^5 + 1$ .)  
 (d)  $p = 1291799$ ,  $g = 17$ ,  $a = 192988$ . (*Hint.*  $p - 1$  has a factor of 709.)

Solution to Exercise 2.28.

(a) Step 1 is to solve

$q$	$e$	$h = g^{(p-1)/q^e}$	$b = a^{(p-1)/q^e}$	$y$ with $h^y = b$
2	4	265	250	15
3	3	374	335	20

Step 2 is to solve

$$x \equiv 15 \pmod{2^4}, \quad x \equiv 20 \pmod{3^3}.$$

The solution is  $\boxed{x=47}$ .

(b) Step 1 is to solve

$q$	$e$	$h = g^{(p-1)/q^e}$	$b = a^{(p-1)/q^e}$	$y$ with $h^y = b$
2	10	4168	38277	523
3	6	674719	322735	681

Step 2 is to solve

$$x \equiv 523 \pmod{2^{10}}, \quad x \equiv 681 \pmod{3^6}.$$

The solution is  $\boxed{x=223755}$ .

(c) Step 1 is to solve

$q$	$e$	$h = g^{(p-1)/q^e}$	$b = a^{(p-1)/q^e}$	$y$ with $h^y = b$
2	1	41022298	1	0
29	5	4	11844727	13192165

In order to solve the discrete logarithm problem modulo  $29^5$ , it is best to solve it step by step. Note that  $4^{29^4} = 18794375$  is an element of order 29 in  $\mathbb{F}_p^*$ . To avoid notational confusion, we use the letter  $u$  for the exponents.

First solve  $18794375^{u_0} = (11844727)^{29^4} = 987085$ . The solution is  $u_0 = 7$ . The value of  $u$  so far is  $u = 7$ .

Solve  $18794375^{u_1} = (11844727 \cdot 4^{-7})^{29^3} = 8303208$ . The solution is  $u_1 = 8$ . The value of  $u$  so far is  $u = 239 = 7 + 8 \cdot 29$ .

Solve  $18794375^{u_2} = (11844727 \cdot 4^{-239})^{29^2} = 30789520$ . The solution is  $u_2 = 26$ . The value of  $u$  so far is  $u = 22105 = 7 + 8 \cdot 29 + 26 \cdot 29^2$ .

Solve  $18794375^{u_3} = (11844727 \cdot 4^{-22105})^{29^1} = 585477$ . The solution is  $u_3 = 18$ . The value of  $u$  so far is  $u = 461107 = 7 + 8 \cdot 29 + 26 \cdot 29^2 + 18 \cdot 29^3$ .

Solve  $18794375^{u_4} = (11844727 \cdot 4^{-461107})^{29^0} = 585477$ . The solution is  $u_4 = 18$ . The final value of  $u$  is  $u = 13192165 = 7 + 8 \cdot 29 + 26 \cdot 29^2 + 18 \cdot 29^3 + 18 \cdot 29^4$ , which is the number you see in the last column of the table.

Step 2 is to solve

$$x \equiv 0 \pmod{2}, \quad x \equiv 13192165 \pmod{29^5}.$$

The solution is  $\boxed{x=33703314}$ .

(d) Step 1 is to solve

$q$	$e$	$h = g^{(p-1)/q^e}$	$b = a^{(p-1)/q^e}$	$y$ with $h^y = b$
2	1	1291798	1	0
709	1	679773	566657	322
911	1	329472	898549	534

There is no magical way to solve the DLP's modulo 709 or 911, although they are easily solved by an exhaustive search on a computer, and a collision algorithm is even faster. Step 2 is to solve

$$x \equiv 0 \pmod{2}, \quad x \equiv 322 \pmod{709}, \quad x \equiv 534 \pmod{911}.$$

The solution is  $\boxed{x=984414}$ .

Section. Rings, quotient rings, polynomial rings, and finite fields

**2.29.** Let  $R$  be a ring with the property that the only way that a product  $a \cdot b$  can be 0 is if  $a = 0$  or  $b = 0$ . (In the terminology of Example 2.56, the ring  $R$  has no zero divisors.) Suppose further that  $R$  has only finitely many elements. Prove that  $R$  is a field. (*Hint.* Let  $a \in R$  with  $a \neq 0$ . What can you say about the map  $R \rightarrow R$  defined by  $b \mapsto a \cdot b$ ?)

Solution to Exercise 2.29.

*A solution for this exercise is not currently available.*

**2.30.** Let  $R$  be a ring. Prove the following properties of  $R$  directly from the ring axioms described in Section 2.10.1.

- Prove that the additive identity element  $0 \in R$  is unique, i.e., prove that there is only one element in  $R$  satisfying  $0 + a = a + 0 = 0$  for every  $a \in R$ .
- Prove that the multiplicative identity element  $1 \in R$  is unique.
- Prove that every element of  $R$  has a unique additive inverse.
- Prove that  $0 \star a = a \star 0 = 0$  for all  $a \in R$ .
- We denote the additive inverse of  $a$  by  $-a$ . Prove that  $-(-a) = a$ .
- Let  $-1$  be the additive inverse of the multiplicative identity element  $1 \in R$ . Prove that  $(-1) \star (-1) = 1$ .
- Prove that  $b \mid 0$  for every nonzero  $b \in R$ .
- Prove that an element of  $R$  has at most one multiplicative inverse.

Solution to Exercise 2.30.

- If  $0$  and  $0'$  are both additive identities, then

$$0' = 0' + 0 = 0.$$



(b) If 1 and  $1'$  are both multiplicative identities, then

$$1' = 1' \star 1 = 1.$$

(c) If  $b$  and  $c$  are both additive inverses of  $a$ , then

$$b = b + 0 = b + (c + b') = (b + c) + b' = 0 + b' = b'.$$

(d)

$$0 \star a = (0 + 0) \star a = (0 \star a) + (0 \star a).$$

Subtracting  $0 \star a$  from both sides give  $0 \star a = 0$ . (Note “subtraction” really means to add the additive inverse.)

(e) Let  $b = -(-a)$ . Then by definition,  $b + (-a) = 0$ . But we also know by definition that  $a + (-a) = 0$ . Since additive inverses are unique from (c), it follows that  $b = a$ .

(f) To ease notation, we let  $i = 1$  and  $u = -1$ . Then

$$0 = 0 \star u = (i + u) \star u = (i \star u) + (u \star u) = u + (u \star u).$$

Thus  $u \star u$  is the additive inverse of  $u$ . Using (e) gives  $(-1) \star (-1) = -(-1) = 1$ .

(g) We have  $b \star 0 = 0$  from (d), so  $b \mid 0$  by definition of divisibility.

(h) Let  $a \in R$  and suppose that  $ab = 1$  and  $ac = 1$ , so  $b$  and  $c$  are both multiplicative inverses of  $a$ . Then

$$b = b \cdot 1 = b \cdot (a \cdot c) = (a \cdot b) \cdot c = 1 \cdot c = c.$$

Thus  $b = c$ , so  $a$  has at most one multiplicative inverse.

**2.31.** Prove Proposition 2.42.

Solution to Exercise 2.31.

*A solution for this exercise is not currently available.*

**2.32.** Prove Proposition 2.44. (*Hint.* First use Exercise 2.31 to prove that the congruence classes  $\overline{a+b}$  and  $\overline{a \star b}$  depend only on the congruence classes of  $a$  and  $b$ .)

Solution to Exercise 2.32.

*A solution for this exercise is not currently available.*

**2.33.** Let  $\mathbb{F}$  be a field and let  $\mathbf{a}$  and  $\mathbf{b}$  be nonzero polynomials in  $\mathbb{F}[x]$ .

- Prove that  $\deg(\mathbf{a} \cdot \mathbf{b}) = \deg(\mathbf{a}) + \deg(\mathbf{b})$ .
- Prove that  $\mathbf{a}$  has a multiplicative inverse in  $\mathbb{F}[x]$  if and only if  $\mathbf{a}$  is in  $\mathbb{F}$ , i.e., if and only if  $\mathbf{a}$  is a constant polynomial.
- Prove that every nonzero element of  $\mathbb{F}[x]$  can be factored into a product of irreducible polynomials. (*Hint.* Use (a), (b), and induction on the degree of the polynomial.)

- (d) Let  $R$  be the ring  $\mathbb{Z}/6\mathbb{Z}$ . Give an example to show that (a) is false for some polynomials  $\mathbf{a}$  and  $\mathbf{b}$  in  $R[x]$ .

*Solution to Exercise 2.33.*

- (a) *A solution for this exercise is not currently available.*  
 (b) If  $\mathbf{a} \cdot \mathbf{b} = 1$ , then taking degrees and using (a) gives

$$0 = \deg(1) = \deg(\mathbf{a} \cdot \mathbf{b}) = \deg(\mathbf{a}) + \deg(\mathbf{b}).$$

The degree of a nonzero polynomial is a nonnegative integer, so we conclude that  $\deg(\mathbf{a}) = \deg(\mathbf{b}) = 0$ . Hence  $\mathbf{a}$  and  $\mathbf{b}$  are constant polynomials.

(c) Polynomials of degree 0 and 1 are already irreducible. Suppose we know that every polynomial of degree smaller than  $n$  can be factored into a product of irreducible polynomials, and let  $\mathbf{a} \in \mathbb{F}[x]$  have degree  $n$ . If  $\mathbf{a}$  is itself irreducible, we're done. Otherwise it factors as  $\mathbf{a} = \mathbf{b} \cdot \mathbf{c}$ , where neither  $\mathbf{b}$  nor  $\mathbf{c}$  is a unit. It follows from (b) that  $\mathbf{b}$  and  $\mathbf{c}$  both have degree at least 1, so using (a) we find that  $\mathbf{b}$  and  $\mathbf{c}$  have degrees that are strictly smaller than the degree of  $\mathbf{a}$ . Hence by induction, both  $\mathbf{b}$  and  $\mathbf{c}$  can be factored as a product of irreducible polynomials. But then their product, which equals  $\mathbf{a}$ , is also a product of irreducible polynomials.

(d) Let  $\mathbf{a} = 2x + 1$  and  $\mathbf{b} = 3x + 1$ , then  $\mathbf{a} \cdot \mathbf{b} = 6x^2 + 5x + 1 = 5x + 1$ , since  $6 = 0$  in  $\mathbb{Z}/6\mathbb{Z}$ . Hence

$$\deg(\mathbf{a}) = \deg(\mathbf{b}) = \deg(\mathbf{a} \cdot \mathbf{b}) = 1,$$

so the degree formula in (a) is false.

**2.34.** Let  $\mathbf{a}$  and  $\mathbf{b}$  be the polynomials

$$\mathbf{a} = x^5 + 3x^4 - 5x^3 - 3x^2 + 2x + 2,$$

$$\mathbf{b} = x^5 + x^4 - 2x^3 + 4x^2 + x + 5.$$

Use the Euclidean algorithm to compute  $\gcd(\mathbf{a}, \mathbf{b})$  in each of the following rings.

- (a)  $\mathbb{F}_2[x]$     (b)  $\mathbb{F}_3[x]$     (c)  $\mathbb{F}_5[x]$     (d)  $\mathbb{F}_7[x]$ .

*Solution to Exercise 2.34.*

- (a)  $\gcd_{\mathbb{F}_2[x]}(\mathbf{a}, \mathbf{b}) = x^3 + x^2 + x + 1$ .  
 (b)  $\gcd_{\mathbb{F}_3[x]}(\mathbf{a}, \mathbf{b}) = x^2 + x + 2$ .  
 (c)  $\gcd_{\mathbb{F}_5[x]}(\mathbf{a}, \mathbf{b}) = x + 4$ .  
 (d)  $\gcd_{\mathbb{F}_7[x]}(\mathbf{a}, \mathbf{b}) = 1$ .

(Note for instructor: The resultant of  $\mathbf{a}$  and  $\mathbf{b}$  is  $-2^3 \cdot 3^2 \cdot 5 \cdot 59 \cdot 107$ , so  $\gcd(\mathbf{a}, \mathbf{b}) = 1$  in  $\mathbb{F}_p[x]$  unless  $p \in \{2, 3, 5, 59, 107\}$ .)

**2.35.** Continuing with the same polynomials  $\mathbf{a}$  and  $\mathbf{b}$  as in Exercise 2.34, for each of the polynomial rings (a), (b), (c), and (d) in Exercise 2.34, find polynomials  $\mathbf{u}$  and  $\mathbf{v}$  satisfying

$$\mathbf{a} \cdot \mathbf{u} + \mathbf{b} \cdot \mathbf{v} = \gcd(\mathbf{a}, \mathbf{b}).$$

Solution to Exercise 2.35.

- (a)  $\mathbf{u} = 1$  and  $\mathbf{v} = 1$ .
- (b)  $\mathbf{u} = x + 1$  and  $\mathbf{v} = 2x$ .
- (c)  $\mathbf{u} = 3x^3 + 4x^2 + x + 2$  and  $\mathbf{v} = 2x^3 + x$ .
- (d)  $\mathbf{u} = 3x^4 + 3x^3 + x^2 + 5x + 4$  and  $\mathbf{v} = 4x^4 + 5x^3 + x^2 + 2x$ .

**2.36.** Prove that the polynomial  $x^3 + x + 1$  is irreducible in  $\mathbb{F}_2[x]$ . (*Hint.* Think about what a factorization would have to look like.)

Solution to Exercise 2.36.

If  $x^3 + x + 1$  factors, then it can be written as the product of a linear polynomial and a quadratic polynomial. Since the only possible coefficients are 0 and 1, this means we would have

$$x^3 + x + 1 = (x + a)(x^2 + bx + c) \quad \text{in } \mathbb{F}_2[x].$$

Putting  $x = 0$  yields  $1 = ac$ , so we must have  $a = c = 1$ . (Remember that  $a$  and  $c$  are in  $\mathbb{F}_2$ , so they are either 0 or 1.) Now we have

$$x^3 + x + 1 = (x + 1)(x^2 + bx + 1),$$

and putting  $x = 1$  yields  $1 = 2 \cdot (2 + b) = 0$ . This contradiction shows that  $x^3 + x + 1$  does not factor in  $\mathbb{F}_2[x]$ .

**2.37.** The multiplication table for the field  $\mathbb{F}_2[x]/(x^3 + x + 1)$  is given in Table 2.5, but we have omitted fourteen entries. Fill in the missing entries. (This is the field described in Example 2.58. You can download and print a copy of Table 2.5 at [www.math.brown.edu/~jhs/MathCrypto/Table2.5.pdf](http://www.math.brown.edu/~jhs/MathCrypto/Table2.5.pdf).)

Solution to Exercise 2.37.

Note that it's not necessary to compute both  $\mathbf{a} \cdot \mathbf{b}$  and  $\mathbf{b} \cdot \mathbf{a}$ . Half missing entries in the table are

$$\begin{aligned} 1 \cdot x^2 &= x^2 \\ x \cdot (x^2 + x) &= x^2 + x + 1 \\ x^2 \cdot x &= x + 1 \\ (x + 1) \cdot 1 &= x + 1 \\ (x^2 + 1) \cdot (x + 1) &= x^2 \\ (x^2 + x) \cdot (x^2 + x + 1) &= x^2 \\ (x^2 + x + 1) \cdot (x^2 + 1) &= x^2 + x. \end{aligned}$$

The other half are the same products in the opposite order.

	0	1	$x$	$x^2$	$1+x$	$1+x^2$	$x+x^2$	$1+x+x^2$
0	0	0	0	0	0	0	0	0
1	0	1	$x$			$1+x^2$	$x+x^2$	$1+x+x^2$
$x$	0	$x$	$x^2$		$x+x^2$	1		$1+x^2$
$x^2$	0			$x+x^2$	$1+x+x^2$	$x$	$1+x^2$	1
$1+x$	0		$x+x^2$	$1+x+x^2$	$1+x^2$		1	$x$
$1+x^2$	0	$1+x^2$	1	$x$		$1+x+x^2$	$1+x$	
$x+x^2$	0	$x+x^2$		$1+x^2$	1	$1+x$	$x$	
$1+x+x^2$	0	$1+x+x^2$	$1+x^2$	1	$x$			$1+x$

Table 2.4: Multiplication table for the field  $\mathbb{F}_2[x]/(x^3 + x + 1)$ 

**2.38.** The field  $\mathbb{F}_7[x]/(x^2 + 1)$  is a field with 49 elements, which for the moment we denote by  $\mathbb{F}_{49}$ . (See Example 2.59 for a convenient way to work with  $\mathbb{F}_{49}$ .)

(a) Is  $2 + 5x$  a primitive root in  $\mathbb{F}_{49}$ ?

(b) Is  $2 + x$  a primitive root in  $\mathbb{F}_{49}$ ?

(c) Is  $1 + x$  a primitive root in  $\mathbb{F}_{49}$ ?

(*Hint.* Lagrange's theorem says that the order of  $u \in \mathbb{F}_{49}$  must divide 48. So if  $u^k \neq 1$  for all proper divisors  $k$  of 48, then  $u$  is a primitive root.)

Solution to Exercise 2.38.

(a) No,  $(2 + x)^8 = 1$ .

(b) Yes. It suffices to check that  $(2 + x)^{16} = 4$  and  $(2 + x)^{24} = 6$  are not equal to 1.

(c) No,  $(1 + x)^{24} = 1$ .

**2.39.** Let  $p$  be a prime number and let  $e \geq 2$ . The quotient ring  $\mathbb{Z}/p^e\mathbb{Z}$  and the finite field  $\mathbb{F}_{p^e}$  are both rings and both have the same number of elements. Describe some ways in which they are intrinsically different.

Solution to Exercise 2.39.

Every nonzero element in the field  $\mathbb{F}_{p^e}$  has a multiplicative inverse, while  $\mathbb{Z}/(p^e)$  has lots of elements that do not have inverses, for example all elements of the form  $kp$  with  $1 \leq k < p^{e-1}$ . In the field  $\mathbb{F}_{p^e}$ , if a product  $ab = 0$ , then either  $a = 0$  or  $b = 0$ . (To see this, note that if  $a \neq 0$ , then  $a^{-1}$  exists, so multiplying  $ab = 0$  by  $a^{-1}$  shows that  $b = 0$ .) On the other hand,  $\mathbb{Z}/(p^e)$  does not have this property. For example,  $p \cdot p^{e-1} = 0$ , but neither  $p$  nor  $p^{e-1}$  is 0 in  $\mathbb{Z}/(p^e)$ . A subtler property is that every element  $\alpha$  of  $\mathbb{F}_{p^e}$  satisfies  $\alpha^{p^e} = \alpha$ , but this is not true in  $\mathbb{Z}/(p^e)$ . For example, if we take  $\alpha = p$ , the  $\alpha^{p^e} = 0$ .

**2.40.** Let  $\mathbb{F}$  be a finite field.

(a) Prove that there is an integer  $m \geq 1$  such that if we add 1 to itself  $m$  times,

$$\underbrace{1 + 1 + \cdots + 1}_{m \text{ ones}},$$

then we get 0. Note that here 1 and 0 are the multiplicative and additive identity elements of the field  $\mathbb{F}$ . If the notation is confusing, you can let  $u$  and  $z$  be the multiplicative and additive identity elements of  $\mathbb{F}$ , and then you need to prove that  $u + u + \cdots + u = z$ . (*Hint.* Since  $\mathbb{F}$  is finite, the numbers  $1, 1 + 1, 1 + 1 + 1, \dots$  cannot all be different.)

- (b) Let  $m$  be the smallest positive integer with the property described in (a). Prove that  $m$  is prime. (*Hint.* If  $m$  factors, show that there are nonzero elements in  $\mathbb{F}$  whose product is zero, so  $\mathbb{F}$  cannot be a field.) This prime is called the *characteristic of the field*  $\mathbb{F}$ .
- (c) Let  $p$  be the characteristic of  $\mathbb{F}$ . Prove that  $\mathbb{F}$  is a finite-dimensional vector space over the field  $\mathbb{F}_p$  of  $p$  elements.
- (d) Use (c) to deduce that  $\mathbb{F}$  has  $p^d$  elements for some  $d \geq 1$ .

Solution to Exercise 2.40.

- (a) The fact that  $\mathbb{F}$  is finite means that when we look at

$$1, \quad 1 + 1, \quad 1 + 1 + 1, \quad 1 + 1 + 1 + 1, \dots$$

eventually we get a repeated value. Subtracting the smaller number of terms from the larger, it follows that some sum of 1's is equal to 0 in  $\mathbb{F}$ .

- (b) Suppose that  $m$  factors as  $m = qr$ . Then we have

$$\underbrace{1 + 1 + \cdots + 1}_{q \text{ ones}} \cdot \underbrace{1 + 1 + \cdots + 1}_{r \text{ ones}} = \underbrace{1 + 1 + \cdots + 1}_{m \text{ ones}} = 0.$$

Since  $\mathbb{F}$  is a field, the only way for a product to be 0 is for one of the factors to be 0, so we have either

$$\underbrace{1 + 1 + \cdots + 1}_{q \text{ ones}} = 0 \quad \text{or} \quad \underbrace{1 + 1 + \cdots + 1}_{r \text{ ones}} = 0 \quad \text{in } \mathbb{F}.$$

But we defined  $m$  to be the smallest number of 1's that sums to 0, so either  $q \geq m$  or  $r \geq m$ . Since we also have  $m = qr$ , it follows that either  $q = m$  (and  $r = 1$ ) or  $r = m$  (and  $q = 1$ ). This proves that  $m$  is prime.

(c) It follows that we have a copy of  $\mathbb{F}_p$  inside  $\mathbb{F}$  by sending 1 to 1 and  $1 + 1$  to  $1 + 1$ , etc. The axioms for a field show that this makes  $\mathbb{F}$  into a vector space using  $\mathbb{F}_p$  as scalars. By standard linear algebra,  $\mathbb{F}$  has a basis as a vector space over  $\mathbb{F}_p$ , and the basis is finite since  $\mathbb{F}$  itself is finite. Hence  $\mathbb{F}$  is a finite-dimensional vector space over  $\mathbb{F}_p$ .

(d) Let  $\mathbf{v}_1, \dots, \mathbf{v}_d$  be a basis for  $\mathbb{F}$  as a vector space over  $\mathbb{F}_p$ . Then every element of  $\mathbb{F}$  can be written uniquely as

$$a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \cdots + a_d \mathbf{v}_d \quad \text{with } a_1, \dots, a_d \in \mathbb{F}_p.$$

There are  $p$  choices of  $a_1$ , and  $p$  choices of  $a_2$ , and  $p$  choices of  $a_3$ , etc. So there are  $p^d$  distinct elements in  $\mathbb{F}$ .

## Chapter 3

# Integer Factorization and RSA

### Exercises for Chapter 3

Section. Euler's theorem and roots modulo  $pq$

**3.1.** Solve the following congruences.

- (a)  $x^{19} \equiv 36 \pmod{97}$ .
- (b)  $x^{137} \equiv 428 \pmod{541}$ .
- (c)  $x^{73} \equiv 614 \pmod{1159}$ .
- (d)  $x^{751} \equiv 677 \pmod{8023}$ .
- (e)  $x^{38993} \equiv 328047 \pmod{401227}$ . (*Hint.*  $401227 = 607 \cdot 661$ .)

*Solution to Exercise 3.1.*

- (a) 97 is prime. The congruence  $19d \equiv 1 \pmod{96}$  has solution  $d \equiv 91 \pmod{96}$ . Then  $x \equiv 36^{91} \equiv 36 \pmod{97}$ .
- (b) 541 is prime. The congruence  $137d \equiv 1 \pmod{540}$  has solution  $d \equiv 473 \pmod{540}$ . Then  $x \equiv 428^{473} \equiv 213 \pmod{541}$ .
- (c)  $1159 = 19 \cdot 61$  and  $18 \cdot 60 = 1080$ . The congruence  $73d \equiv 1 \pmod{1080}$  has solution  $d \equiv 577 \pmod{1080}$ . Then  $x \equiv 614^{577} \equiv 158 \pmod{1159}$ . More efficiently,  $g = \gcd(18, 60) = 6$  and  $(18)(60)/6 = 180$ . The congruence  $73d \equiv 1 \pmod{180}$  has solution  $d \equiv 37 \pmod{180}$ . Then  $x \equiv 614^{37} \equiv 158 \pmod{1159}$ .
- (d)  $8023 = 71 \cdot 113$  and  $71 \cdot 112 = 7840$ . The congruence  $751d \equiv 1 \pmod{7840}$  has solution  $d \equiv 7151 \pmod{7840}$ . Then  $x \equiv 677^{7151} \equiv 1355 \pmod{8023}$ . More efficiently,  $g = \gcd(70, 112) = 14$  and  $(70)(112)/14 = 560$ . The congruence  $751d \equiv 1 \pmod{560}$  has solution  $d \equiv 431 \pmod{560}$ . Then  $x \equiv 677^{431} \equiv 1355 \pmod{8023}$ .
- (e)  $401227 = 607 \cdot 661$  and  $608 \cdot 660 = 399960$ . The congruence  $38993d \equiv 1 \pmod{399960}$  has the solution  $d \equiv 265457 \pmod{399960}$ . Then  $x \equiv$

$328047^{265457} \equiv 36219 \pmod{401227}$ . More efficiently,  $g = \gcd(606, 660) = 6$  and  $(606)(660)/6 = 66660$ . The congruence  $38993d \equiv 1 \pmod{66660}$  has the solution  $d \equiv 65477 \pmod{66660}$ . Then  $x \equiv 328047^{65477} \equiv 36219 \pmod{401227}$ .

**3.2.** Let  $p$  and  $q$  be distinct primes and let  $e$  and  $d$  be integers satisfying

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

Suppose further that  $c$  is an integer with  $\gcd(c, pq) > 1$ . Prove that

$$x \equiv c^d \pmod{pq} \quad \text{is a solution to the congruence} \quad x^e \equiv c \pmod{pq},$$

thereby completing the proof of Proposition 3.4.

Solution to Exercise 3.2.

If  $pq \mid c$ , then the solution is  $x = 0$ . So the interesting case is when  $c$  is divisible by exactly one of  $p$  and  $q$ , say  $p \mid c$  and  $q \nmid c$ . Then  $x \equiv c^d \equiv 0 \pmod{p}$  is a solution to  $x^e \equiv c \equiv 0 \pmod{p}$ , so we only need to check that it is true modulo  $q$ . We compute

$$(c^d)^e \equiv c^{1+k(p-1)(q-1)} \equiv c \cdot (c^{q-1})^{k(p-1)} \equiv c \pmod{q},$$

since  $c^{q-1} \equiv 1 \pmod{q}$  from Fermat's little theorem.

**3.3.** Recall from Section 1.3 that *Euler's phi function*  $\phi(N)$  is the function defined by

$$\phi(N) = \#\{0 \leq k < N : \gcd(k, N) = 1\}.$$

In other words,  $\phi(N)$  is the number of integers between 0 and  $N-1$  that are relatively prime to  $N$ , or equivalently, the number of elements in  $\mathbb{Z}/N\mathbb{Z}$  that have inverses modulo  $N$ .

- Compute the values of  $\phi(6)$ ,  $\phi(9)$ ,  $\phi(15)$ , and  $\phi(17)$ .
- If  $p$  is prime, what is the value of  $\phi(p)$ ?
- Prove *Euler's formula*

$$a^{\phi(N)} \equiv 1 \pmod{N} \quad \text{for all integers } a \text{ satisfying } \gcd(a, N) = 1.$$

(*Hint.* Mimic the proof of Fermat's little theorem (Theorem 1.25), but instead of looking at all of the multiples of  $a$  as was done in (1.8), just take the multiples  $ka$  of  $a$  for values of  $k$  satisfying  $\gcd(k, N) = 1$ .)

Solution to Exercise 3.3.

*A solution for this exercise is not currently available.*

**3.4.** Euler's phi function has many beautiful properties.

- If  $p$  and  $q$  are distinct primes, how is  $\phi(pq)$  related to  $\phi(p)$  and  $\phi(q)$ ?

- (b) If  $p$  is prime, what is the value of  $\phi(p^2)$ ? How about  $\phi(p^j)$ ? Prove that your formula for  $\phi(p^j)$  is correct. (*Hint.* Among the numbers between 0 and  $p^j - 1$ , remove the ones that have a factor of  $p$ . The ones that are left are relatively prime to  $p$ .)
- (c) Let  $M$  and  $N$  be integers satisfying  $\gcd(M, N) = 1$ . Prove the multiplication formula

$$\phi(MN) = \phi(M)\phi(N).$$

- (d) Let  $p_1, p_2, \dots, p_r$  be the distinct primes that divide  $N$ . Use your results from (b) and (c) to prove the following formula:

$$\phi(N) = N \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

- (e) Use the formula in (d) to compute the following values of  $\phi(N)$ .

(i)  $\phi(1728)$ . (ii)  $\phi(1575)$ . (iii)  $\phi(889056)$  (*Hint.*  $889056 = 2^5 \cdot 3^4 \cdot 7^3$ ).

Solution to Exercise 3.4.

- (a)–(d) *A solution for this exercise is not currently available.*
- (e) (i)  $\phi(1728) = 576$ , (ii)  $\phi(1575) = 720$ , (iii)  $\phi(889056) = 254016$ .

**3.5.** Let  $N$ ,  $c$ , and  $e$  be positive integers satisfying the conditions  $\gcd(N, c) = 1$  and  $\gcd(e, \phi(N)) = 1$ .

- (a) Explain how to solve the congruence

$$x^e \equiv c \pmod{N},$$

assuming that you know the value of  $\phi(N)$ . (*Hint.* Use the formula in Exercise 3.3(c).)

- (b) Solve the following congruences. (The formula in Exercise 3.4(d) may be helpful for computing the value of  $\phi(N)$ .)

- (i)  $x^{577} \equiv 60 \pmod{1463}$ .  
(ii)  $x^{959} \equiv 1583 \pmod{1625}$ .  
(iii)  $x^{133957} \equiv 224689 \pmod{2134440}$ .

Solution to Exercise 3.5.

- (a) *A solution for this exercise is not currently available.*
- (b) (i)  $N = 7 \cdot 11 \cdot 19$ , so

$$\phi(1463) = 1463 \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{11}\right) \left(1 - \frac{1}{19}\right) = 1080.$$

We compute  $d \equiv 577^{-1} \equiv 73 \pmod{1080}$ , so

$$x \equiv 60^{73} \equiv \boxed{1390} \pmod{1463}.$$



Check:  $1390^{577} \equiv 60 \pmod{1463}$ . ✓

(ii)  $N = 5^3 \cdot 13$ , so

$$\phi(1625) = 1625 \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{13}\right) = 1200.$$

We compute  $d \equiv 959^{-1} \equiv 239 \pmod{1200}$ , so

$$x \equiv 1583^{239} \equiv \boxed{147} \pmod{1625}.$$

Check:  $147^{959} \equiv 1583 \pmod{1625}$ . ✓

(iii)  $N = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11^2$ , so

$$\begin{aligned} \phi(2134440) &= 2134440 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{11}\right) \\ &= 443520. \end{aligned}$$

We compute  $d \equiv 133957^{-1} \equiv 326413 \pmod{443520}$ , so

$$x \equiv 224689^{326413} \equiv \boxed{1892929} \pmod{2134440}.$$

Check:  $1892929^{133957} \equiv 224689 \pmod{2134440}$ . ✓

Section. The RSA public key cryptosystem

**3.6.** Alice publishes her RSA public key: modulus  $N = 2038667$  and exponent  $e = 103$ .

- (a) Bob wants to send Alice the message  $m = 892383$ . What ciphertext does Bob send to Alice?
- (b) Alice knows that her modulus factors into a product of two primes, one of which is  $p = 1301$ . Find a decryption exponent  $d$  for Alice.
- (c) Alice receives the ciphertext  $c = 317730$  from Bob. Decrypt the message.

*Solution to Exercise 3.6.*

- (a) Bob sends  $c = m^e = 892383^{103} \equiv \boxed{45293} \pmod{2038667}$ .
- (b) The modulus is  $N = 2038667 = 1301 \cdot 1567$ , so  $\phi(N) = 1300 \cdot 1568 = 2035800$ . A decryption exponent is given by a solution to

$$103d \equiv 1 \pmod{2035800}.$$

The solution is  $d \equiv \boxed{810367} \pmod{2035800}$ .

- (c) Alice needs to solve

$$m^{103} \equiv 317730 \pmod{2038667}.$$

Raising both sides to the  $d^{\text{th}}$  power, where  $d = 810367$  is her decryption exponent, yields

$$m \equiv 317730^{810367} \equiv \boxed{514407} \pmod{2038667}.$$

**3.7.** Bob's RSA public key has modulus  $N = 12191$  and exponent  $e = 37$ . Alice sends Bob the ciphertext  $c = 587$ . Unfortunately, Bob has chosen too small a modulus. Help Eve by factoring  $N$  and decrypting Alice's message. (*Hint.*  $N$  has a factor smaller than 100.)

Solution to Exercise 3.7.

The modulus factors as  $N = 12191 = 73 \cdot 167$ , so  $\phi(N) = 72 \cdot 166 = 11952$ . The congruence

$$37d \equiv 1 \pmod{11952}$$

has solution  $d \equiv 11629 \pmod{11952}$ . Then

$$m \equiv 587^{11629} \equiv \boxed{4894} \pmod{12191}$$

is a solution to  $m^{37} \equiv 587 \pmod{12191}$ .

It is possible to be a bit more efficient, using the fact that  $g = \gcd(72, 166) = 2$  and  $(72)(166)/2 = 5976$ . Thus a solution to the congruence

$$37d \equiv 1 \pmod{5976}$$

is a decryption exponent, giving the smaller decryption exponent  $d \equiv 5653 \pmod{5976}$ . Of course, this gives the same plaintext

$$m \equiv 587^{5653} \equiv \boxed{4894} \pmod{12191}.$$

**3.8.** For each of the given values of  $N = pq$  and  $(p-1)(q-1)$ , use the method described in Remark 3.10 to determine  $p$  and  $q$ .

- (a)  $N = pq = 352717$  and  $(p-1)(q-1) = 351520$ .
- (b)  $N = pq = 77083921$  and  $(p-1)(q-1) = 77066212$ .
- (c)  $N = pq = 109404161$  and  $(p-1)(q-1) = 109380612$ .
- (d)  $N = pq = 172205490419$  and  $(p-1)(q-1) = 172204660344$ .

Solution to Exercise 3.8.

(a) Suppose that  $N = pq = 352717$  and  $(p-1)(q-1) = 351520$ . Then  $p+q = N+1 - (p-1)(q-1) = 1198$ , so

$$X^2 - (p+q)X + N = X^2 - 1198X + 352717 = (X - 677)(X - 521).$$

Hence  $N = 352717 = 677 \cdot 521$ .

(b) Suppose that  $N = pq = 77083921$  and  $(p-1)(q-1) = 77066212$ . Then  $p+q = N+1 - (p-1)(q-1) = 17710$ , so

$$X^2 - (p+q)X + N = X^2 - 17710X + 77083921 = (X - 10007)(X - 7703).$$

Hence  $N = 77083921 = 10007 \cdot 7703$ .

(c) Suppose that  $N = pq = 109404161$  and  $(p-1)(q-1) = 109380612$ . Then  $p+q = N+1 - (p-1)(q-1) = 23550$ , so

$$X^2 - (p+q)X + N = X^2 - 23550X + 109404161 = (X - 6367)(X - 17183).$$

Hence  $N = 109404161 = 6367 \cdot 17183$ .

(d) Suppose that  $N = pq = 172205490419$  and  $(p-1)(q-1) = 172204660344$ . Then  $p+q = N+1 - (p-1)(q-1) = 830076$ , so

$$X^2 - (p+q)X + N = X^2 - 830076X + 172205490419 = (X - 407893)(X - 422183).$$

Hence  $N = 172205490419 = 407893 \cdot 422183$ .

**3.9.** A *decryption exponent* for an RSA public key  $(N, e)$  is an integer  $d$  with the property that  $a^{de} \equiv a \pmod{N}$  for all integers  $a$  that are relatively prime to  $N$ .

- (a) Suppose that Eve has a magic box that creates decryption exponents for  $(N, e)$  for a fixed modulus  $N$  and for a large number of different encryption exponents  $e$ . Explain how Eve can use her magic box to try to factor  $N$ .
- (b) Let  $N = 38749709$ . Eve's magic box tells her that the encryption exponent  $e = 10988423$  has decryption exponent  $d = 16784693$  and that the encryption exponent  $e = 25910155$  has decryption exponent  $d = 11514115$ . Use this information to factor  $N$ .
- (c) Let  $N = 225022969$ . Eve's magic box tells her the following three encryption/decryption pairs for  $N$ :

$$(70583995, 4911157), \quad (173111957, 7346999), \quad (180311381, 29597249).$$

Use this information to factor  $N$ .

- (d) Let  $N = 1291233941$ . Eve's magic box tells her the following three encryption/decryption pairs for  $N$ :

$$(1103927639, 76923209), \quad (1022313977, 106791263), \quad (387632407, 7764043).$$

Use this information to factor  $N$ .

**Solution to Exercise 3.9.**

Let  $e_1, e_2, \dots, e_n$  be a bunch of random encryption exponents, and suppose that Eve uses her magic box to create decryption exponents  $d_1, d_2, \dots, d_n$ . The numbers  $K$  with the property that  $a^K \equiv a \pmod{N}$  for all  $a$  satisfying  $\gcd(a, N) = 1$  are numbers satisfying

$$K \equiv 1 \left( \text{mod} \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} \right).$$

Thus  $d_i e_i - 1$  is a multiple of  $(p-1)(q-1)/\gcd(p-1, q-1)$  for all  $1 \leq i \leq n$ . Assuming that the  $e_i$ 's are reasonably random, Eve will find that

$$T = \gcd(d_1 e_1 - 1, d_2 e_2 - 1, d_3 e_3 - 1, \dots, d_n e_n - 1) \quad (3.1)$$

is equal to a small multiple of

$$\frac{(p-1)(q-1)}{\gcd(p-1, q-1)}.$$

Next Eve uses the fact that  $\gcd(p-1, q-1)$  is even and tends to be fairly small. So she first assumes that  $T = (p-1)(q-1)/2$  and uses this to compute  $R = N+1 - (p-1)(q-1) = N+1 - 2T$ . If she is right about the value of  $T$ , then  $R$  will equal  $p+q$ , and she can recover  $p$  and  $q$  by factoring  $x^2 - Tx + N$ . If this doesn't work, she repeats the process with  $R = N+1-3T$ ,  $R = N+1-4T$ , etc. Continuing in this fashion, she should recover  $p$  and  $q$  fairly quickly.

Eve can save a bit of time in finding the right multiple of  $T$ . The idea is that  $N+1 - kT$  should equal  $p+q$ , and in practice  $p$  and  $q$  will have more or less the same order of magnitude. So Eve wants  $N+1 - kT \approx 2\sqrt{N}$ , which means that she should take  $k \approx (N+1 - 2\sqrt{N})/T$ .

(b)

$$\begin{aligned} & \gcd(16784693 \cdot 10988423 - 1, 11514115 \cdot 25910155 - 1) \\ &= \gcd(184437306609138, 298332504337824) \\ &= 19368558 \end{aligned}$$

First Eve tries  $N+1 - 1 \cdot \gcd = 19381152$ , but  $x^2 - 19381152x + 38749709$  is irreducible. Next she tries  $N+1 - 2 \cdot \gcd = 12594$ , and this time she finds that  $x^2 - 12594x + 38749709 = (x - 7247)(x - 5347)$ . Hence  $N = 38749709 = 7247 \cdot 5347$ .

(c)

$$\begin{aligned} & \gcd(4911157 \cdot 70583995 - 1, 7346999 \cdot 173111957 - 1, \\ & \quad 29597249 \cdot 180311381 - 1) \\ &= \gcd(346649081132214, 1271853374967042, 5336720840990868) \\ &= 37498566 \end{aligned}$$

Eve computes  $(\sqrt{225022969} - 1)^2 / 37498566 \approx 6.00004193$ , which suggests that she should try  $N+1 - 6 \cdot \gcd = 31574$ . This gives

$$x^2 - 31574x + 225022969 = (x - 20707)(x - 10867).$$

Hence  $N = 225022969 = 20707 \cdot 10867$ .

(d)

$$\begin{aligned} & \gcd(76923209 \cdot 1103927639 - 1, 106791263 \cdot 1022313977 - 1, \\ & \quad 7764043 \cdot 387632407 - 1) \\ &= \gcd(84917656495673550, 109174200786382950, 3009594676141500) \\ &= 129112350 \end{aligned}$$

Eve computes  $(\sqrt{1291233941} - 1)^2 / 129112350 \approx 10.0002987$ , which suggests that she should use  $N + 1 - 10 \cdot \gcd = 110442$ . This yields

$$x^2 - 110442x + 1291233941 = (x - 97151)(x - 13291).$$

Hence  $N = 1291233941 = 97151 \cdot 13291$ .

**3.10.** Here is an example of a public key system that was proposed at a cryptography conference. It is supposed to be faster and more efficient than RSA.

Alice chooses two large primes  $p$  and  $q$  and she publishes  $N = pq$ . It is assumed that  $N$  is hard to factor. Alice also chooses three random numbers  $g$ ,  $r_1$ , and  $r_2$  modulo  $N$  and computes

$$g_1 \equiv g^{r_1(p-1)} \pmod{N} \quad \text{and} \quad g_2 \equiv g^{r_2(q-1)} \pmod{N}.$$

Her public key is the triple  $(N, g_1, g_2)$  and her private key is the pair of primes  $(p, q)$ .

Now Bob wants to send the message  $m$  to Alice, where  $m$  is a number modulo  $N$ . He chooses two random integers  $s_1$  and  $s_2$  modulo  $N$  and computes

$$c_1 \equiv mg_1^{s_1} \pmod{N} \quad \text{and} \quad c_2 \equiv mg_2^{s_2} \pmod{N}.$$

Bob sends the ciphertext  $(c_1, c_2)$  to Alice.

Decryption is extremely fast and easy. Alice use the Chinese remainder theorem to solve the pair of congruences

$$x \equiv c_1 \pmod{p} \quad \text{and} \quad x \equiv c_2 \pmod{q}.$$

- Prove that Alice's solution  $x$  is equal to Bob's plaintext  $m$ .
- Explain why this cryptosystem is not secure.

Solution to Exercise 3.10.

- Notice that

$$c_1 \equiv mg_1^{s_1} \equiv mg^{s_1 r_1(p-1)} \equiv m \pmod{p}$$

by Fermat's little theorem, and similarly  $c_2 \equiv m \pmod{q}$ . Hence Alice's solutions satisfies  $x \equiv m \pmod{pq}$ .

- As in (a), we observe that  $g_1 \equiv 1 \pmod{p}$  from Fermat's little theorem. On the other hand, most likely  $g_1 \not\equiv 1 \pmod{q}$ . So Eve can recover  $p$  from the trivial gcd computation

$$\gcd(g_1 - 1, N) = p.$$

(If, by some rare coincidence,  $g_1 \equiv 1 \pmod{q}$ , then  $c_1 \equiv m \pmod{N}$ , so although Eve cannot factor  $N$ , she can read Bob's message.)

Section. Implementation and security issues

**3.11.** Formulate a man-in-the-middle attack, similar to the attack described in Example 3.12 on page 122, for the following public key cryptosystems.

- (a) The ElGamal public key cryptosystem (Table 2.3 on page 70).
- (b) The RSA public key cryptosystem (Table 3.1 on page 119).

Solution to Exercise 3.11.

*A solution for this exercise is not currently available.*

**3.12.** Alice decides to use RSA with the public key  $N = 1889570071$ . In order to guard against transmission errors, Alice has Bob encrypt his message twice, once using the encryption exponent  $e_1 = 1021763679$  and once using the encryption exponent  $e_2 = 519424709$ . Eve intercepts the two encrypted messages

$$c_1 = 1244183534 \quad \text{and} \quad c_2 = 732959706.$$

Assuming that Eve also knows  $N$  and the two encryption exponents  $e_1$  and  $e_2$ , use the method described in Example 3.14 to help Eve recover Bob's plaintext without finding a factorization of  $N$ .

Solution to Exercise 3.12.

With notation as in Example 3.14, we find that

$$u \cdot c_1 + v \cdot c_2 = 1$$

with

$$u = 252426389 \quad \text{and} \quad v = -496549570.$$

Then the plaintext is

$$m \equiv c_1^u \cdot c_2^v \equiv 1054592380 \pmod{N}.$$

### Section. Primality testing

**3.13.** We stated that the number 561 is a Carmichael number, but we never checked that  $a^{561} \equiv a \pmod{561}$  for every value of  $a$ .

- (a) The number 561 factors as  $3 \cdot 11 \cdot 17$ . First use Fermat's little theorem to prove that

$$a^{561} \equiv a \pmod{3}, \quad a^{561} \equiv a \pmod{11}, \quad \text{and} \quad a^{561} \equiv a \pmod{17}$$

for every value of  $a$ . Then explain why these three congruences imply that  $a^{561} \equiv a \pmod{561}$  for every value of  $a$ .

- (b) Mimic the idea used in (a) to prove that each of the following numbers is a Carmichael number. (To assist you, we have factored each number into primes.)

- (i)  $1729 = 7 \cdot 13 \cdot 19$

- (ii)  $10585 = 5 \cdot 29 \cdot 73$

- (iii)  $75361 = 11 \cdot 13 \cdot 17 \cdot 31$
- (iv)  $1024651 = 19 \cdot 199 \cdot 271$
- (c) Prove that a Carmichael number must be odd.
- (d) Prove that a Carmichael number must be a product of *distinct* primes.
- (e) Look up Korselt's criterion in a book or online, write a brief description of how it works, and use it to show that  $29341 = 13 \cdot 37 \cdot 61$  and  $172947529 = 307 \cdot 613 \cdot 919$  are Carmichael numbers.

Solution to Exercise 3.13.

*A solution for this exercise is not currently available.*

Here is a list of all Carmichael up to 100000, plus a few others.

- $561 = 3 \cdot 11 \cdot 17$
- $1105 = 5 \cdot 13 \cdot 17$
- $1729 = 7 \cdot 13 \cdot 19$
- $2465 = 5 \cdot 17 \cdot 29$
- $2821 = 7 \cdot 13 \cdot 31$
- $6601 = 7 \cdot 23 \cdot 41$
- $8911 = 7 \cdot 19 \cdot 67$
- $10585 = 5 \cdot 29 \cdot 73$
- $15841 = 7 \cdot 31 \cdot 73$
- $29341 = 13 \cdot 37 \cdot 61$
- $41041 = 7 \cdot 11 \cdot 13 \cdot 41$
- $46657 = 13 \cdot 37 \cdot 97$
- $52633 = 7 \cdot 73 \cdot 103$
- $62745 = 3 \cdot 5 \cdot 47 \cdot 89$
- $63973 = 7 \cdot 13 \cdot 19 \cdot 37$
- $75361 = 11 \cdot 13 \cdot 17 \cdot 31$
- $294409 = 37 \cdot 73 \cdot 109$
- $56052361 = 211 \cdot 421 \cdot 631$
- $118901521 = 271 \cdot 541 \cdot 811$
- $172947529 = 307 \cdot 613 \cdot 919$

$$\bullet \quad 1024651 = 19 \cdot 199 \cdot 271$$

**3.14.** Use the Miller–Rabin test on each of the following numbers. In each case, either provide a Miller–Rabin witness for the compositeness of  $n$ , or conclude that  $n$  is probably prime by providing 10 numbers that are not Miller–Rabin witnesses for  $n$ .

- (a)  $n = 1105$ . (Yes, 5 divides  $n$ , but this is just a warm-up exercise!)  
 (b)  $n = 294409$  (c)  $n = 294409$   
 (d)  $n = 118901509$  (e)  $n = 118901521$   
 (f)  $n = 118901527$  (g)  $n = 118915387$

Solution to Exercise 3.14.

(a)  $n - 1 = 1104 = 2^4 \cdot 69$ .

$$\begin{aligned} 2^{69} &\equiv -138 \pmod{1105} \\ 2^{2 \cdot 69} &\equiv 259 \pmod{1105} \\ 2^{4 \cdot 69} &\equiv -324 \pmod{1105} \\ 2^{8 \cdot 69} &\equiv 1 \pmod{1105} \end{aligned}$$

Thus 1105 is composite. It factors as  $n = 5 \cdot 13 \cdot 17$ .

(b)  $n - 1 = 294408 = 2^3 \cdot 36801$ .

$$\begin{aligned} 2^{36801} &\equiv 512 \pmod{294409} \\ 2^{2 \cdot 36801} &\equiv -32265 \pmod{294409} \\ 2^{4 \cdot 36801} &\equiv 1 \pmod{294409} \end{aligned}$$

Thus 294409 is composite. It factors as  $n = 37 \cdot 73 \cdot 109$ .

(c)  $n - 1 = 294438 = 2^1 \cdot 147219$ .

$$\begin{aligned} 2^{147219} &\equiv 1 \pmod{294439} \\ 3^{147219} &\equiv -1 \pmod{294439} \\ 5^{147219} &\equiv 1 \pmod{294439} \end{aligned}$$

Thus 2, 3, 5 are not Miller–Rabin witnesses for 294439. It turns out that 294439 is prime.

(d)  $n - 1 = 118901508 = 2^2 \cdot 29725377$ .



$$\begin{aligned}
2^{29725377} &\equiv 7906806 \pmod{118901509} \\
2^{2 \cdot 29725377} &\equiv -1 \pmod{118901509} \\
3^{29725377} &\equiv -1 \pmod{118901509} \\
3^{2 \cdot 29725377} &\equiv 1 \pmod{118901509} \\
5^{29725377} &\equiv -1 \pmod{118901509} \\
5^{2 \cdot 29725377} &\equiv 1 \pmod{118901509} \\
7^{29725377} &\equiv 7906806 \pmod{118901509} \\
7^{2 \cdot 29725377} &\equiv -1 \pmod{118901509} \\
11^{29725377} &\equiv -1 \pmod{118901509} \\
11^{2 \cdot 29725377} &\equiv 1 \pmod{118901509}
\end{aligned}$$

Thus 2, 3, 5, 7, and 11 are not Miller–Rabin witnesses for 118901509. It turns out that 118901509 is prime.

(e)  $n - 1 = 118901520 = 2^4 \cdot 7431345$

$$\begin{aligned}
2^{7431345} &\equiv 45274074 \pmod{118901521} \\
2^{2 \cdot 7431345} &\equiv 1758249 \pmod{118901521} \\
2^{4 \cdot 7431345} &\equiv 1 \pmod{118901521} \\
2^{8 \cdot 7431345} &\equiv 1 \pmod{118901521}
\end{aligned}$$

Thus 118901521 is composite. It factors as  $118901521 = 271 \cdot 541 \cdot 811$ .

(f)  $n - 1 = 118901526 = 2^1 \cdot 59450763$ .

$$\begin{aligned}
2^{59450763} &\equiv 1 \pmod{118901527} \\
3^{59450763} &\equiv -1 \pmod{118901527} \\
5^{59450763} &\equiv -1 \pmod{118901527} \\
7^{59450763} &\equiv 1 \pmod{118901527} \\
11^{59450763} &\equiv 1 \pmod{118901527}
\end{aligned}$$

Thus 2, 3, 5, 7, and 11 are not Miller–Rabin witnesses for 118901527. It turns out that 118901527 is prime.

(g)  $n - 1 = 118915386 = 2^1 \cdot 59457693$ .

$$2^{59457693} \equiv -5081012 \pmod{118915387}$$

Thus 118915387 is composite. It factors as  $n = 6571 \cdot 18097$ .

**3.15.** Looking back at Exercise 3.9, let's suppose that for a given  $N$ , the magic box can produce only one decryption exponent. Equivalently, suppose that an RSA key pair has been compromised and that the private decryption exponent corresponding to the public encryption exponent has been discovered. Show how the basic idea in the Miller–Rabin primality test can be applied to use this information to factor  $N$ .

Solution to Exercise 3.15.

We are given an encryption/decryption pair  $(e, d)$ , which means that

$$a^{de} \equiv a \pmod{N} \quad \text{for all } 1 \leq a < N.$$

So for most values of  $a$  we have  $a^{de-1} \equiv 1 \pmod{N}$ . (This is true unless  $\gcd(a, N) > 1$ , in which case  $\gcd(a, N)$  is a nontrivial factor of  $N$ .) Using the idea of the Miller–Rabin test, we factor

$$de = 2^k r \quad \text{with } r \text{ odd.}$$

Then for random choices of  $a$ , we look at

$$a^r, a^{2r}, a^{4r}, \dots, a^{2^k r} \pmod{N}.$$

We know that the last entry in the list is 1.

Now suppose that  $N$  factors as  $pq$ , where we do not know  $p$  and  $q$ . We choose a value for  $a$ . The Miller–Rabin test applied to  $p$  tells us that either

$$a^r \equiv 1 \pmod{p}, \quad \text{or else} \quad a^{2^i r} \equiv -1 \pmod{p} \quad \text{for some } 0 \leq i < k.$$

(If the latter is true, we take  $i$  to be the smallest such value.) Note that we do not know the value of  $i$ , because we do not know the value of  $p$ , but that's okay. Next we do the same thing with  $q$ . Thus the Miller–Rabin test tells us that either

$$a^r \equiv 1 \pmod{q}, \quad \text{or else} \quad a^{2^j r} \equiv -1 \pmod{q} \quad \text{for some } 0 \leq j < k,$$

where again we choose the smallest such  $j$ .

We now consider several cases. If  $a^r \equiv 1 \pmod{p}$  and  $a^r \not\equiv 1 \pmod{q}$ , then we recover  $p$  by computing

$$\gcd(N, a^r - 1) = p.$$

Similarly, if  $a^r \not\equiv 1 \pmod{p}$  and  $a^r \equiv 1 \pmod{q}$ , then  $\gcd(N, a^r - 1) = q$ , so again we win. On the other hand, if  $a^r \equiv 1 \pmod{N}$ , then we get no useful information, so we need to go try a different value for  $a$ .

In the remaining cases we have  $a^r \not\equiv 1 \pmod{p}$  and  $a^r \not\equiv 1 \pmod{q}$ . Suppose that  $i$  and  $j$  are different, say  $i < j$ . Then

$$a^{2^i r} \equiv -1 \pmod{p} \quad \text{and} \quad a^{2^i r} \not\equiv -1 \pmod{q},$$

So computing  $\gcd(N, a^{2^i r} + 1) = p$  recovers  $p$ . A similar method works if  $j < i$ . And finally, if  $i = j$ , then we get no useful information and need to try a different value for  $a$ .

We can summarize the above solution as the following algorithm:

1. Choose a random value  $1 < a < N$ .

2. Compute  $\gcd(a, N)$ . If it is not equal to 1, then it is a nontrivial factor of  $N$ .
  3. Let  $(e, d)$  be the encryption/decryption pair. Factor  $de - 1 = 2^k r$  with  $r$  odd.
  4. Compute  $\gcd(N, a^r - 1)$ . If it is a nontrivial factor of  $N$ , you're done.
  5. For each  $0 \leq i < k$ , compute  $\gcd(N, a^{2^i r} + 1)$ . If it is a nontrivial factor of  $N$ , you're done.
  6. If you haven't found a factor of  $N$ , go back to Step 1 and choose a new value of  $a$ .
- 3.16.** The function  $\pi(X)$  counts the number of primes between 2 and  $X$ .
- (a) Compute the values of  $\pi(20)$ ,  $\pi(30)$ , and  $\pi(100)$ .
  - (b) Write a program to compute  $\pi(X)$  and use it to compute  $\pi(X)$  and the ratio  $\pi(X)/(X/\ln(X))$  for  $X = 100$ ,  $X = 1000$ ,  $X = 10000$ , and  $X = 100000$ . Does your list of ratios make the prime number theorem plausible?

*Solution to Exercise 3.16.*

$X$	$\pi(X)$	$\pi(X)/(X/\ln(X))$
10	4	0.921
20	8	1.198
30	10	1.134
100	25	1.151
1000	168	1.161
10000	1229	1.132
100000	9592	1.104
1000000	78498	1.084

**3.17.** Let

$$\pi_1(X) = (\# \text{ of primes } p \text{ between 2 and } X \text{ satisfying } p \equiv 1 \pmod{4}),$$

$$\pi_3(X) = (\# \text{ of primes } p \text{ between 2 and } X \text{ satisfying } p \equiv 3 \pmod{4}).$$

Thus every prime other than 2 gets counted by either  $\pi_1(X)$  or by  $\pi_3(X)$ .

- (a) Compute the values of  $\pi_1(X)$  and  $\pi_3(X)$  for each of the following values of  $X$ . (i)  $X = 10$ . (ii)  $X = 25$ . (iii)  $X = 100$ .
- (b) Write a program to compute  $\pi_1(X)$  and  $\pi_3(X)$  and use it to compute their values and the ratio  $\pi_3(X)/\pi_1(X)$  for  $X = 100$ ,  $X = 1000$ ,  $X = 10000$ , and  $X = 100000$ .
- (c) Based on your data from (b), make a conjecture about the relative sizes of  $\pi_1(X)$  and  $\pi_3(X)$ . Which one do you think is larger? What do you think is the limit of the ratio  $\pi_3(X)/\pi_1(X)$  as  $X \rightarrow \infty$ ?

*Solution to Exercise 3.17.*

$X$	$\pi_1(X)$	$\pi_3(X)$	$\pi_3(X)/\pi_1(X)$
10	1	2	2.0000
25	3	5	1.6667
100	11	13	1.1818
1000	80	87	1.0875
10000	609	619	1.0164
100000	4783	4808	1.0052
1000000	39175	39322	1.0038

(c) From the data, it appears that  $\pi_3(X) > \pi_1(X)$  for all  $X$ . This is actually false, but the first  $X$  for which the inequality is reversed is extremely large. In any case, the ratio satisfies  $\lim_{X \rightarrow \infty} \pi_3(X)/\pi_1(X) = 1$ . This is a special case of Dirichlet's theorem on primes in arithmetic progressions, which says the following. Let  $\gcd(a, N) = 1$  and let  $\pi_{a,N}(X)$  be the number of primes  $p$  between 2 and  $X$  satisfying  $p \equiv a \pmod{N}$ . Then  $\lim_{X \rightarrow \infty} \pi_{a,N}(X)/\pi(X) = 1/\phi(N)$ .

**3.18.** We noted in Section 3.4 that it really makes no sense to say that the number  $n$  has probability  $1/\ln(n)$  of being prime. Any particular number that you choose either will be prime or will not be prime; there are no numbers that are 35% prime and 65% composite! In this exercise you will prove a result that gives a more sensible meaning to the statement that a number has a certain probability of being prime. You may use the prime number theorem (Theorem 3.20) for this problem.

- (a) Fix a (large) number  $N$  and suppose that Bob chooses a random number  $n$  in the interval  $\frac{1}{2}N \leq n \leq \frac{3}{2}N$ . If he repeats this process many times, prove that approximately  $1/\ln(N)$  of his numbers will be prime. More precisely, define

$$P(N) = \frac{\text{number of primes between } \frac{1}{2}N \text{ and } \frac{3}{2}N}{\text{number of integers between } \frac{1}{2}N \text{ and } \frac{3}{2}N} = \left[ \begin{array}{l} \text{Probability that an integer } n \text{ in the} \\ \text{interval } \frac{1}{2}N \leq n \leq \frac{3}{2}N \text{ is a prime num-} \\ \text{ber} \end{array} \right],$$

and prove that

$$\lim_{N \rightarrow \infty} \frac{P(N)}{1/\ln(N)} = 1.$$

This shows that if  $N$  is large, then  $P(N)$  is approximately  $1/\ln(N)$ .

- (b) More generally, fix two numbers  $c_1$  and  $c_2$  satisfying  $c_1 < c_2$ . Bob chooses random numbers  $n$  in the interval  $c_1N \leq n \leq c_2N$ . Keeping  $c_1$  and  $c_2$  fixed, let

$$P(c_1, c_2; N) = \left[ \begin{array}{l} \text{Probability that an integer } n \text{ in the in-} \\ \text{terval } c_1N \leq n \leq c_2N \text{ is a prime num-} \\ \text{ber} \end{array} \right].$$

In the following formula, fill in the box with a simple function of  $N$  so that the statement is true:

$$\lim_{N \rightarrow \infty} \frac{P(c_1, c_2; N)}{\boxed{\phantom{000}}} = 1.$$

*Solution to Exercise 3.18.*

We will just write  $P(N)$ , instead of  $P(c_1, c_2; N)$ .

$$\begin{aligned} P(N) &= \frac{\# \text{ of primes between } c_1 N \text{ and } c_2 N}{N} \\ &= \frac{\pi(c_2 N) - \pi(c_1 N)}{N} \\ &= \frac{c_2}{\ln(c_2 N)} - \frac{c_1}{\ln(c_1 N)} + o\left(\frac{1}{\ln(N)}\right) \quad \text{from the prime number theorem} \\ &= \frac{(c_2 - c_1) \ln(N) + O(1)}{\ln(c_1 N) \ln(c_2 N)} + o\left(\frac{1}{\ln(N)}\right) \\ &= \frac{c_2 - c_1}{\ln(N)} + o\left(\frac{1}{\ln(N)}\right) \end{aligned}$$

Hence  $P(N)$  divided by  $(c_2 - c_1)/\ln(N)$  goes to 1 as  $N \rightarrow \infty$ , or equivalently,

$$\lim_{N \rightarrow \infty} \frac{P(N)}{\ln(N)} = c_2 - c_1.$$

For part (a), we have  $c_1 = \frac{1}{2}$  and  $c_2 = \frac{3}{2}$ , so the limit is 1.

**3.19.** Continuing with the previous exercise, explain how to make mathematical sense of the following statements.

- (a) A randomly chosen *odd* number  $N$  has probability  $2/\ln(N)$  of being prime. (What is the probability that a randomly chosen even number is prime?)
- (b) A randomly chosen number  $N$  satisfying  $N \equiv 1 \pmod{3}$  has probability  $3/(2 \ln(N))$  of being prime.
- (c) A randomly chosen number  $N$  satisfying  $N \equiv 1 \pmod{6}$  has probability  $3/\ln(N)$  of being prime.
- (d) Let  $m = p_1 p_2 \cdots p_r$  be a product of distinct primes and let  $k$  be a number satisfying  $\gcd(k, m) = 1$ . What number should go into the box to make statement (3.35) correct? Why?

$$\begin{array}{l} \text{A randomly chosen number } N \text{ satisfying} \\ N \equiv k \pmod{m} \quad \text{has} \quad \text{probabil-} \quad (3.2) \\ \text{ity } \boxed{\phantom{000}} / \ln(N) \text{ of being prime.} \end{array}$$

- (e) Same question, but for arbitrary  $m$ , not just for  $m$  that are products of distinct primes.

Solution to Exercise 3.19.

(a,b,c) A solution for this exercise is not currently available.

(d) If  $m = p_1 \cdots p_r$ , then the probability that  $N \equiv k \pmod{m}$  is prime is approximately

$$\prod_{i=1}^r \left( \frac{p_i}{p_i - 1} \right) \cdot \frac{1}{\ln(N)}.$$

(e) More generally, for arbitrary  $m$  and  $k$  satisfying  $\gcd(m, k) = 1$ , the probability that  $N \equiv k \pmod{m}$  is prime is approximately

$$\prod_{p|m} \left( \frac{p}{p-1} \right) \cdot \frac{1}{\ln(N)}.$$

This is often written as

$$\prod_{p|m} \left( 1 - \frac{1}{p} \right)^{-1} \cdot \frac{1}{\ln(N)},$$

which is also equal to  $N/(\phi(N) \ln(N))$ , where  $\phi(N)$  is Euler's phi function.

**3.20.** The *logarithmic integral function*  $\text{Li}(X)$  is defined to be

$$\text{Li}(X) = \int_2^X \frac{dt}{\ln t}.$$

(a) Prove that

$$\text{Li}(X) = \frac{X}{\ln X} + \int_2^X \frac{dt}{(\ln t)^2} + O(1).$$

(Hint. Integration by parts.)

(b) Compute the limit

$$\lim_{X \rightarrow \infty} \frac{\text{Li}(X)}{X/\ln X}.$$

(Hint. Break the integral in (a) into two pieces,  $2 \leq t \leq \sqrt{X}$  and  $\sqrt{X} \leq t \leq X$ , and estimate each piece separately.)

(c) Use (b) to show that formula (3.12) on page 131 implies the prime number theorem (Theorem 3.20).

Solution to Exercise 3.20.

A solution for this exercise is not currently available.

Section. Pollard's  $p-1$  factorization algorithm

**3.21.** Use Pollard's  $p-1$  method to factor each of the following numbers.

(a)  $n = 1739$       (b)  $n = 220459$       (c)  $n = 48356747$

Be sure to show your work and to indicate which prime factor  $p$  of  $n$  has the property that  $p - 1$  is a product of small primes.

Solution to Exercise 3.21.

(a)

$$\begin{array}{lll} 2^{3!} - 1 \equiv 63 & (\text{mod } 1739) & \gcd(2^{3!} - 1, 1739) = 1 \\ 2^{4!} - 1 \equiv 1082 & (\text{mod } 1739) & \gcd(2^{4!} - 1, 1739) = 1 \\ 2^{5!} - 1 \equiv 1394 & (\text{mod } 1739) & \gcd(2^{5!} - 1, 1739) = 1 \\ 2^{6!} - 1 \equiv 1443 & (\text{mod } 1739) & \gcd(2^{6!} - 1, 1739) = 37 \end{array}$$

This gives  $1739 = 37 \cdot 47$ . Note that  $p - 1 = 36 = 2^2 \cdot 3^2$  and  $q - 1 = 46 = 2 \cdot 23$ .

(b)

$$\begin{array}{lll} 2^{3!} - 1 \equiv 63 & (\text{mod } 220459) & \gcd(2^{3!} - 1, 220459) = 1 \\ 2^{4!} - 1 \equiv 22331 & (\text{mod } 220459) & \gcd(2^{4!} - 1, 220459) = 1 \\ 2^{5!} - 1 \equiv 85053 & (\text{mod } 220459) & \gcd(2^{5!} - 1, 220459) = 1 \\ 2^{6!} - 1 \equiv 4045 & (\text{mod } 220459) & \gcd(2^{6!} - 1, 220459) = 1 \\ 2^{7!} - 1 \equiv 43102 & (\text{mod } 220459) & \gcd(2^{7!} - 1, 220459) = 1 \\ 2^{8!} - 1 \equiv 179600 & (\text{mod } 220459) & \gcd(2^{8!} - 1, 220459) = 449 \end{array}$$

This gives  $220459 = 449 \cdot 491$ . Note that  $p - 1 = 448 = 2^6 \cdot 7$  and  $q - 1 = 490 = 2 \cdot 5 \cdot 7^2$ .

(c)

$$\begin{array}{lll} 2^{15!} - 1 \equiv 46983890 & (\text{mod } 48356747) & \gcd(2^{15!} - 1, 48356747) = 1 \\ 2^{16!} - 1 \equiv 8398520 & (\text{mod } 48356747) & \gcd(2^{16!} - 1, 48356747) = 1 \\ 2^{17!} - 1 \equiv 9367159 & (\text{mod } 48356747) & \gcd(2^{17!} - 1, 48356747) = 1 \\ 2^{18!} - 1 \equiv 17907955 & (\text{mod } 48356747) & \gcd(2^{18!} - 1, 48356747) = 1 \\ 2^{19!} - 1 \equiv 13944672 & (\text{mod } 48356747) & \gcd(2^{19!} - 1, 48356747) = 6917 \end{array}$$

This gives  $48356747 = 6917 \cdot 6991$ . Note that  $p - 1 = 6916 = 2^2 \cdot 7 \cdot 13 \cdot 19$  and  $q - 1 = 6990 = 2 \cdot 3 \cdot 5 \cdot 233$ .

**3.22.** A prime of the form  $2^n - 1$  is called a *Mersenne prime*.

- Factor each of the numbers  $2^n - 1$  for  $n = 2, 3, \dots, 10$ . Which ones are Mersenne primes?
- Find the first seven Mersenne primes. (You may need a computer.)
- If  $n$  is even and  $n > 2$ , prove that  $2^n - 1$  is not prime.
- If  $3 \mid n$  and  $n > 3$ , prove that  $2^n - 1$  is not prime.
- More generally, prove that if  $n$  is a composite number, then  $2^n - 1$  is not prime. Thus all Mersenne primes have the form  $2^p - 1$  with  $p$  a prime number.

- (f) What is the largest known Mersenne prime? Are there any larger primes known? (You can find out at the “Great Internet Mersenne Prime Search” web site [www.mersenne.org/prime.htm](http://www.mersenne.org/prime.htm).)
- (g) Write a one page essay on Mersenne primes, starting with the discoveries of Father Mersenne and ending with GIMPS.

Solution to Exercise 3.22.

The factorization of  $2^n - 1$  for  $2 \leq n \leq 20$  is

	$2^{11} - 1 = 2047 = 23 \cdot 89$
$2^2 - 1 = 3 = 3$	$2^{12} - 1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$
$2^3 - 1 = 7 = 7$	$2^{13} - 1 = 8191 = 8191$
$2^4 - 1 = 15 = 3 \cdot 5$	$2^{14} - 1 = 16383 = 3 \cdot 43 \cdot 127$
$2^5 - 1 = 31 = 31$	$2^{15} - 1 = 32767 = 7 \cdot 31 \cdot 151$
$2^6 - 1 = 63 = 3^2 \cdot 7$	$2^{16} - 1 = 65535 = 3 \cdot 5 \cdot 17 \cdot 257$
$2^7 - 1 = 127 = 127$	$2^{17} - 1 = 131071 = 131071$
$2^8 - 1 = 255 = 3 \cdot 5 \cdot 17$	$2^{18} - 1 = 262143 = 3^3 \cdot 7 \cdot 19 \cdot 73$
$2^9 - 1 = 511 = 7 \cdot 73$	$2^{19} - 1 = 524287 = 524287$
$2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31$	$2^{20} - 1 = 1048575 = 3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41$

Thus the first few Mersenne primes are

$$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 31, \quad 2^7 - 1 = 127, \\ 2^{13} - 1 = 8191, \quad 2^{17} - 1 = 131071, \quad 2^{19} - 1 = 524287.$$

Notice that  $2^p - 1$  is prime for all primes  $p < 20$  except for  $p = 11$ . However, this is somewhat misleading. For the primes  $20 < p < 40$ , only  $2^{31} - 1$  yields a Mersenne prime.

$$2^{23} - 1 = 8388607 = 47 \cdot 178481 \\ 2^{29} - 1 = 536870911 = 233 \cdot 1103 \cdot 2089 \\ 2^{31} - 1 = 2147483647 = 2147483647 \\ 2^{37} - 1 = 137438953471 = 223 \cdot 616318177 \\ 2^{41} - 1 = 2199023255551 = 13367 \cdot 164511353 \\ 2^{43} - 1 = 8796093022207 = 431 \cdot 9719 \cdot 2099863 \\ 2^{47} - 1 = 140737488355327 = 2351 \cdot 4513 \cdot 13264529$$

- (c) If  $n$  is even, say  $n = 2m$ , then  $2^n - 1 = 2^{2m} - 1 = (2^m - 1)(2^m + 1)$ , so  $2^n - 1$  is composite unless  $2^m - 1 = 1$ , i.e. unless  $m = 1$  and  $n = 2$ .



(d) Similarly,  $2^{3m} - 1 = (2^m - 1)(2^{2m} + 2^m + 1)$ , so it is composite unless  $m = 1$ .

(e) More generally,

$$2^{km} - 1 = (2^m - 1)(2^{(k-1)m} + 2^{(k-2)m} + \cdots + 2^{2m} + 2^m + 1),$$

so  $2^{km} - 1$  is composite unless  $m = 1$  or  $k = 1$ . Notice that what we are really doing is using the standard identity

$$x^k - 1 = (x - 1)(x^{(k-1)} + x^{(k-2)} + \cdots + x^2 + x + 1)$$

with  $x = 2^m$ .

(f) As of January 2008, the largest known Mersenne prime is  $2^{32582657} - 1$ , which was discovered in September 2006 as part of the GIMPS project.

## Section. Factorization via difference of squares

**3.23.** For each of the following numbers  $N$ , compute the values of

$$N + 1^2, \quad N + 2^2, \quad N + 3^2, \quad N + 4^2, \quad \dots$$

as we did in **Example 3.33** until you find a value  $N + b^2$  that is a perfect square  $a^2$ . Then use the values of  $a$  and  $b$  to factor  $N$ .

- (a)  $N = 53357$       (b)  $N = 34571$       (c)  $N = 25777$       (d)  $N = 64213$

Solution to Exercise 3.23.

(a)

$$\begin{aligned} 53357 + 1^2 &= 53358 && \text{not a square,} \\ 53357 + 2^2 &= 53361 = 231^2 && \text{** square **} \end{aligned}$$

Thus

$$53357 = 231^2 - 2^2 = (231 + 2)(231 - 2) = 233 \cdot 229.$$

(b)

$$\begin{aligned} 34571 + 1^2 &= 34572 && \text{not a square,} \\ 34571 + 2^2 &= 34575 && \text{not a square,} \\ 34571 + 3^2 &= 34580 && \text{not a square,} \\ 34571 + 4^2 &= 34587 && \text{not a square,} \\ 34571 + 5^2 &= 34596 = 186^2 && \text{** square **} \end{aligned}$$

Thus

$$34571 = 186^2 - 5^2 = (186 + 5)(186 - 5) = 191 \cdot 181.$$

(c)

$$\begin{aligned} 25777 + 1^2 &= 25778 && \text{not a square} \\ 25777 + 2^2 &= 25781 && \text{not a square} \\ 25777 + 3^2 &= 25786 && \text{not a square} \\ 25777 + 4^2 &= 25793 && \text{not a square} \\ 25777 + 5^2 &= 25802 && \text{not a square} \\ 25777 + 6^2 &= 25813 && \text{not a square} \\ 25777 + 7^2 &= 25826 && \text{not a square} \\ 25777 + 8^2 &= 25841 && \text{not a square} \\ 25777 + 9^2 &= 25858 && \text{not a square} \\ 25777 + 10^2 &= 25877 && \text{not a square} \\ 25777 + 11^2 &= 25898 && \text{not a square} \\ 25777 + 12^2 &= 25921 = 161^2 && \text{** square **} \end{aligned}$$

Thus

$$25777 = 161^2 - 12^2 = (161 + 12)(161 - 12) = 173 \cdot 149.$$

(d) Most people will give up before finishing this one unless they write a computer program! It is included to make people aware that this method doesn't always work.

$64213 + 1^2 = 64214$	not a square
$64213 + 2^2 = 64217$	not a square
$64213 + 3^2 = 64222$	not a square
$64213 + 4^2 = 64229$	not a square
$\vdots$	$\vdots$
$64213 + 121^2 = 78854$	not a square
$64213 + 122^2 = 79097$	not a square
$64213 + 123^2 = 79342$	not a square
$64213 + 124^2 = 79589$	not a square
$64213 + 125^2 = 79838$	not a square
$64213 + 126^2 = 80089 = 283^2$	** square **

Thus

$$64213 = 283^2 - 126^2 = (283 + 126)(283 - 126) = 409 \cdot 157.$$

**3.24.** For each of the listed values of  $N$ ,  $k$ , and  $b_{\text{init}}$ , factor  $N$  by making a list of values of  $k \cdot N + b^2$ , starting at  $b = b_{\text{init}}$  and incrementing  $b$  until  $k \cdot N + b^2$  is a perfect square. Then take greatest common divisors as we did in Example 3.34.

(a)	$N = 143041$	$k = 247$	$b_{\text{init}} = 1$
(b)	$N = 1226987$	$k = 3$	$b_{\text{init}} = 36$
(c)	$N = 2510839$	$k = 21$	$b_{\text{init}} = 90$

Solution to Exercise 3.24.

(a)

$247 \cdot 143041 + 1^2 = 35331128$	not a square
$247 \cdot 143041 + 2^2 = 35331131$	not a square
$247 \cdot 143041 + 3^2 = 35331136 = 5944^2$	** square **

Thus

$$247 \cdot 143041 = 5944^2 - 3^2 = (5944 + 3)(5944 - 3) = 5947 \cdot 5941.$$

$$\gcd(143041, 5947) = 313, \quad \gcd(143041, 5941) = 457$$

(b)

$$\begin{array}{ll} 3 \cdot 1226987 + 36^2 = 3682257 & \text{not a square} \\ 3 \cdot 1226987 + 37^2 = 3682330 & \text{not a square} \\ 3 \cdot 1226987 + 38^2 = 3682405 & \text{not a square} \\ 3 \cdot 1226987 + 39^2 = 3682482 & \text{not a square} \\ 3 \cdot 1226987 + 40^2 = 3682561 = 1919^2 & \text{** square **} \end{array}$$

Thus

$$3 \cdot 1226987 = 1919^2 - 40^2 = (1919 + 40)(1919 - 40) = 1959 \cdot 1879.$$

$$\gcd(1226987, 1959) = 653, \quad \gcd(1226987, 1879) = 1879$$

(c)

$$\begin{array}{ll} 21 \cdot 2510839 + 90^2 = 52735719 & \text{not a square} \\ 21 \cdot 2510839 + 91^2 = 52735900 & \text{not a square} \\ 21 \cdot 2510839 + 92^2 = 52736083 & \text{not a square} \\ 21 \cdot 2510839 + 93^2 = 52736268 & \text{not a square} \\ 21 \cdot 2510839 + 94^2 = 52736455 & \text{not a square} \\ 21 \cdot 2510839 + 95^2 = 52736644 = 7262^2 & \text{** square **} \end{array}$$

Thus

$$21 \cdot 2510839 = 7262^2 - 95^2 = (7262 + 95)(7262 - 95) = 7357 \cdot 7167.$$

$$\gcd(2510839, 7357) = 1051, \quad \gcd(2510839, 7167) = 2389$$

**3.25.** For each part, use the data provided to find values of  $a$  and  $b$  satisfying  $a^2 \equiv b^2 \pmod{N}$ , and then compute  $\gcd(N, a - b)$  in order to find a nontrivial factor of  $N$ , as we did in Examples 3.36 and 3.37.

(a)  $N = 61063$ 

$$\begin{array}{llll} 1882^2 \equiv 270 & \pmod{61063} & \text{and} & 270 = 2 \cdot 3^3 \cdot 5 \\ 1898^2 \equiv 60750 & \pmod{61063} & \text{and} & 60750 = 2 \cdot 3^5 \cdot 5^3 \end{array}$$

(b)  $N = 52907$ 

$$\begin{array}{llll} 399^2 \equiv 480 & \pmod{52907} & \text{and} & 480 = 2^5 \cdot 3 \cdot 5 \\ 763^2 \equiv 192 & \pmod{52907} & \text{and} & 192 = 2^6 \cdot 3 \\ 773^2 \equiv 15552 & \pmod{52907} & \text{and} & 15552 = 2^6 \cdot 3^5 \\ 976^2 \equiv 250 & \pmod{52907} & \text{and} & 250 = 2 \cdot 5^3 \end{array}$$

(c)  $N = 198103$

$$\begin{array}{llll}
 1189^2 \equiv 27000 & (\text{mod } 198103) & \text{and} & 27000 = 2^3 \cdot 3^3 \cdot 5^3 \\
 1605^2 \equiv 686 & (\text{mod } 198103) & \text{and} & 686 = 2 \cdot 7^3 \\
 2378^2 \equiv 108000 & (\text{mod } 198103) & \text{and} & 108000 = 2^5 \cdot 3^3 \cdot 5^3 \\
 2815^2 \equiv 105 & (\text{mod } 198103) & \text{and} & 105 = 3 \cdot 5 \cdot 7
 \end{array}$$

(d)  $N = 2525891$

$$\begin{array}{llll}
 1591^2 \equiv 5390 & (\text{mod } 2525891) & \text{and} & 5390 = 2 \cdot 5 \cdot 7^2 \cdot 11 \\
 3182^2 \equiv 21560 & (\text{mod } 2525891) & \text{and} & 21560 = 2^3 \cdot 5 \cdot 7^2 \cdot 11 \\
 4773^2 \equiv 48510 & (\text{mod } 2525891) & \text{and} & 48510 = 2 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11 \\
 5275^2 \equiv 40824 & (\text{mod } 2525891) & \text{and} & 40824 = 2^3 \cdot 3^6 \cdot 7 \\
 5401^2 \equiv 1386000 & (\text{mod } 2525891) & \text{and} & 1386000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11
 \end{array}$$

Solution to Exercise 3.25.

(a)

$$\begin{aligned}
 1882^2 \cdot 1898^2 &\equiv (2 \cdot 3^3 \cdot 5)(2 \cdot 3^5 \cdot 5^3) \pmod{61063} \\
 &= (2 \cdot 3^4 \cdot 5^2)^2 \\
 &= 4050^2
 \end{aligned}$$

$$\gcd(61063, 1882 \cdot 1898 - 4050) = 227 \quad \text{Eureka!}$$

(b) The most natural combination to try first is

$$\begin{aligned}
 763^2 \cdot 773^2 &\equiv (2^6 \cdot 3)(2^6 \cdot 3^5) \pmod{52907} \\
 &= (2^6 \cdot 3^3)^2 \\
 &= 1728^2
 \end{aligned}$$

$$\gcd(52907, 763 \cdot 773 - 1728) = 277 \quad \text{Eureka!}$$

So this works. However, if instead we use

$$\begin{aligned}
 399^2 \cdot 763^2 \cdot 976^2 &\equiv (2^5 \cdot 3 \cdot 5)(2^6 \cdot 3)(2 \cdot 5^3) \pmod{52907} \\
 &= (2^6 \cdot 3 \cdot 5^2)^2 \\
 &= 4800^2,
 \end{aligned}$$

then we do not win, since

$$\gcd(52907, 399 \cdot 763 \cdot 976 - 4800) = 52907 \quad \text{No help}$$

(c) First we try



Solution to Exercise 3.26.

- (a)  $\psi(25, 3) = 10$
- (b)  $\psi(35, 5) = 18$
- (c)  $\psi(50, 7) = 30$
- (d)  $\psi(100, 5) = 33$
- (e)  $\psi(100, 7) = 45$

**3.27.** An integer  $M$  is called *B-power-smooth* if every prime power  $p^e$  dividing  $M$  satisfies  $p^e \leq B$ . For example,  $180 = 2^2 \cdot 3^2 \cdot 5$  is 10-power-smooth, since the largest prime power dividing 180 is 9, which is smaller than 10.

- (a) Suppose that  $M$  is *B-power-smooth*. Prove that  $M$  is also *B-smooth*.
- (b) Suppose that  $M$  is *B-smooth*. Is it always true that  $M$  is also *B-power-smooth*? Either prove that it is true or give an example for which it is not true.
- (c) The following is a list of 20 randomly chosen numbers between 1 and 1000, sorted from smallest to largest. Which of these numbers are 10-power-smooth? Which of them are 10-smooth?

{84, 141, 171, 208, 224, 318, 325, 366, 378, 390, 420, 440,  
504, 530, 707, 726, 758, 765, 792, 817}

- (d) Prove that  $M$  is *B-power-smooth* if and only if  $M$  divides the least common multiple of  $[1, 2, \dots, B]$ . (The *least common multiple* of a list of numbers  $k_1, \dots, k_r$  is the smallest number  $K$  that is divisible by every number in the list.)

Solution to Exercise 3.27.

(a,b,d) *A solution for this exercise is not currently available.*

(c) The numbers  $84 = 2^2 \cdot 3 \cdot 7$ ,  $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$ ,  $504 = 2^3 \cdot 3^2 \cdot 7$ , and are 10-power-smooth. They are also 10-smooth, of course, as are the additional numbers  $224 = 2^5 \cdot 7$  and  $378 = 2 \cdot 3^3 \cdot 7$ .

**3.28.** Let  $L(N) = e^{\sqrt{(\ln N)(\ln \ln N)}}$  as usual. Suppose that a computer does one billion operations per second.

- (a) How many seconds does it take to perform  $L(2^{100})$  operations?
  - (b) How many hours does it take to perform  $L(2^{250})$  operations?
  - (c) How many days does it take to perform  $L(2^{350})$  operations?
  - (d) How many years does it take to perform  $L(2^{500})$  operations?
  - (e) How many years does it take to perform  $L(2^{750})$  operations?
  - (f) How many years does it take to perform  $L(2^{1000})$  operations?
  - (g) How many years does it take to perform  $L(2^{2000})$  operations?
- (For simplicity, you may assume that there are 365.25 days in a year.)

Solution to Exercise 3.28.

- (a)  $N = 2^{100} : L(N) = 2^{24.73}$  steps takes 0.03 seconds.
- (b)  $N = 2^{250} : L(N) = 2^{43.12}$  steps takes 2.65 hours.

- (c)  $N = 2^{350}$  :  $L(N) = 2^{52.66}$  steps takes 82.24 days.
- (d)  $N = 2^{500}$  :  $L(N) = 2^{64.95}$  steps takes 1129.30 years.
- (e)  $N = 2^{750}$  :  $L(N) = 2^{82.26}$  steps takes  $10^{8.26}$  years.
- (f)  $N = 2^{1000}$  :  $L(N) = 2^{97.14}$  steps takes  $10^{12.74}$  years.
- (g)  $N = 2^{2000}$  :  $L(N) = 2^{144.48}$  steps takes  $10^{26.99}$  years.

**3.29.** Prove that the function  $L(X) = e^{\sqrt{(\ln X)(\ln \ln X)}}$  is subexponential. That is, prove the following two statements.

- (a) For every positive constant  $\alpha$ , no matter how large,  $L(X) = \Omega((\ln X)^\alpha)$ .
- (b) For every positive constant  $\beta$ , no matter how small,  $L(X) = \mathcal{O}(X^\beta)$ .

Solution to Exercise 3.29.

*A solution for this exercise is not currently available.*

**3.30.** For any fixed positive constants  $a$  and  $b$ , define the function

$$F_{a,b}(X) = e^{(\ln X)^{1/a} (\ln \ln X)^{1/b}}.$$

Prove the following properties of  $F_{a,b}(X)$ .

- (a) If  $a > 1$ , prove that  $F_{a,b}(X)$  is subexponential.
- (b) If  $a = 1$ , prove that  $F_{a,b}(X)$  is exponential.
- (c) What happens if  $a < 1$ ?

Solution to Exercise 3.30.

*A solution for this exercise is not currently available.*

**3.31.** This exercise asks you to verify an assertion in the proof of Corollary 3.44. Let  $L(X)$  be the usual function  $L(X) = e^{\sqrt{(\ln X)(\ln \ln X)}}$ .

- (a) Prove that there is a value of  $\epsilon > 0$  such that

$$(\ln X)^\epsilon < \ln L(X) < (\ln X)^{1-\epsilon} \quad \text{for all } X > 10.$$

- (b) Let  $c > 0$ , let  $Y = L(X)^c$ , and let  $u = (\ln X)/(\ln Y)$ . Prove that

$$u^{-u} = L(X)^{-\frac{1}{2c}(1+o(1))}.$$

Solution to Exercise 3.31.

- (a) is clear, any  $\epsilon < \frac{1}{2}$  will work.
- (b) We first compute

$$u = \frac{\ln X}{\ln L(X)^c} = \frac{\ln X}{c\sqrt{(\ln X)(\ln \ln X)}} = \frac{1}{c} \sqrt{\frac{\ln X}{\ln \ln X}}.$$

Then



$$\begin{aligned}
u \ln u &= \frac{1}{c} \sqrt{\frac{\ln X}{\ln \ln X}} \ln \left( \frac{1}{c} \sqrt{\frac{\ln X}{\ln \ln X}} \right) \\
&= \frac{1}{c} \sqrt{\frac{\ln X}{\ln \ln X}} \left[ \frac{1}{2} \ln \ln X - \frac{1}{2} \ln \ln \ln X - \ln c \right] \\
&= \frac{1}{2c} \sqrt{\ln X \ln \ln X} (1 + o(1)) \\
&= \frac{1}{2c} (\ln L(X)) (1 + o(1)).
\end{aligned}$$

Hence

$$u^u = L(X)^{\frac{1}{2c}(1+o(1))}.$$

**3.32.** Proposition 3.47 assumes that we choose random numbers  $a$  modulo  $N$ , compute  $a^2 \pmod{N}$ , and check whether the result is  $B$ -smooth. We can achieve better results if we take values for  $a$  of the form

$$a = \lfloor \sqrt{N} \rfloor + k \quad \text{for } 1 \leq k \leq K.$$

(For simplicity, you may treat  $K$  as a fixed integer, independent of  $N$ . More rigorously, it is necessary to take  $K$  equal to a power of  $L(N)$ , which has a small effect on the final answer.)

- (a) Prove that  $a^2 - N \leq 2K\sqrt{N} + K^2$ , so in particular,  $a^2 \pmod{N}$  is smaller than a multiple of  $\sqrt{N}$ .
- (b) Prove that  $L(\sqrt{N}) \approx L(N)^{1/\sqrt{2}}$  by showing that

$$\lim_{N \rightarrow \infty} \frac{\log L(\sqrt{N})}{\log L(N)^{1/\sqrt{2}}} = 1.$$

More generally, prove that in the same sense,  $L(N^{1/r}) \approx L(N)^{1/\sqrt{r}}$  for any fixed  $r > 0$ .

- (c) Re-prove Proposition 3.47 using this better choice of values for  $a$ . Set  $B = L(N)^c$  and find the optimal value of  $c$ . Approximately how many relations are needed to factor  $N$ ?

Solution to Exercise 3.32.

(a) We have  $a = \sqrt{N} + \epsilon + k$  for some  $0 \leq \epsilon < 1$ . Hence  $a^2 - N = 2(\epsilon + k)\sqrt{N} + (\epsilon + k)^2 \leq 2K\sqrt{N} + K^2$ .

(b) A rough computation shows that

$$\begin{aligned}
L(\sqrt{N}) &= e^{\sqrt{(\ln \sqrt{N})(\ln \ln \sqrt{N})}} \\
&= e^{\sqrt{(\frac{1}{2} \ln N)(\ln \frac{1}{2} \ln N)}} \\
&\approx e^{\sqrt{(\frac{1}{2} \ln N)(\ln \ln N)}} = L(N)^{1/\sqrt{2}}.
\end{aligned}$$

More precisely, we first simplify

$$\begin{aligned} \frac{\log L(N^{1/r})}{\log L(N)^{1/\sqrt{r}}} &= \frac{\sqrt{\ln N^{1/r} \ln \ln N^{1/r}}}{(1/\sqrt{r})\sqrt{\ln N \ln \ln N}} \\ &= \sqrt{\frac{(1/r)(\ln N)(\ln(1/r) + \ln \ln N)}{(1/r)(\ln N)(\ln \ln N)}} \\ &= \sqrt{\frac{-\ln r}{\ln \ln N}} + 1. \end{aligned}$$

It is clear that if  $r$  is fixed, then this last expression goes to 1 as  $N \rightarrow \infty$ .

(c) We mimic the proof of Proposition 3.47. The probability that a random number that is approximately  $\sqrt{N}$  is  $B$ -smooth is  $\psi(\sqrt{N}, B)/\sqrt{N}$ , and we need approximately  $\pi(B)$  relations, so we need to check approximately

$$\frac{\pi(B)}{\psi(\sqrt{N}, B)/\sqrt{N}} \quad \text{numbers.} \quad (3.3)$$

We set  $B = L(\sqrt{N})^c$ , substitute into ??, and use Theorem ?? and the prime number theorem (Theorem 3.20) to get (we ignore various lower-order log terms)

$$\frac{\pi(L(\sqrt{N})^c)}{\psi(\sqrt{N}, L(\sqrt{N})^c)/\sqrt{N}} \approx \frac{L(\sqrt{N})^c}{L(\sqrt{N})^{-1/2c}} \approx L(N)^{\frac{1}{\sqrt{2}}(c + \frac{1}{2c})}.$$

The exponent is minimized when  $c = \frac{1}{\sqrt{2}}$ , so we should take  $B = L(\sqrt{N})^{1/\sqrt{2}} \approx L(N)^{1/2}$  and we need to check approximately  $L(N)$  numbers in order to factor  $N$ . Of course, our assumptions mean that this is an underestimate, but this exercise suggests that without some significant new idea, the running time of this method will be at least  $O(L(N))$ .

**3.33.** Illustrate the quadratic sieve, as was done in Figure 3.3 (page 157), by sieving prime powers up to  $B$  on the values of  $F(T) = T^2 - N$  in the indicated range.

- Sieve  $N = 493$  using prime powers up to  $B = 11$  on values from  $F(23)$  to  $F(38)$ . Use the relation(s) that you find to factor  $N$ .
- Extend the computations in (a) by using prime powers up to  $B = 16$  and sieving values from  $F(23)$  to  $F(50)$ . What additional value(s) are sieved down to 1 and what additional relation(s) do they yield?

Solution to Exercise 3.33.

- We sieve the following values, as illustrated in Table ??:

- The congruence  $t^2 \equiv 493 \equiv 1 \pmod{2}$  has solution  $t \equiv 1 \pmod{2}$ , so we sieve 2 from  $F(23)$ ,  $F(25)$ ,  $F(27)$ ,...

- The congruence  $t^2 \equiv 493 \equiv 1 \pmod{3}$  has solutions  $t \equiv 1 \pmod{3}$  and  $t \equiv 2 \pmod{3}$ , so first we sieve 3 from  $F(23)$ ,  $F(26)$ ,  $F(29)$ , ..., and then we sieve 3 from  $F(25)$ ,  $F(28)$ ,  $F(31)$ , ...
- The congruence  $t^2 \equiv 493 \equiv 1 \pmod{4}$  has solution  $t \equiv 1 \pmod{2}$ , so we sieve another 2 from  $F(23)$ ,  $F(25)$ ,  $F(27)$ , ...
- The congruence  $t^2 \equiv 493 \equiv 3 \pmod{5}$  has no solutions.
- The congruence  $t^2 \equiv 493 \equiv 3 \pmod{7}$  has no solutions.
- The congruence  $t^2 \equiv 493 \equiv 5 \pmod{8}$  has no solutions.
- The congruence  $t^2 \equiv 493 \equiv 7 \pmod{9}$  has solutions  $t \equiv 4 \pmod{9}$  and  $t \equiv 5 \pmod{9}$ , so first we sieve another 3 from  $F(31)$  and then we sieve another 3 from  $F(23)$  and  $F(32)$ .
- The congruence  $t^2 \equiv 493 \equiv 9 \pmod{11}$  has solutions  $t \equiv 3 \pmod{11}$  and  $t \equiv 8 \pmod{11}$ , so first we sieve 11 from  $F(25)$  and  $F(36)$  and then we sieve 11 from  $F(30)$ .

The two values  $F(23)$  and  $F(25)$  have been sieved down to 1, yielding the congruences

$$F(23) \equiv 36 \equiv 2^2 \cdot 3^2 \pmod{493} \quad \text{and} \quad F(25) \equiv 132 \equiv 2^2 \cdot 3 \cdot 11 \pmod{493}.$$

Since  $F(23)$  is itself congruent to a square, we can compute

$$\gcd(23 - 2 \cdot 3, 493) = 17,$$

which gives the factorization  $493 = 17 \cdot 29$ .

(b) The first step is to make Table ?? wider, i.e. sieve the values from  $F(23)$  to  $F(50)$  using prime powers up to  $B = 11$ . The next step is to sieve out the additional prime powers up to  $B = 16$ .

The congruence  $t^2 \equiv 493 \equiv 12 \pmod{13}$  has solutions  $t \equiv 5 \pmod{13}$  and  $t \equiv 8 \pmod{13}$ , so first we sieve 13 from  $F(31)$  and  $F(44)$ , and then we sieve 13 from  $F(34)$  and  $F(47)$ . The only other prime power up to  $B = 16$  is 16, and the congruence  $t^2 \equiv 493 \equiv 13 \pmod{16}$  has no solutions (as indeed it cannot, since we already noted that  $t^2 \equiv 493 \pmod{8}$  has no solutions).

We do not give the entire sieve table, but merely observe that two more values have been sieved down to 1, namely

$$F(31) = 468 \equiv 2^2 \cdot 3^2 \cdot 13 \pmod{493} \quad \text{and} \quad F(47) = 1716 \equiv 2^2 \cdot 3 \cdot 11 \cdot 13 \pmod{493}.$$

Combining these with the earlier fully sieved values gives the relation

$$(25 \cdot 31 \cdot 47)^2 \equiv (2^2 \cdot 3 \cdot 11) \cdot (2^2 \cdot 3^2 \cdot 13) \cdot (2^2 \cdot 3 \cdot 11 \cdot 13) \equiv (2^3 \cdot 3^2 \cdot 11 \cdot 13)^3 \pmod{493}.$$

Unfortunately,

$$\gcd(25 \cdot 31 \cdot 47 - 2^3 \cdot 3^2 \cdot 11 \cdot 13, 493) = \gcd(26129, 493) = 493,$$

so this relation does not give a factorization of 493.

23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
36	83	132	183	236	291	348	407	468	531	596	663	732	803	876	951
$\downarrow^2$		$\downarrow^2$		$\downarrow^2$		$\downarrow^2$		$\downarrow^2$		$\downarrow^2$		$\downarrow^2$		$\downarrow^2$	
18	83	66	183	118	291	174	407	234	531	298	663	366	803	438	951
$\downarrow^3$			$\downarrow^3$			$\downarrow^3$			$\downarrow^3$			$\downarrow^3$			$\downarrow^3$
6	83	66	61	118	291	58	407	234	177	298	663	122	803	438	317
		$\downarrow^3$			$\downarrow^3$			$\downarrow^3$			$\downarrow^3$			$\downarrow^3$	
6	83	22	61	118	97	58	407	78	177	298	221	122	803	146	317
$\downarrow^2$		$\downarrow^2$		$\downarrow^2$		$\downarrow^2$		$\downarrow^2$		$\downarrow^2$		$\downarrow^2$		$\downarrow^2$	
3	83	11	61	59	97	29	407	39	177	149	221	61	803	73	317
								$\downarrow^3$							
3	83	11	61	59	97	29	407	13	177	149	221	61	803	73	317
$\downarrow^3$								$\downarrow^3$							
1	83	11	61	59	97	29	407	13	59	149	221	61	803	73	317
		$\downarrow^{11}$											$\downarrow^{11}$		
1	83	1	61	59	97	29	407	13	59	149	221	61	73	73	317
							$\downarrow^{11}$								
1	83	1	61	59	97	29	37	13	59	149	221	61	73	73	317

Table 3.1: Sieving  $N = 493$ 

**3.34.** Let  $\mathbb{Z}[\beta]$  be the ring described in Example 3.54, i.e.,  $\beta$  is a root of  $f(x) = 1 + 3x - 2x^3 + x^4$ . For each of the following pairs of elements  $u, v \in \mathbb{Z}[\beta]$ , compute the sum  $u + v$  and the product  $uv$ . Your answers should involve only powers of  $\beta$  up to  $\beta^3$ .

- (a)  $u = -5 - 2\beta + 9\beta^2 - 9\beta^3$  and  $v = 2 + 9\beta - 7\beta^2 + 7\beta^3$ .
- (b)  $u = 9 + 9\beta + 6\beta^2 - 5\beta^3$  and  $v = -4 - 6\beta - 2\beta^2 - 5\beta^3$ .
- (c)  $u = 6 - 5\beta + 3\beta^3 + 3\beta^3$  and  $v = -2 + 7\beta + 6\beta^2$ .

*Solution to Exercise 3.34.*

- (a)  $u + v = -3 + 7\beta + 2\beta^2 - 2\beta^3$  and  $uv = 148 + 425\beta + 98\beta^2 - 85\beta^3$ .
- (b)  $u + 4 = 5 + 3\beta + 4\beta^2 - 10\beta^3$  and  $uv = -69 - 219\beta - 211\beta^2 - 88\beta^3$ .
- (c)  $u + v = 4 + \beta + 9\beta^2 + 3\beta^3$  and  $uv = -87 - 189\beta - 66\beta^2 + 129\beta^3$ .

Section. The index calculus and discrete logarithms

**3.35.** This exercise asks you to use the index calculus to solve a discrete logarithm problem. Let  $p = 19079$  and  $g = 17$ .

- (a) Verify that  $g^i \pmod{p}$  is 5-smooth for each of the values  $i = 3030$ ,  $i = 6892$ , and  $i = 18312$ .
- (b) Use your computations in (a) and linear algebra to compute the discrete logarithms  $\log_g(2)$ ,  $\log_g(3)$ , and  $\log_g(5)$ . (Note that  $19078 = 2 \cdot 9539$  and that 9539 is prime.)
- (c) Verify that  $19 \cdot 17^{-12400}$  is 5-smooth.

- (d) Use the values from (b) and the computation in (c) to solve the discrete logarithm problem

$$17^x \equiv 19 \pmod{19079}.$$

Solution to Exercise 3.35.

- (a) We have

$$g^{3030} \equiv 2^2 \cdot 3^6 \cdot 5, \quad g^{6892} \equiv 2^{11} \cdot 3^2, \quad g^{18312} \equiv 2^4 \cdot 3 \cdot 5^3.$$

- (b) We get the linear equations

$$\begin{aligned} 3030 &= 2x_2 + 6x_3 + x_5 \\ 6892 &= 11x_2 + 2x_3 \\ 18312 &= 4x_2 + x_3 + 2x_5 \end{aligned}$$

Solving modulo 2 and modulo 9539 gives

$$\begin{aligned} (x_2, x_3, x_5) &\equiv (0, 0, 0) \pmod{2}, \\ (x_2, x_3, x_5) &\equiv (8195, 1299, 7463) \pmod{9539}. \end{aligned}$$

Hence

$$(x_2, x_3, x_5) \equiv (17734, 10838, 17002) \pmod{19079}.$$

- (c) We compute

$$h \cdot g^{-12224} \equiv 2^{13} \pmod{19079}.$$

- (d) Hence

$$\log_g(h) = 12224 + 13 \cdot \log_g(2) = 242766 \equiv 13830 \pmod{p-1}.$$

We check that  $17^{13830} \equiv 19 \pmod{19079}$ . ✓

Section. Quadratic residues and quadratic reciprocity

**3.36.** Let  $p$  be an odd prime and let  $a$  be an integer with  $p \nmid a$ .

- (a) Prove that  $a^{(p-1)/2}$  is congruent to either 1 or  $-1$  modulo  $p$ .  
 (b) Prove that  $a^{(p-1)/2}$  is congruent to 1 modulo  $p$  if and only if  $a$  is a quadratic residue modulo  $p$ . (*Hint.* Let  $g$  be a primitive root for  $p$  and use the fact, proven during the course of proving Proposition 3.60, that  $g^m$  is a quadratic residue if and only if  $m$  is even.)  
 (c) Prove that  $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$ . (This holds even if  $p \mid a$ .)  
 (d) Use (c) to prove Theorem 3.61(a), that is, prove that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Solution to Exercise 3.36.

*A solution for this exercise is not currently available.*

**3.37.** Prove that the three parts of the quadratic reciprocity theorem (Theorem 3.61) are equivalent to the following three concise formulas, where  $p$  and  $q$  are odd primes:

$$(a) \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad (b) \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad (c) \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

*Solution to Exercise 3.37.*

*A solution for this exercise is not currently available.*

**3.38.** Let  $p$  be a prime satisfying  $p \equiv 3 \pmod{4}$ .

(a) Let  $a$  be a quadratic residue modulo  $p$ . Prove that the number

$$b \equiv a^{\frac{p+1}{4}} \pmod{p}$$

has the property that  $b^2 \equiv a \pmod{p}$ . (*Hint.* Write  $\frac{p+1}{2}$  as  $1 + \frac{p-1}{2}$  and use Exercise 3.36.) This gives an easy way to take square roots modulo  $p$  for primes that are congruent to 3 modulo 4.

(b) Use (a) to compute the following square roots modulo  $p$ . Be sure to check your answers.

(i) Solve  $b^2 \equiv 116 \pmod{587}$ .

(ii) Solve  $b^2 \equiv 3217 \pmod{8627}$ .

(iii) Solve  $b^2 \equiv 9109 \pmod{10663}$ .

*Solution to Exercise 3.38.*

This was proven in Chapter 2, see Proposition 2.27, but it is included here as an exercise because of its importance, and because the use of the Legendre symbol makes for a short proof.

(a)

$$b^2 \equiv a^{\frac{p+1}{2}} \equiv a^{1+\frac{p-1}{2}} \equiv a \cdot \left(\frac{a}{p}\right) \equiv a \pmod{p}.$$

We are using  $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$  from the previous exercise and the assumption that  $a$  is a quadratic residue, which tells us that  $\left(\frac{a}{p}\right) = 1$ .

(b) (i)  $116^{(587+1)/4} = 116^{147} \equiv 65 \pmod{587}$ . Check:  $65^2 \equiv 116 \pmod{587}$ .

(ii)  $3217^{(8627+1)/4} \equiv 1865^{2157} \equiv 2980 \pmod{8627}$ . Check:  $2980^2 \equiv 3217 \pmod{8627}$ .

(iii)  $9109^{(10663+1)/4} \equiv 9109^{2666} \equiv 3502 \pmod{10663}$ . Check:  $3502^2 \equiv 1554 \pmod{10663}$ . Oops, what's going on? The problem is that  $\left(\frac{9109}{10663}\right) = -1$ , so 9109 is not a quadratic residue modulo 10663. In fact, the previous exercise tells us that  $b^2 \equiv \left(\frac{a}{p}\right)a \pmod{p}$ , and indeed in this case we have  $3502^2 \equiv -9109 \pmod{10663}$ .

**3.39.** Recall that for any  $a \in \mathbb{F}_p^*$ , the discrete logarithm of  $a$  (with respect to a primitive root  $g$ ) is a number  $\log_g(a)$  satisfying

$$g^{\log_g(a)} \equiv a \pmod{p}.$$

Prove that

$$\left(\frac{a}{p}\right) = (-1)^{\log_g(a)} \quad \text{for all } a \in \mathbb{F}_p^*.$$

Thus quadratic reciprocity gives a fast method to compute the parity of  $\log_g(a)$ .

Solution to Exercise 3.39.

To ease notation, let  $k = \log_g(a)$ . Then

$$\begin{aligned} \left(\frac{a}{p}\right) &\equiv a^{(p-1)/2} \pmod{p} && \text{from earlier exercise,} \\ &\equiv g^{k(p-1)/2} \pmod{p} && \text{from definition of discrete log,} \\ &\equiv (-1)^k \pmod{p} && \text{since } g^{(p-1)/2} \equiv 1 \pmod{p}. \end{aligned}$$

**3.40.** Let  $p \geq 5$  be a prime. We say that  $a$  is a *cubic residue modulo*  $p$  if  $p \nmid a$  and there is an integer  $c$  satisfying  $a \equiv c^3 \pmod{p}$ .

- Let  $a$  and  $b$  be cubic residues modulo  $p$ . Prove that  $ab$  is a cubic residue modulo  $p$ .
- Give an example to show that (unlike the case with quadratic residues) it is possible for none of  $a$ ,  $b$ , and  $ab$  to be a cubic residue modulo  $p$ .
- Let  $g$  be a primitive root modulo  $p$ . Prove that  $a$  is a cubic residue modulo  $p$  if and only if  $3 \mid \log_g(a)$ , where  $\log_g(a)$  is the discrete logarithm of  $a$ .

Solution to Exercise 3.40.

It is easiest to prove (c) first, but we give a direct proof of (a). The assumption is that there are numbers  $c$  and  $d$  satisfying

$$a \equiv c^3 \pmod{p} \quad \text{and} \quad b \equiv d^3 \pmod{p}.$$

Then  $ab \equiv (cd)^3 \pmod{p}$ , so  $ab$  is also a cubic residue modulo  $p$ .

(b,c) *A solution for this exercise is not currently available.*

**Section. Probabilistic encryption and the Goldwasser–Micali cryptosystem**

**3.41.** Perform the following encryptions and decryptions using the Goldwasser–Micali public key cryptosystem (Table 3.9).

- Bob's public key is the pair  $N = 1842338473$  and  $a = 1532411781$ . Alice encrypts three bits and sends Bob the ciphertext blocks

$$1794677960, \quad 525734818, \quad \text{and} \quad 420526487.$$

Decrypt Alice's message using the factorization

$$N = pq = 32411 \cdot 56843.$$

- (b) Bob's public key is  $N = 3149$  and  $a = 2013$ . Alice encrypts three bits and sends Bob the ciphertext blocks 2322, 719, and 202. Unfortunately, Bob used primes that are much too small. Factor  $N$  and decrypt Alice's message.
- (c) Bob's public key is  $N = 781044643$  and  $a = 568980706$ . Encrypt the three bits 1, 1, 0 using, respectively, the three random values

$$r = 705130839, \quad r = 631364468, \quad r = 67651321.$$

*Solution to Exercise 3.41.*

(a) Decrypt  $c = 1794677960$  by computing  $\left(\frac{1794677960}{32411}\right) = -1$ , which gives the plaintext bit  $m = 1$ . Decrypt  $c = 525734818$  by computing  $\left(\frac{525734818}{32411}\right) = 1$ , which gives the plaintext bit  $m = 0$ . Decrypt  $c = 420526487$  by computing  $\left(\frac{420526487}{32411}\right) = -1$ , which gives the plaintext bit  $m = 1$ . Alice's plaintext is  $(1, 0, 1)$ .

(b) The factorization of  $m$  is  $m = 3149 = 47 \cdot 57$ . Decrypt  $c = 2322$  by computing  $\left(\frac{2322}{47}\right) = -1$ , which gives the plaintext bit  $m = 1$ . Decrypt  $c = 719$  by computing  $\left(\frac{719}{47}\right) = 1$ , which gives the plaintext bit  $m = 0$ . Decrypt  $c = 202$  by computing  $\left(\frac{202}{47}\right) = 1$ , which gives the plaintext bit  $m = 0$ . Thus Alice's plaintext is  $(1, 0, 0)$ .

(c) Although it is not needed to do this problem, the factorization of  $m$  is  $m = 781044643 = 22109 \cdot 35327$ . Encrypt  $m = 1$  using  $r = 705130839$ . Compute  $c \equiv ar^2 \equiv 568980706 \cdot 705130839^2 \equiv 517254876 \pmod{781044643}$ . Encrypt  $m = 1$  using  $r = 631364468$ . Compute  $c \equiv ar^2 \equiv 568980706 \cdot 631364468^2 \equiv 4308279 \pmod{781044643}$ . Encrypt  $m = 0$  using  $r = 67651321$ . Compute  $c \equiv r^2 \equiv 67651321^2 \equiv 660699010 \pmod{781044643}$ . The ciphertext for  $(1, 1, 0)$  is  $(517254876, 4308279, 660699010)$ .

**3.42.** Suppose that the plaintext space  $\mathcal{M}$  of a certain cryptosystem is the set of bit strings of length  $2b$ . Let  $e_k$  and  $d_k$  be the encryption and decryption functions associated with a key  $k \in \mathcal{K}$ . This exercise describes one method of turning the original cryptosystem into a probabilistic cryptosystem. Most practical cryptosystems that are currently in use rely on more complicated variants of this idea in order to thwart certain types of attacks. (See Section 8.6 for further details.)

Alice sends Bob an encrypted message by performing the following steps:

1. Alice chooses a  $b$ -bit message  $m'$  to be encrypted.
2. Alice chooses a string  $r$  consisting of  $b$  random bits.
3. Alice sets  $m = r \parallel (r \oplus m')$ , where  $\parallel$  denotes concatenation<sup>1</sup> and  $\oplus$  denotes exclusive or (see Section 1.7.4). Notice that  $m$  has length  $2b$  bits.
4. Alice computes  $c = e_k(m)$  and sends the ciphertext  $c$  to Bob.

<sup>1</sup>The *concatenation* of two bit strings is formed by placing the first string before the second string. For example,  $1101 \parallel 1001$  is the bit string  $11011001$ .



- (a) Explain how Bob decrypts Alice's message and recovers the plaintext  $m'$ . We assume, of course, that Bob knows the decryption function  $d_k$ .
- (b) If the plaintexts and the ciphertexts of the original cryptosystem have the same length, what is the message expansion ratio of the new probabilistic cryptosystem?
- (c) More generally, if the original cryptosystem has a message expansion ratio of  $\mu$ , what is the message expansion ratio of the new probabilistic cryptosystem?

Solution to Exercise 3.42.

- (a) Bob decrypts  $c$  to recover  $m = d_k(c)$ . He splits  $m$  up into two pieces  $m = r \parallel s$ , where  $r$  consists of the first  $b$  bits of  $m$  and  $s$  consists of the last  $b$  bits of  $m$ . Then he recovers Alice's plaintext  $m'$  by computing  $r \oplus s$ .
- (b) The new probabilistic cryptosystem has plaintext length  $b$  bits and ciphertext length  $2b$  bits, so its message expansion ratio is 2.
- (c) The plaintexts in the original cryptosystem have length  $2b$  bits, and it has message expansion  $\mu$ , so its ciphertexts have length  $2b\mu$  bits. The new probabilistic cryptosystem has plaintext length  $b$  bits, so its message expansion ratio is  $2b\mu/b = 2\mu$ .

# Chapter 4

## Combinatorics, Probability, and Information Theory

### Exercises for Chapter 4

Section. Basic principles of counting

**4.1.** The Rhind papyrus is an ancient Egyptian mathematical manuscript that is more than 3500 years old. Problem 79 of the Rhind papyrus poses a problem that can be paraphrased as follows: there are seven houses; in each house lives seven cats; each cat kills seven mice; each mouse has eaten seven spelt seeds<sup>1</sup>; each spelt seed would have produced seven hekat<sup>2</sup> of spelt. What is the sum of all of the named items? Solve this 3500 year old problem.

Solution to Exercise 4.1.

$$\underbrace{7}_{\text{houses}} + \underbrace{7^2}_{\text{cats}} + \underbrace{7^3}_{\text{mice}} + \underbrace{7^4}_{\text{spelt}} + \underbrace{7^5}_{\text{hekat}} = 19607.$$

As stated in the Rhind papyrus, the problem and solution looks more or less as follows:

		houses	7
1	2,801	cats	49
2	5,602	mice	343
4	11,204	spelt	2,301
		hekat	16,807
	Total 19,607	Total	19,607

---

<sup>1</sup> *Spelt* is an ancient type of wheat.

<sup>2</sup> A *hekat* is  $\frac{1}{30}$  of a cubic cubit, which is approximately 4.8 liters.

Notice that the author has made a mistake in the value of  $7^4 = 2401$ , but that his final answer is correct. The last column in the Rhind papyrus is the same as our solution, adding up powers of 7. In the first column the author gives an alternative computational method based on the fact that  $2801 = 1 + 7 + 7^2 + 7^3 + 7^4$ . Thus he computes

$$\begin{aligned} 7 + 7^2 + 7^3 + 7^4 + 7^5 &= 7 \cdot (1 + 7 + 7^2 + 7^3 + 7^4) \\ &= (1 + 2 + 4) \cdot (1 + 7 + 7^2 + 7^3 + 7^4) \\ &= 2801 + 2 \cdot 2801 + 4 \cdot 2801. \end{aligned}$$

This double-and-add method is very reminiscent of many modern algorithms.

- 4.2.** (a) How many  $n$ -tuples  $(x_1, x_2, \dots, x_n)$  are there if the coordinates are required to be integers satisfying  $0 \leq x_i < q$ ?
- (b) Same question as (a), except now there are separate bounds  $0 \leq x_i < q_i$  for each coordinate.
- (c) How many  $n$ -by- $n$  matrices are there if the entries  $x_{i,j}$  of the matrix are integers satisfying  $0 \leq x_{i,j} < q$ ?
- (d) Same question as (a), except now the order of the coordinates does not matter. So for example,  $(0, 0, 1, 3)$  and  $(1, 0, 3, 0)$  are considered the same. (This one is rather tricky.)
- (e) Twelve students are each taking four classes, for each class they need two loose-leaf notebooks, for each notebook they need 100 sheets of paper, and each sheet of paper has 32 lines on it. Altogether, how many students, classes, notebooks, sheets, and lines are there? (Bonus. Make this or a similar problem of your own devising into a rhyme like the St. Ives riddle.)

Solution to Exercise 4.2.

- (a) There are  $q$  choices for each coordinate, so a total of  $q^n$  possible  $n$ -tuples.
- (b) Now there are  $q_1$  choices for  $x_1$ , and  $q_2$  choices for  $x_2$ , and so on. Hence the total number of possibilities is the product  $q_1 q_2 \cdots q_n$ .
- (c) This is the same as (a), except now there are  $n^2$  entries to be filled in. So there are  $q^{n^2}$  possible matrices.
- (d) The idea is to count the quantity of each number that appears. Say there are  $k_0$  zeros,  $k_1$  ones, etc. Then  $k_0 + k_1 + \cdots + k_{q-1} = n$ , so we need to count the number of ways to split  $n$  into a sum of  $q$  nonnegative pieces. The answer to this is  $\binom{q+n-1}{q-1}$ , which is also equal to  $\binom{q+n-1}{n}$ .
- (e) The total number of students, classes, notebooks, sheets, and lines is

$$307200 = \underbrace{12}_{\text{students}} \cdot \underbrace{4}_{\text{classes}} \cdot \underbrace{2}_{\text{notebooks}} \cdot \underbrace{100}_{\text{sheets}} \cdot \underbrace{32}_{\text{lines}}.$$

- 4.3.** (a) List all of the permutations of the set  $\{A, B, C\}$ .
- (b) List all of the permutations of the set  $\{1, 2, 3, 4\}$ .

- (c) How many permutations are there of the set  $\{1, 2, \dots, 20\}$ ?  
 (d) Seven students are to be assigned to seven dormitory rooms, each student receiving his or her own room. In how many ways can this be done?  
 (e) How many different words can be formed with the four symbols  $A, A, B, C$ ?

Solution to Exercise 4.3.

(a)

$(A, B, C), (A, C, B), (B, A, C), (B, C, A), (C, A, B), (C, B, A).$

(b) There are 24 permutations of  $\{1, 2, 3, 4\}$ . They are

$(1, 2, 3, 4) \quad (1, 2, 4, 3) \quad (1, 3, 2, 4) \quad (1, 3, 4, 2) \quad (1, 4, 2, 3) \quad (1, 4, 3, 2)$   
 $(2, 1, 3, 4) \quad (2, 1, 4, 3) \quad (2, 3, 1, 4) \quad (2, 3, 4, 1) \quad (2, 4, 1, 3) \quad (2, 4, 3, 1)$   
 $(3, 1, 2, 4) \quad (3, 1, 4, 2) \quad (3, 2, 1, 4) \quad (3, 2, 4, 1) \quad (3, 4, 1, 2) \quad (3, 4, 2, 1)$   
 $(4, 1, 2, 3) \quad (4, 1, 3, 2) \quad (4, 2, 1, 3) \quad (4, 2, 3, 1) \quad (4, 3, 1, 2) \quad (4, 3, 2, 1)$

(c) There are  $20! = 2432902008176640000 \approx 2.43 \cdot 10^{18}$  permutations of  $\{1, 2, \dots, 20\}$ .

(d) If the rooms are labeled  $1, 2, \dots, 7$ , then each permutation of the students gives a way of assigning rooms, by putting the first listed student in room #1, the second listed student in room #2, etc. So there are  $7! = 5040$  ways to assign rooms.

(e) There are 4 choices for placement of  $B$ , then 3 choices for placement of  $C$ , after which the two  $A$ 's go in the remaining places, so there are 12 words.

**4.4.** (a) List the 24 possible permutations of the letters  $A_1, A_2, B_1, B_2$ . If  $A_1$  is indistinguishable from  $A_2$ , and  $B_1$  is indistinguishable from  $B_2$ , show how the permutations become grouped into 6 distinct letter arrangements, each containing 4 of the original 24 permutations.

- (b) Using the seven symbols  $A, A, A, A, B, B, B$ , how many different seven letter words can be formed?  
 (c) Using the nine symbols  $A, A, A, A, B, B, B, C, C$ , how many different nine letter words can be formed?  
 (d) Using the seven symbols  $A, A, A, A, B, B, B$ , how many different five letter words can be formed?

Solution to Exercise 4.4.

(a) Here are the 24 permutations.

$(A_1, A_2, B_1, B_2) \quad (A_1, A_2, B_2, B_1) \quad (A_2, A_1, B_1, B_2) \quad (A_2, A_1, B_2, B_1)$   
 $(A_1, B_1, A_2, B_2) \quad (A_1, B_2, A_2, B_1) \quad (A_2, B_1, A_1, B_2) \quad (A_2, B_2, A_1, B_1)$   
 $(A_1, B_1, B_2, A_2) \quad (A_1, B_2, B_1, A_2) \quad (A_2, B_1, B_2, A_1) \quad (A_2, B_2, B_1, A_1)$   
 $(B_1, B_2, A_2, A_1) \quad (B_1, B_2, A_1, A_2) \quad (B_2, B_1, A_1, A_2) \quad (B_2, B_1, A_2, A_1)$   
 $(B_1, A_1, A_2, B_2) \quad (B_1, A_2, A_1, B_2) \quad (B_2, A_1, A_2, B_1) \quad (B_2, A_2, A_1, B_1)$   
 $(B_1, A_1, B_2, A_2) \quad (B_1, A_2, B_2, A_1) \quad (B_2, A_1, B_1, A_2) \quad (B_2, A_2, B_1, A_1)$

If  $A_1 = A_2$  and  $B_1 = B_2$ , then the four entries in each row become the same.

(b) We need to pick 4 of the 7 spots for the  $A$ 's, then the  $B$ 's go into the remaining 3 spots. Hence there are  $\binom{7}{4} = 35$  such words.

(c) We need to pick 4 of the 9 spots for the  $A$ 's, then we need to pick 3 of the remaining 5 spots for the  $B$ 's, then the  $C$ 's go into the remaining 2 spots. Hence there are  $\binom{9}{4}\binom{5}{3} = 126 \cdot 10 = 1260$  such words.

(d) We can form five letter words using anywhere from two to four  $A$ 's. So we need to count the number of five letter words using each of

$$\{A, A, A, A, B\}, \quad \{A, A, A, B, B\}, \quad \text{and} \quad \{A, A, B, B, B\}.$$

So there are

$$\binom{5}{4} + \binom{5}{3} + \binom{5}{2} = 25 \quad \text{different five letter words.}$$

- 4.5.** (a) There are 100 students eligible for an award, and the winner gets to choose from among 5 different possible prizes. How many possible outcomes are there?
- (b) Same as in (a), but this time there is a first place winner, a second place winner, and a third place winner, each of whom gets to select a prize. However, there is only one of each prize. How many possible outcomes are there?
- (c) Same as in (b), except that there are multiple copies of each prize, so each of the three winners may choose any of the prizes. Now how many possible outcomes are there? Is this larger or smaller than your answer from (b)?
- (d) Same as in (c), except that rather than specifying a first, second, and third place winner, we just choose three winning students without differentiating between them. Now how many possible outcomes are there? Compare the size of your answers to (b), (c), and (d).

Solution to Exercise 4.5.

- (a) There are  $100 \cdot 5 = 500$  outcomes.
- (b) This can be split into first choosing the three winners (in order), which can be done in  $100 \cdot 99 \cdot 98$  ways, and then choosing the three prizes (in order), which can be done in  $5 \cdot 4 \cdot 3$  ways. Then using the basic counting principle, the total number of outcomes is

$$100 \cdot 99 \cdot 98 \cdot 5 \cdot 4 \cdot 3 = 58212000 \approx 10^{7.77}.$$

- (b) This time there are  $5 \cdot 5 \cdot 5$  ways to choose the prizes, so the total number of outcomes is

$$100 \cdot 99 \cdot 98 \cdot 5 \cdot 5 \cdot 5 = 121275000 \approx 10^{8.08}.$$

- (c) Since the order of the students does not matter, there are now  $\binom{100}{3} = \frac{100 \cdot 99 \cdot 98}{3!}$  ways to choose the students. Hence the total number of outcomes is

$$\frac{100 \cdot 99 \cdot 98}{3!} \cdot 5 \cdot 5 \cdot 5 = 20212500 \approx 10^{7.31}.$$

**4.6.** Use the binomial theorem (Theorem 4.10) to compute each of the following quantities.

(a)  $(5z + 2)^3$       (b)  $(2a - 3b)^4$       (c)  $(x - 2)^5$

*Solution to Exercise 4.6.*

(a)  $(5z + 2)^3 = 125z^3 + 225z^2 + 135z + 27.$   
 (b)  $(2a - 3b)^4 = 16a^4 - 96a^3b + 216a^2b^2 - 216ab^3 + 81b^4.$   
 (c)  $(x - 2)^5 = x^5 - 10x^4 + 40x^3 - 80x^2 + 80x - 32.$

**4.7.** The binomial coefficients satisfy many interesting identities. Give three proofs of the identity

$$\binom{n}{j} = \binom{n-1}{j-1} + \binom{n-1}{j}.$$

- (a) For Proof #1, use the definition of  $\binom{n}{j}$  as  $\frac{n!}{(n-j)!j!}$ .  
 (b) For Proof #2, use the binomial theorem (Theorem 4.10) and compare the coefficients of  $x^j y^{n-j}$  on the two sides of the identity

$$(x + y)^n = (x + y)(x + y)^{n-1}.$$

- (c) For Proof #3, argue directly that choosing  $j$  objects from a set of  $n$  objects can be decomposed into either choosing  $j - 1$  objects from  $n - 1$  objects or choosing  $j$  objects from  $n - 1$  objects.

*Solution to Exercise 4.7.*

**Proof #1:**

$$\begin{aligned} \binom{n-1}{j-1} + \binom{n-1}{j} &= \frac{(n-1)!}{(n-j)!(j-1)!} + \frac{(n-1)!}{(n-1-j)!j!} \\ &= \frac{(n-1)!}{(n-1-j)!(j-1)!} \left[ \frac{1}{n-j} + \frac{1}{j} \right] \\ &= \frac{(n-1)!}{(n-1-j)!(j-1)!} \cdot \frac{n}{(n-j)j} \\ &= \frac{n!}{(n-j)!j!} \\ &= \binom{n}{j}. \end{aligned}$$

**Proof #2:** Expand both sides of  $(x + y)^n = (x + y)(x + y)^{n-1}$  using the binomial theorem:

$$\begin{aligned}
\sum_{j=0}^n \binom{n}{j} x^j y^{n-j} &= (x+y) \sum_{j=0}^{n-1} \binom{n-1}{j} x^j y^{n-1-j} \\
&= \sum_{j=0}^{n-1} \binom{n-1}{j} x^{j+1} y^{n-1-j} + \sum_{j=0}^{n-1} \binom{n-1}{j} x^j y^{n-j} \\
&= \sum_{j=1}^n \binom{n-1}{j-1} x^j y^{n-j} + \sum_{j=0}^{n-1} \binom{n-1}{j} x^j y^{n-j} \\
&= x^n + \sum_{j=1}^{n-1} \left[ \binom{n-1}{j-1} + \binom{n-1}{j} \right] x^j y^{n-j} + y^n.
\end{aligned}$$

Comparing the coefficients of  $x^j y^{n-j}$  on the two sides gives the desired identity.

Another way to illustrate the same proof is to write the expansion of  $(x+y)^n$  for  $n = 0, 1, 2, 3, \dots$  in the form of a triangle called Pascal's triangle.

**Proof #3:** Let the  $n$  objects be  $A_1, \dots, A_n$ . Treat the last one as special, so label them as  $A_1, \dots, A_{n-1}, B$ . In choosing  $j$  of these  $n$  objects, there are two possibilities, namely either  $B$  is chosen or it is not chosen. The number of ways to choose  $j$  objects without  $B$  is  $\binom{n-1}{j}$ , since we are choosing  $j$  objects from among the  $n-1$   $A$ 's. The number of ways to choose  $j$  objects including  $B$  is  $\binom{n-1}{j-1}$ , since having already selected  $B$ , we are need to choose  $j-1$  objects from among the  $n-1$   $A$ 's.

**4.8.** Let  $p$  be a prime number. This exercise sketches another proof of Fermat's little theorem (Theorem 1.25).

- (a) If  $1 \leq j \leq p-1$ , prove that the binomial coefficient  $\binom{p}{j}$  is divisible by  $p$ .  
(b) Use (a) and the binomial theorem (Theorem 4.10) to prove that

$$(a+b)^p \equiv a^p + b^p \pmod{p} \quad \text{for all } a, b \in \mathbb{Z}.$$

- (c) Use (b) with  $b = 1$  and induction on  $a$  to prove that  $a^p \equiv a \pmod{p}$  for all  $a \geq 0$ .  
(d) Use (c) to deduce that  $a^{p-1} \equiv 1 \pmod{p}$  for all  $a$  with  $\gcd(p, a) = 1$ .

Solution to Exercise 4.8.

(a)

$$\binom{p}{j} = \frac{p(p-1)(p-2) \cdots (p-j+1)}{j!}.$$

The denominator has no factors of  $p$ , so the  $p$  in the numerator does not cancel.

(b)

$$(a+b)^p = \sum_{j=0}^p \binom{p}{j} a^j b^{p-j} \equiv a^p + b^p \pmod{p},$$

since (a) tells us that the middle terms in the sum are all divisible by  $p$ .

(c) Suppose we know that  $a^p \equiv a \pmod{p}$ , which we do for the starting value  $a = 0$ . Then using (b) we have

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}.$$

Hence the result is also true for  $a+1$ . By induction, it is true for all  $a \geq 0$ .

(d) If  $p \nmid a$ , then we can multiply both sides of  $a^p \equiv a \pmod{p}$  by  $a^{-1} \pmod{p}$ .

**4.9.** We know that there are  $n!$  different permutations of the set  $\{1, 2, \dots, n\}$ .

- (a) How many of these permutations leave no number fixed?
- (b) How many of these permutations leave at least one number fixed?
- (c) How many of these permutations leave exactly one number fixed?
- (d) How many of these permutations leave at least two numbers fixed?

For each part of this problem, give a formula or algorithm that can be used to compute the answer for an arbitrary value of  $n$ , and then compute the value for  $n = 10$  and  $n = 26$ . (This exercise generalizes Exercise 1.5.)

Solution to Exercise 4.9.

Let  $\mathbf{S}(n, k)$  denote the number of permutations of  $n$  elements that fix at least  $k$  elements, let  $\mathbf{R}(n, k)$  denote the number of permutations of  $n$  elements that fix *exactly*  $k$  elements, and let  $!n$  (the *subfactorial* of  $n$ ) denote the number of permutations of  $n$  elements that fix no elements (such permutations are called *derangements*). Notice that  $!n = \mathbf{R}(n, 0)$ . See the solution to Exercise exercise:derangement for the derivation of the following formulas:

$$\begin{aligned} !n &= n! \sum_{k=0}^n \frac{(-1)^k}{k!} = \lfloor n!/e \rfloor, \\ \mathbf{R}(n, k) &= \binom{n}{k} !(n-k) = \binom{n}{k} \left\lfloor \frac{(n-k)!}{e} \right\rfloor, \\ \mathbf{S}(n, k) &= \sum_{j=k}^n \mathbf{R}(n, j) = n! - \sum_{j=0}^{k-1} \mathbf{R}(n, j). \end{aligned}$$

(a) No letters fixed is  $\mathbf{R}(n, 0) = !n$ . This is called the  $n^{\text{th}}$  *derangement number*. For  $n = 10$  we get

$$\mathbf{R}(10, 0) = !10 = \lfloor 10!/e \rfloor = \lfloor 1334960.916 \rfloor = 1334961.$$

For  $n = 26$  we get

$$\begin{aligned} \mathbf{R}(26, 0) = !26 &= \lfloor 26!/e \rfloor = \lfloor 148362637348470135821287824.964 \rfloor \\ &= 148362637348470135821287825. \end{aligned}$$

(b) At least one letter fixed is  $n!$  minus no letters fixed, so



$$S(n, 1) = n! - R(n, 0) = n! - !n = n! - \lfloor n!/e \rfloor.$$

Hence

$$S(10, 1) = 10! - \lfloor 10!/e \rfloor = 2293839,$$

$$S(26, 1) = 26! - \lfloor 26!/e \rfloor = 254928823778135499762712175.$$

(c) Exactly 1 letter fixed is

$$R(n, 1) = n \cdot (n-1)! = n \left\lfloor \frac{(n-1)!}{e} \right\rfloor,$$

so

$$R(10, 1) = 10 \left\lfloor \frac{9!}{e} \right\rfloor = 1334960,$$

$$R(26, 1) = 26 \left\lfloor \frac{25!}{e} \right\rfloor = 148362637348470135821287824.$$

(d) At least two letters fixed is  $n!$  minus zero or one letters fixed, so

$$\begin{aligned} S(n, 1) &= n! - R(n, 0) - R(1, 0) = n! - !n - n \cdot (n-1)! \\ &= n! - \lfloor n!/e \rfloor - n \lfloor (n-1)!/e \rfloor. \end{aligned}$$

Hence

$$S(10, 1) = 10! - \lfloor 10!/e \rfloor - 10 \cdot \lfloor 9!/e \rfloor = 958879,$$

$$S(26, 1) = 26! - \lfloor 26!/e \rfloor - 26 \cdot \lfloor 25!/e \rfloor = 106566186429665363941424351.$$

#### Section. The Vigenère cipher

**4.10.** Encrypt each of the following Vigenère plaintexts using the given keyword and the Vigenère tableau (Table 4.1).

(a) Keyword: **hamlet**

Plaintext: **To be, or not to be, that is the question.**

(b) Keyword: **fortune**

Plaintext: **The treasure is buried under the big W.**

#### Solution to Exercise 4.10.

(a) Vigenère Keyword: hamlet

t	b	e	o	r	n	o	t	t	o	b	e	t	h	a	t	i	s	t	h	e	q	u	e	s	t	i	o	n	
h	a	m	l	e	t	h	a	m	l	e	t	h	a	m	l	e	t	h	a	m	l	e	t	h	a	m	l	e	t
a	o	n	p	s	k	u	o	f	e	s	u	l	t	t	l	x	b	z	t	t	p	u	n	l	s	f	t	s	g

(b) Vigenère Keyword: fortune

t	h	e	t	r	e	a	s	u	r	e	i	s	b	u	r	i	e	d	u	n	d	e	r	t	h	e	b	i	g	w
f	o	r	t	u	n	e	f	o	r	t	u	n	e	f	o	r	t	u	n	e	f	o	r	t	u	n	e	f	o	r
y	v	v	m	l	r	e	x	i	i	x	c	f	f	z	f	z	x	x	h	r	i	s	i	m	b	r	f	n	u	n

**4.11.** Decrypt each of the following Vigenère ciphertexts using the given keyword and the Vigenère tableau (Table 4.1).

(a) Keyword: **condiment**

Ciphertext: **r s g h z b m c x t d v f s q h n i g q x r n b m**  
**p d n s q s m b t r k u**

(b) Keyword: **rabbithole**

Ciphertext: **k h f e q y m s c i e t c s i g j v p w f f b s q**  
**m o a p x z c s f x e p s o x y e n p k d a i c x**  
**c e b s m t t p t x z o o e q l a f l g k i p o c**  
**z s w q m t a u j w g h b o h v r j t q h u**

*Solution to Exercise 4.11.*

(a) Vigenère Keyword: **condiment**

Ciphertext: **r s g h z b m c x t d v f s q h n i g q x r n b m**  
 Keyword: **c o n d i m e n t c o n d i m e n t c o n d i m e**  
 Plaintext: **p e t e r p i p e r p i c k e d a p e c k o f p i**

Ciphertext: **p d n s q s m b t r k u**  
 Keyword: **n t c o n d i m e n t c**  
 Plaintext: **c k l e d p e p p e r s**

*Plaintext.* Peter Piper picked a peck of pickled peppers!

(b) Vigenère Keyword: **rabbithole**

Ciphertext: **k h f e q y m s c i e t c s i g j v p w f f b s q**  
 Keyword: **r a b b i t h o l e r a b b i t h o l e r a b b i**  
 Plaintext: **t h e d i f f e r e n t b r a n c h e s o f a r i**

Ciphertext: **m o a p x z c s f x e p s o x y e n p k d a i c x**  
 Keyword: **t h o l e r a b b i t h o l e r a b b i t h o l e**  
 Plaintext: **t h m e t i c r e p l i e d t h e m o c k t u r t**

Ciphertext: **c e b s m t t p t x z o o e q l a f l g k i p o c**  
 Keyword: **r a b b i t h o l e r a b b i t h o l e r a b b i**  
 Plaintext: **l e a r e a m b i t i o n d i s t r a c t i o n u**

Ciphertext: **z s w q m t a u j w g h b o h v r j t q h u**  
 Keyword: **t h o l e r a b b i t h o l e r a b b i t h**  
 Plaintext: **g l i f i c a t i o n a n d d e r i s i o n**

*Plaintext.* The different branches of arithmetic, replied the Mock Turtle, are ambition, distraction, uglification, and derision. (From Lewis Carroll's *Alice in Wonderland*.)

**4.12.** Explain how a cipher wheel with rotating inner wheel (see Figure 1.1 on page 3) can be used in place of a Vigenère tableau (Table 4.1) to perform Vigenère encryption and decryption. Illustrate by describing the sequence of rotations used to perform a Vigenère encryption with the keyword **mouse**.

*Solution to Exercise 4.12.*

*A solution for this exercise is not currently available.*

**4.13.** Let

$\mathbf{s}$  = “I am the very model of a modern major general.”

$\mathbf{t}$  = “I have information vegetable, animal, and mineral.”

- Make frequency tables for  $\mathbf{s}$  and  $\mathbf{t}$ .
- Compute  $\text{IndCo}(\mathbf{s})$  and  $\text{IndCo}(\mathbf{t})$ .
- Compute  $\text{MutIndCo}(\mathbf{s}, \mathbf{t})$ .

*Solution to Exercise 4.13.*

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
(a) Freq $\mathbf{s}$	4	0	0	2	6	1	1	1	1	1	0	2	4	2	4	0	0	4	0	1	0	1	0	0	1	0
Freq $\mathbf{t}$	8	1	0	1	4	1	1	1	5	0	0	3	3	5	2	0	0	2	0	2	0	2	0	0	0	0

(b)  $IC(\mathbf{s}) = 0.0424$  and  $IC(\mathbf{t}) = 0.0544$ .

(c)  $MIC(\mathbf{s}, \mathbf{t}) = 0.0517$

**4.14.** The following strings are blocks from a Vigenère encryption. It turns out that the keyword contains a repeated letter, so two of these blocks were encrypted with the same shift. Compute  $\text{MutIndCo}(\mathbf{s}_i, \mathbf{s}_j)$  for  $1 \leq i < j \leq 3$  and use these values to deduce which two strings were encrypted using the same shift.

$\mathbf{s}_1$  = iwseesetftuonhdptbunnybioeatneghictdnsevi

$\mathbf{s}_2$  = qibfhroeqeickxmirqqlflgkrqkejbejpepldfjbk

$\mathbf{s}_3$  = iesnnciiheptevaireittuevmhoootttrtaaflnatg

*Solution to Exercise 4.14.*

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
(a) Freq $\mathbf{s}_1$	1	2	1	2	6	1	1	2	4	0	0	0	0	5	2	1	0	0	3	5	2	1	1	0	1	0
Freq $\mathbf{s}_2$	0	4	1	1	5	3	1	1	3	3	4	3	1	0	1	2	4	3	0	0	0	0	0	1	0	0
Freq $\mathbf{s}_3$	4	0	1	0	5	1	1	2	5	0	0	1	1	3	3	1	0	2	1	7	1	2	0	0	0	0

$$\text{MutIndCo}(\mathbf{s}_1, \mathbf{s}_2) = 0.0375,$$

$$\text{MutIndCo}(\mathbf{s}_1, \mathbf{s}_3) = 0.0744,$$

$$\text{MutIndCo}(\mathbf{s}_2, \mathbf{s}_3) = 0.0369.$$

Thus  $\mathbf{s}_1$  and  $\mathbf{s}_3$  were probably encrypted using the same shift, so the first and third letters of the keyword are probably the same.

**4.15.** (a) One of the following two strings was encrypted using a simple substitution cipher, while the other is a random string of letters. Compute the index of coincidence of each string and use the results to guess which is which.

$s_1 = \text{RCZBWBHSLPSCPILHBGZJTGBIBJGLYIJIBFHCQQFZBYFP},$   
 $s_2 = \text{KHQWGI ZMGKPOYRKHUITDUXLXCWZOTWPAHFOHMGFEVUEJJ}.$

- (b) One of the following two strings was encrypted using a simple substitution cipher, while the other is a random permutation of the same set of letters.

$s_1 = \text{NTDCFVDHCTHKGUNGKEPGXKEWNECKEGWEWETWKUEVHDKK}$   
 $\text{CDGCWXXDEEAMNHGNDIWUVWSSCTUNIGDSWKE}$   
 $s_2 = \text{IGWSKGEHEXNGECKVWNKVWNKSUTEHTWHEKDNCDXWSIEKD}$   
 $\text{AECKFGNDCPUCKDNCUVWEMGEKWGEUTDGTWHD}$

Thus their Indices of Coincidence are identical. Develop a method to compute a bigram index of coincidence, i.e., the frequency of pairs of letters, and use it to determine which string is most likely the encrypted text.

(Bonus: Decrypt the encrypted texts in (a) and (b), but be forewarned that the plaintexts are in Latin.)

Solution to Exercise 4.15.

(a) The Indices of Coincidence of the two strings are  $\text{IndCo}(s_1) = 0.0576$  and  $\text{IndCo}(s_2) = 0.0303$ , so most likely  $s_1$  is the encrypted text and  $s_2$  is the random string. The plaintext for  $s_1$  is “Facilius per partes in cognitionem totius adducimur,” which translated into English says “We are more easily led part by part to an understanding of the whole.” The phrase is due to Seneca.

(b) The Indices of Coincidence are identical,  $\text{IndCo}(s_1) = \text{IndCo}(s_2) = 0.0672$ . In general, let  $A = \{a_1, a_2, \dots, a_k\}$  be a set of distinct objects (letters, bigrams, turtles, etc.) and let  $B = (b_1, b_2, \dots, b_n)$  be a list of elements from  $A$ , where the  $b_i$  do not need to be distinct. For each  $1 \leq i \leq k$ , let  $F_i$  denote the number of  $b$ 's that are equal to  $a_i$ , i.e.,  $F_i$  is the frequency with which  $a_i$  appears in the list  $B$ . Then the index of coincidence of the set  $B$  is

$$\text{IndCo}(B) = \frac{1}{n(n-1)} \sum_{i=1}^k F_i(F_i - 1).$$

So now we can apply the theory of Index of Coincidence to the set of bigrams that appear in a string. And we would expect that the index should be higher for the string that is the encrypted message and lower for the string with the same letters, but randomly rearranged. We find that

$$\text{IndCo}(\text{Bigrams in } s_1) = 0.004,$$

$$\text{IndCo}(\text{Bigrams in } s_2) = 0.010.$$

Thus it seems likely that the second string  $s_2$  is the encrypted plaintext. This is the case, and the plaintext for  $s_2$  is “Frustra laborant quotquot se calculationibus fatigant pro inventione quadraturae circuli,” which translated into English says “Futile is the labor of those who fatigue themselves with calculations to square the circle.” The phrase is due to Michael Stifel (1544).

```

nhqrk vvvfe fwgjo mzejgc kocgk lejrj wossy wgvkk hnesg kwebi
bkkcj vqazx wnvll zetjc zwgqz zwhah kwdxj fgnyw gdfgh bitig
mrkwn nsuhy iecru ljjvs qlvww zzxyv woenx ujgyr kqbfj lvjzx
dxjfg nywus rwoar xhvwx ssmja vkrwt uhktm malcz ygrsz xwnvl
lzavs hyigh rvwpn ljazl nispv jahym ntewj jvrzg qvzcr estul
fkwis tfylk ysnir rddpb svxux zjgqk xouhs zzrjj kyiwc zckov
qyhdv rhhny wqhyi rjdqm iwutf nkzgd vvibg oenwb kolca mskle
cuwvz rgusl zgfhy etfre ijyvy ghfau wvwtv xlljv vywyj apgzv
trggr dxfgs cepts tiiih vjjvt tcxfj hciiv voaro lrxij vjnok
mvrwg kmirt twfer oimbs qgrgc

```

Table 4.1: A Vigenère ciphertext for Exercise 4.16

**4.16.** Table 4.13 is a Vigenère ciphertext in which we have marked some of the repeated trigrams for you. How long do you think the keyword is? Why?

Bonus: Complete the cryptanalysis and recover the plaintext.

*Solution to Exercise 4.16.*

Trigram	Appears at places	Differences
hyi	109, 206 and 313	$97 = 97$ $107 = 107$ $204 = 2^2 \cdot 3 \cdot 17$
jjv	117, 235, 372, and 422	$118 = 2 \cdot 59$ $137 = 137$ $255 = 3 \cdot 5 \cdot 17$ $305 = 5 \cdot 61$ $187 = 11 \cdot 17$ $50 = 2 \cdot 5^2$
nyw	88, 156, and 309	$68 = 2^2 \cdot 17$ $221 = 13 \cdot 17$ $153 = 3^2 \cdot 17$

The keyword has length 17. The keyword used for encryption was

`fourscoreandseven`.

The plaintext is

It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to Heaven, we were all going direct the other way—in short, the period was so far like the present period,

togmg gbymk kcqiv dmlxk kbyif vcuek cuuis vvxqs pwwej koqgg  
 phumt whlsf yovww knhhm rcqfq vvhkw psued ugrsf ctwij khvfa  
 thkef fwptj ggivv cgdra pgwvm osqyg hkdvt whuev kcwyj psgsn  
 gfwsl jsfse ooqhw tofsh aciin gfbif gabgj adwsy topml ecqzw  
 asgvs fwrqs fsfvq rhdrs nmvmk cbhrv kblxk gzi

Table 4.2: A Vigenère ciphertext for Exercise 4.17

Blocks		Shift Amount												
$i$	$j$	0	1	2	3	4	5	6	7	8	9	10	11	12
1	2	.044	.047	.021	.054	.046	.038	.022	.034	.057	.035	.040	.023	.038
1	3	.038	.031	.027	.037	.045	.036	.034	.032	.039	.039	.047	.038	.050
1	4	.025	.039	.053	.043	.023	.035	.032	.043	.029	.040	.041	.050	.027
1	5	.050	.050	.025	.031	.038	.045	.037	.028	.032	.038	.063	.033	.034
2	3	.035	.037	.039	.031	.031	.035	.047	.048	.034	.031	.031	.067	.053
2	4	.040	.033	.046	.031	.033	.023	.052	.027	.031	.039	.078	.034	.029
2	5	.042	.040	.042	.029	.033	.035	.035	.038	.037	.057	.039	.038	.040
3	4	.032	.033	.035	.049	.053	.027	.030	.022	.047	.036	.040	.036	.052
3	5	.043	.043	.040	.034	.033	.034	.043	.035	.026	.030	.050	.068	.044
4	5	.045	.033	.044	.046	.021	.032	.030	.038	.047	.040	.025	.037	.068

Blocks		Shift Amount												
$i$	$j$	13	14	15	16	17	18	19	20	21	22	23	24	25
1	2	.040	.063	.033	.025	.032	.055	.038	.030	.032	.045	.035	.030	.044
1	3	.026	.046	.042	.053	.027	.024	.040	.047	.048	.018	.037	.034	.066
1	4	.042	.050	.042	.031	.024	.052	.027	.051	.020	.037	.042	.069	.031
1	5	.030	.048	.039	.030	.034	.038	.042	.035	.036	.043	.055	.030	.035
2	3	.039	.015	.030	.045	.049	.037	.023	.036	.030	.049	.039	.050	.037
2	4	.027	.048	.050	.037	.032	.021	.035	.043	.047	.041	.047	.042	.035
2	5	.033	.035	.039	.033	.037	.047	.037	.028	.034	.066	.054	.032	.022
3	4	.040	.048	.041	.044	.033	.028	.039	.027	.036	.017	.038	.051	.065
3	5	.039	.029	.045	.040	.033	.028	.031	.037	.038	.036	.033	.051	.036
4	5	.049	.033	.029	.043	.028	.033	.020	.040	.040	.041	.039	.039	.059

Table 4.3: Mutual indices of coincidence for Exercise 4.17

that some of its noisiest authorities insisted on its being received,  
 for good or for evil, in the superlative degree of comparison only.

These are the opening lines of *A Tale of Two Cities* by Charles Dickens.

**4.17.** We applied a Kasiski test to the Vigenère ciphertext listed in Table 4.14 and found that the key length is probably 5. We then performed a mutual index of coincidence test to each shift of each pair of blocks and listed the results for you in Table 4.15. (This is the same type of table as Table 4.5 in the text, except that we haven't underlined the large values.) Use Table 4.15 to guess the relative rotations of the blocks, as we did in Table 4.6. This will give you a rotated version of the keyword. Try rotating it, as we did in Table 4.7, to find the correct keyword and decrypt the text.

Solution to Exercise 4.17.

The table of likely shift relations gives

$i$	$j$	Shift	MutIndCo	Shift Relation
2	3	11	0.067	$\beta_2 - \beta_3 = 11$
2	4	10	0.078	$\beta_2 - \beta_4 = 10$
3	5	11	0.068	$\beta_3 - \beta_5 = 11$
4	5	12	0.068	$\beta_4 - \beta_5 = 12$
1	3	25	0.066	$\beta_1 - \beta_3 = 25$
1	4	24	0.069	$\beta_1 - \beta_4 = 24$
2	5	22	0.066	$\beta_2 - \beta_5 = 22$
3	4	25	0.065	$\beta_3 - \beta_4 = 25$

Table 4.4: Large indices of coincidence and shift relations

Shift	Keyword	Decrypted Text
0	AMBCQ	tcfkqgpxkukqpgfdakvukpxgvpqtcucitgcvjwocpk
1	BNCDR	sbejpflowjtjpofeczjutjowfoupsbtbhsfbuivnboj
2	CODES	radioenvisionedbyitsinventorasagreathumani
3	DPEFT	qzchndmuhrrhmdcaxhsrhmdmsnqzrzfqdzsgtlzmh
4	EQFGU	pybgmcltgqgmlcbzwgrqgltrmpyqyepcyrfskylg
5	FRGHV	oxaflbksfpflkbayvfqpfksbkqlopxdobxqerjxkf
6	GSHIW	nwzekajreoekjazxuepoejrajpknowcnawpdqiwe
7	HTIJX	mvydjzqidndjizywtndondiqziojmvnbmzvocphvid
8	IUJKY	luxciyhpcmcihyxvscnmchpyhnilumalyunboguhc
$\vdots$	$\vdots$	$\vdots$

Table 4.5: Decryption using shifts of the keyword AJCHWJZ

$$\beta_2 = \beta_1 + 12, \quad \beta_3 = \beta_1 + 1, \quad \beta_4 = \beta_1 + 2, \quad \beta_5 = \beta_1 + 16.$$

Hence the keyword is a rotation of AMBCQ. The table lists the rotations of this word with the corresponding decryptions. We see immediately that the keyword is CODES. The full plaintext reads as follows:

Radio, envisioned by its inventor as a great humanitarian contribution, was seized upon by the generals soon after its birth and impressed as an instrument of war. But radio turned over to the commander a copy of every enemy cryptogram it conveyed. Radio made cryptanalysis an end in itself.

*The Code-Breakers*, Chapter 10, 1967, David Kahn

**4.18.** Table 4.16 gives a Vigenère ciphertext for you to analyze from scratch. It is probably easiest to do so by writing a computer program, but you are welcome to try to decrypt it with just paper and pencil.

- (a) Make a list of matching trigrams as we did in Table 4.3. Use the Kasiski test on matching trigrams to find the likely key length.

mgodt beida psgls akowu hxukc iawlr csoyh prtrt udrqh cengx  
 uuqtu habxw dgkie ktsnp sekld zlvnh wefss glzrn peaoy lbyig  
 uaafv eqgjo ewabz saawl rzjpv feyky gylwu btlyd kroec bpfvt  
 psgki puxfb uxfuq cvymy okagl sactt uwlrz psgiy ytpsf rjfuw  
 igxhr oyazd rakce dxeyr pdobr buehr uwcue ekfic zehrq ijezr  
 xsyor tcylf egcy

Table 4.6: A Vigenère ciphertext for Exercise 4.18

Trigram	Appears at places	Difference
awl	27 and 118	91
ehr	228 and 242	14
gki	62 and 153	91
gls	13 and 174	161
lsa	14 and 175	161
psg	11 and 151 and 186	140 and 35
sgl	12 and 85	73
tps	150 and 192	42
uxf	157 and 161	4
wlr	28 and 119 and 182	91 and 63

Table 4.7: Repeated trigrams in the ciphertext

- Make a table of indices of coincidence for various key lengths, as we did in Table 4.4. Use your results to guess the probable key length.
- Using the probable key length from (a) or (b), make a table of mutual indices of coincidence between rotated blocks, as we did in Table 4.5. Pick the largest indices from your table and use them to guess the relative rotations of the blocks, as we did in Table 4.6.
- Use your results from (c) to guess a rotated version of the keyword, and then try the different rotations as we did in Table 4.7 to find the correct keyword and decrypt the text.

Solution to Exercise 4.18.

A list of repeated trigrams for the Kasiski test is given in the Table. The list of differences (sorted) is

$$\{4, 14, 35, 42, 63, 73, 91, 91, 91, 140, 154, 161, 161, 175\}.$$

Thus a good guess for the period is 7.

Solving the relations in the table gives

$$\beta_2 = \beta_1 + 9, \quad \beta_3 = \beta_1 + 2, \quad \beta_4 = \beta_1 + 7, \quad \beta_5 = \beta_1 + 22, \quad \beta_6 = \beta_1 + 9.$$

(There is actually one erroneous relation, namely  $\beta_2 - \beta_5 = 24$ , but our solution satisfies the other 10 relations, which makes it likely that it is correct.) In order



Block Size	Average Index	Individual Indices of Coincidence
4	0.043	0.038, 0.043, 0.042, 0.046
5	0.044	0.048, 0.052, 0.046, 0.030, 0.041
6	0.042	0.036, 0.050, 0.042, 0.051, 0.038, 0.035
7	0.060	0.058, 0.060, 0.081, 0.054, 0.059, 0.065, 0.047
8	0.046	0.042, 0.051, 0.030, 0.053, 0.040, 0.051, 0.057, 0.040
9	0.041	0.041, 0.053, 0.042, 0.037, 0.052, 0.030, 0.054, 0.030, 0.030

Table 4.8: Index of coincidence for various block sizes

Blocks		Shift Amount												
$i$	$j$	0	1	2	3	4	5	6	7	8	9	10	11	12
1	2	.037	.035	.043	.037	.045	.035	.053	.046	.035	.034	.046	.030	.024
1	3	.020	.046	.035	.041	.046	.030	.033	.039	.037	.033	.040	.048	.036
1	4	.038	.031	.045	.035	.039	.030	.046	.043	.050	.041	.026	.035	.039
1	5	.053	.037	.027	.034	<b>.065</b>	.048	.038	.036	.048	.028	.022	.036	.044
1	6	.024	.027	.048	.044	.039	.043	.043	.040	.024	.036	.053	.043	.039
1	7	.048	.055	.038	.036	.033	.031	.037	.047	.041	.023	.035	.041	.049
2	3	.040	.035	.026	.046	.039	.027	.051	<b>.071</b>	.022	.026	.062	.033	.039
2	4	.038	.045	<b>.070</b>	.029	.034	.044	.035	<b>.037</b>	.042	.038	.030	.042	.037
2	5	.041	.038	.051	.032	.021	.028	.043	.025	.031	.049	.039	.031	.044
2	6	<b>.067</b>	.034	.028	.050	.048	.027	.036	.045	.028	.023	.034	.056	.031
2	7	.030	.030	.047	.031	.035	.035	.056	.031	.034	.051	.048	.031	.033
3	4	.033	.048	.035	.033	.044	.046	.040	.023	.044	.028	.048	.037	.037
3	5	.034	.040	.054	.042	.026	.026	.056	.042	.036	.032	.046	.031	.035
3	6	.050	.042	.022	.029	.047	.038	.036	.033	.041	.041	.030	.030	.038
3	7	.033	.025	.032	.059	.038	.039	.028	.037	.033	.053	.039	.026	.039
4	5	.053	.040	.036	.021	.042	.032	.031	.038	.035	.033	.038	.058	.045
4	6	.020	.037	.041	.040	.043	.041	.031	.015	.030	.049	.043	.035	.030
4	7	.040	.038	.030	.028	.052	.032	.041	.041	.058	.029	.030	.036	.045
5	6	.022	.045	.050	.031	.034	.053	.047	.023	.037	.044	.030	.024	.044
5	7	.039	.034	.028	.038	.044	.020	.039	.050	.057	.028	.035	.050	.038
6	7	.032	.029	.052	.049	.028	.037	.035	.031	.031	.058	.055	.024	.033

Blocks		Shift Amount												
$i$	$j$	13	14	15	16	17	18	19	20	21	22	23	24	25
1	2	.047	.047	.021	.030	<b>.070</b>	.043	.030	.046	.038	.028	.030	.039	.029
1	3	.033	.051	.030	.047	.044	.032	.026	.055	.031	.016	.046	<b>.080</b>	.024
1	4	.035	.037	.058	.039	.021	.036	.062	.042	.036	.042	.024	.033	.039
1	5	.031	.028	.054	.052	.036	.040	.049	.041	.022	.032	.039	.030	.030
1	6	.046	.038	.014	.033	<b>.066</b>	.039	.024	.043	.036	.021	.036	.055	.041
1	7	.040	.040	.048	.038	.026	.023	.053	.041	.033	.031	.053	.030	.029
2	3	.035	.038	.029	.042	.037	.044	.023	.044	.035	.040	.049	.033	.033
2	4	.050	.029	.045	.035	.039	.033	.026	.033	.033	.039	.028	.054	.036
2	5	.064	.041	.032	.033	.044	.025	.020	.038	.037	.037	.037	<b>.072</b>	.048
2	6	.025	.038	.034	.036	.028	.043	.047	.038	.038	.048	.048	.026	.043
2	7	.043	.034	.033	.036	.041	.023	.048	.044	.056	.031	.042	.038	.039
3	4	.027	.034	.033	.042	.048	.055	.022	.021	<b>.073</b>	.039	.033	.042	.035
3	5	.028	.050	.033	.035	.054	.054	.036	.033	.040	.043	.031	.024	.041
3	6	.047	.049	.042	.050	.026	.018	<b>.065</b>	.048	.027	.050	.041	.024	.035
3	7	.043	.046	.035	.041	.041	.042	.027	.029	.039	.047	.036	.033	.059
4	5	.036	.032	.044	.038	.037	.033	.040	.029	.029	.053	.048	.046	.034
4	6	.038	.035	.036	.041	.047	.048	.034	.038	.046	.041	.038	.063	.043
4	7	.044	.037	.037	.021	.041	.038	.053	.037	.043	.032	.041	.033	.042
5	6	<b>.065</b>	.031	.021	.039	.042	.028	.028	.058	.035	.024	.043	.057	.042
5	7	.034	.033	.050	.028	.028	.035	.045	.030	.042	.053	.056	.029	.037
6	7	.036	.042	.032	.048	.050	.025	.032	.037	.056	.035	.030	.045	.038

Table 4.9: Mutual indices of coincidence for shifted blocks

$i$	$j$	Shift	MutIndCo	Shift Relation
1	5	4	0.065	$\beta_1 - \beta_5 = 4$
2	3	7	0.071	$\beta_2 - \beta_3 = 7$
2	4	2	0.070	$\beta_2 - \beta_4 = 2$
2	6	0	0.067	$\beta_2 - \beta_6 = 0$
1	2	17	0.070	$\beta_1 - \beta_2 = 17$
1	3	24	0.080	$\beta_1 - \beta_3 = 24$
1	6	17	0.066	$\beta_1 - \beta_6 = 17$
2	5	24	0.072	$\beta_2 - \beta_5 = 24$
3	4	21	0.073	$\beta_3 - \beta_4 = 21$
3	6	19	0.065	$\beta_3 - \beta_6 = 19$
5	6	13	0.065	$\beta_5 - \beta_6 = 13$

Table 4.10: Large indices of coincidence and shift relations

to find  $\beta_7$ , we look at the mutual indices that involve Block 7 and are greater than 0.058. There are three of them:

$i$	$j$	Shift	MutIndCo	Shift Relation
3	7	3	0.059	$\beta_3 - \beta_7 = 3$
3	7	25	0.059	$\beta_3 - \beta_7 = 25$
4	7	8	0.058	$\beta_4 - \beta_7 = 8$

Only one of the first two can be correct, but the third yields  $\beta_7 = \beta_1 + 25$ . This agrees with  $\beta_7 = \beta_3 - 3 = 25$ , so is probably correct. Thus the amounts that Blocks 2 through 7 are rotated exceed the amount that Block 1 is rotated by 9, 2, 7, 22, 9, and 25, respectively. For example, if the first letter of the keyword is A, then the full keyword is AJCHWJZ. The shifts of this keyword and decryptions are listed in the table.

We find that the keyword is ENGLAND, and the full plaintext reads as follows:

It is to be questioned whether in the whole length and breadth of the world there is a more admirable spot for a man in love to pass a day or two than the typical English village. It combines the comforts of civilization with the restfulness of solitude in a manner equalled by no other spot except the New York Public Library.

*A Damsel in Distress*, 1919, P.G. Wodehouse

**4.19.** The *autokey cipher* is similar to the Vigenère cipher, except that rather than repeating the key, it simply uses the key to encrypt the first few letters and then uses the plaintext itself (shifted over) to continue the encryption. For example, in order to encrypt the message “The autokey cipher is cool” using the keyword **random**, we proceed as follows:

Shift	Keyword	Decrypted Text
0	AJCHWJZ	mxmwxsfuiyiwxsrihalixlivmrxlialspipirkxle
1	BKDIXKA	lwlvwrehtxhvwlrqhgzkhwkhulqwkzhkrohohqjwkd
2	CLEJYLB	kvkuvqdgswguvkqpgfyjgvjgtpvjgyjqngngpivjc
3	DMFKZMC	jujtupcfrvftujpofexifuifsjouifxipmfmfohuib
4	ENGLAND	itistobequestionedwhetherinthewholelengtha
5	FOHMBOE	hshrsnadptdrshnmcdvgdsgdqhmvgdvgndkdmfsgz
6	GPINCPF	grgqrmzcoscqrgrmlcbufcrfcpglrfcufmjcclerfy
7	HQJODQG	fqfpqlybnrbpqflkbatebqebfofkqebtelibibkdqex
8	IRKPERH	epeopkxamqaopekjazsdapdanejpdasdkhahajcpdw
9	JSLQFSI	dodnojwzlpznodjizyrczoczmidioczrcjgzgzigbovcv
⋮	⋮	⋮

Table 4.11: Decryption using shifts of the keyword AJCHWJZ

Plaintext	t h e a u t o k e y c i p h e r i s c o o l
Key	r a n d o m t h e a u t o k e y c i p h e r
Ciphertext	k h r d i f h r i y w b d r i p k a r v s c

The autokey cipher has the advantage that different messages are encrypted using different keys (except for the first few letters). Further, since the key does not repeat, there is no key length, so the autokey is not directly susceptible to a Kasiski or index of coincidence analysis. A disadvantage of the autokey is that a single mistake in encryption renders the remainder of the message unintelligible. According to [58], Vigenère invented the autokey cipher in 1586, but his invention was ignored and forgotten before being reinvented in the 1800s.

- Encrypt the following message using the autokey cipher:  
 Keyword: LEAR  
 Plaintext: Come not between the dragon and his wrath.
- Decrypt the following message using the autokey cipher:  
 Keyword: CORDELIA  
 Ciphertext: pckkm yowvz ejwzk knyzv vurux cstri tgac
- Eve intercepts an autokey ciphertext and manages to steal the accompanying plaintext:  
 Plaintext ifmusicbethethefoodofloveplayon  
 Ciphertext azdzwqvjjfbwnqphhmptjsszfjci  
 Help Eve to figure out the keyword that was used for encryption. Describe your method in sufficient generality to show that the autokey cipher is susceptible to chosen plaintext attacks.
- Bonus Problem: Try to formulate a statistical or algebraic attack on the autokey cipher, assuming that you are given a large amount of ciphertext to analyze.

Solution to Exercise 4.19.

(a)

c o m e n o t b e t w e e n t h e d r a g o n a n d h i s w r a t h  
 l e a r c o m e n o t b e t w e e n t h e d r a g o n a n d h i s w  
 n s m v p c f f r h p f i g p l i q k h k r e a t r u i f z y i l d

The ciphertext is nsmvp cffrh pfigp liqkh kreat ruifz yild.

(b)

p c k k m y o w v z e j w z k k n y z v v u r u x c s t r i t g a c  
 c o r d e l i a n o t h i n g w i l l c o m e o f n o t h i n g s p  
 n o t h i n g w i l l c o m e o f n o t h i n g s p e a k a g a i n

The plaintext is **Nothing will come of nothing. Speak again.** These are King Lear's tragically inaccurate words to his youngest daughter Cordelia.

(c) The keyword is **SURFEIT**. The line is from Shakespeare's *Twelfth Night*, and the full encryption is

i f m u s i c b e t h e f o o d o f l o v e p l a y o n  
 s u r f e i t i f m u s i c b e t h e f o o d o f l o v  
 a z d z w q v j j f b w n q p h h m p t j s s z f j c i

## Section. Probability theory

**4.20.** Use the definition (4.15) of the probability of an event to prove the following basic facts about probability theory.

(a) Let  $E$  and  $F$  be disjoint events. Then

$$\Pr(E \cup F) = \Pr(E) + \Pr(F).$$

(b) Let  $E$  and  $F$  be events that need not be disjoint. Then

$$\Pr(E \cup F) = \Pr(E) + \Pr(F) - \Pr(E \cap F).$$

(c) Let  $E$  be an event. Then  $\Pr(E^c) = 1 - \Pr(E)$ .

(d) Let  $E_1, E_2, E_3$  be events. Prove that

$$\begin{aligned} \Pr(E_1 \cup E_2 \cup E_3) &= \Pr(E_1) + \Pr(E_2) + \Pr(E_3) - \Pr(E_1 \cap E_2) \\ &\quad - \Pr(E_1 \cap E_3) - \Pr(E_2 \cap E_3) + \Pr(E_1 \cap E_2 \cap E_3). \end{aligned}$$

The formulas in (b) and (d) and their generalization to  $n$  events are known as the *inclusion-exclusion principle*.

Solution to Exercise 4.20.

*A solution for this exercise is not currently available.*

**4.21.** We continue with the coin tossing scenario from Example 4.23, so our experiment consists in tossing a fair coin ten times. Compute the probabilities of the following events.

- (a) The first and last tosses are both heads.
- (b) Either the first toss or the last toss (or both) are heads.
- (c) Either the first toss or the last toss (but not both) are heads.
- (d) There are exactly  $k$  heads and  $10 - k$  tails. Compute the probability for each value of  $k$  between 0 and 10. (*Hint.* To save time, note that the probability of exactly  $k$  heads is the same as the probability of exactly  $k$  tails.)
- (e) There is an even number of heads.
- (f) There is an odd number of heads.

Solution to Exercise 4.21.

We label the events in the parts of this problem as  $E_{(a)}$ ,  $E_{(b)}$ ,  $E_{(c,k)}$ , etc.

- (a)  $\Pr(E_{(a)}) = \frac{1}{4}$ .
- (b)  $\Pr(E_{(b)}) = 1 - \Pr(E_{(b)}^c) = 1 - \frac{1}{4} = \frac{3}{4}$ .
- (c)  $\Pr(E_{(c)}) = \Pr(E_{(b)}) - \Pr(E_{(a)}) = \frac{1}{2}$ .
- (d)

$$\Pr(E_{(d,0)}) = \binom{10}{0} \cdot \frac{1}{2^{10}} = \frac{1}{1024} = \frac{1}{1024} \approx 0.0010$$

$$\begin{aligned}
\Pr(E_{(d,1)}) &= \binom{10}{1} \cdot \frac{1}{2^{10}} = \frac{10}{1024} = \frac{5}{512} \approx 0.0098 \\
\Pr(E_{(d,2)}) &= \binom{10}{2} \cdot \frac{1}{2^{10}} = \frac{45}{1024} = \frac{45}{1024} \approx 0.0439 \\
\Pr(E_{(d,3)}) &= \binom{10}{3} \cdot \frac{1}{2^{10}} = \frac{120}{1024} = \frac{15}{128} \approx 0.1172 \\
\Pr(E_{(d,4)}) &= \binom{10}{4} \cdot \frac{1}{2^{10}} = \frac{210}{1024} = \frac{105}{512} \approx 0.2051 \\
\Pr(E_{(d,5)}) &= \binom{10}{5} \cdot \frac{1}{2^{10}} = \frac{252}{1024} = \frac{63}{256} \approx 0.2461 \\
\Pr(E_{(d,6)}) &= \binom{10}{6} \cdot \frac{1}{2^{10}} = \frac{210}{1024} = \frac{105}{512} \approx 0.2051 \\
\Pr(E_{(d,7)}) &= \binom{10}{7} \cdot \frac{1}{2^{10}} = \frac{120}{1024} = \frac{15}{128} \approx 0.1172 \\
\Pr(E_{(d,8)}) &= \binom{10}{8} \cdot \frac{1}{2^{10}} = \frac{45}{1024} = \frac{45}{1024} \approx 0.0439 \\
\Pr(E_{(d,9)}) &= \binom{10}{9} \cdot \frac{1}{2^{10}} = \frac{10}{1024} = \frac{5}{512} \approx 0.0098 \\
\Pr(E_{(d,10)}) &= \binom{10}{10} \cdot \frac{1}{2^{10}} = \frac{1}{1024} = \frac{1}{1024} \approx 0.0010
\end{aligned}$$

(e)

$$\Pr(E_{(e)}) = \Pr(\text{Even number of heads}) = \sum_{k \text{ even}} \Pr(E_{(c,k)}) = \frac{1}{2}.$$

(f)  $\Pr(E_{(f)}) = \Pr(E_{(d)}) = \frac{1}{2}.$ 

**4.22.** Alice offers to make the following bet with you. She will toss a fair coin 14 times. If exactly 7 heads come up, she will give you \$4; otherwise you must give her \$1. Would you take this bet? If so, and if you repeated the bet 10000 times, how much money would you expect to win or lose?

Solution to Exercise 4.22.

The probability of winning the bet is

$$\binom{14}{7} \cdot \frac{1}{2^{14}} = \frac{3432}{16384} = \frac{429}{2048} \approx 0.2095.$$

Thus your probability of winning the bet is slightly larger than  $\frac{1}{5}$ , so it is worthwhile making the bet. (Note that if the probability of winning were exactly  $\frac{1}{5}$ , then in five trials you would expect to win once for plus \$4 and lose four times for minus \$4, so you would end up even.) In 10000 trials, you

would expect to win the bet approximately 2095 times, for a gain of \$8380, and to lose the bet approximately 7905 times, for a loss of \$7905. Hence your average net gain for 10000 trials is \$475.

**4.23.** Let  $E$  and  $F$  be events.

- (a) Prove that  $\Pr(E | E) = 1$ . Explain in words why this is reasonable.
- (b) If  $E$  and  $F$  are disjoint, prove that  $\Pr(F | E) = 0$ . Explain in words why this is reasonable.
- (c) Let  $F_1, \dots, F_n$  be events satisfying  $F_i \cap F_j = \emptyset$  for all  $i \neq j$ . We say that  $F_1, \dots, F_n$  are *pairwise disjoint*. Prove then that

$$\Pr\left(\bigcup_{i=1}^n F_i\right) = \sum_{i=1}^n \Pr(F_i).$$

- (d) Let  $F_1, \dots, F_n$  be pairwise disjoint as in (c), and assume further that

$$F_1 \cup \dots \cup F_n = \Omega,$$

where recall that  $\Omega$  is the entire sample space. Prove the following general version of the decomposition formula (4.20) in Proposition 4.24(a):

$$\Pr(E) = \sum_{i=1}^n \Pr(E | F_i) \Pr(F_i).$$

- (e) Prove a general version of Bayes's formula:

$$\Pr(F_i | E) = \frac{\Pr(E | F_i) \Pr(F_i)}{\Pr(E | F_1) \Pr(F_1) + \Pr(E | F_2) \Pr(F_2) + \dots + \Pr(E | F_n) \Pr(F_n)}.$$

Solution to Exercise 4.23.

(a)  $\Pr(E | E) = \frac{\Pr(E \cap E)}{\Pr(E)} = \frac{\Pr(E)}{\Pr(E)} = 1$ . It is clear that if we know that  $E$  occurs, then the probability that  $E$  occurs is 1.

(b)  $\Pr(F | E) = \frac{\Pr(F \cap E)}{\Pr(E)} = \frac{\Pr(\emptyset)}{\Pr(E)} = 0$ . If  $E$  occurs and  $F$  is disjoint from  $E$ , then none of the individual events in  $F$  can possibly occur, so the probability of  $F$  is clearly 0.

(c) One can argue directly by summing over the elements in the  $F_i$ 's or use induction on  $n$ , since we already know the formula for  $n = 2$ .

(d) The assumptions of  $F_1, \dots, F_n$  imply that

$$E = \bigcup_{i=1}^n (E \cap F_i) \quad \text{and} \quad (E \cap F_i) \cap (E \cap F_j) = \emptyset \quad \text{for } i \neq j.$$

Hence

$$\begin{aligned}
\Pr(E) &= \Pr\left(\bigcup_{i=1}^n (E \cap F_i)\right) \\
&= \sum_{i=1}^n \Pr(E \cap F_i) \quad \text{since the } E \cap F_i \text{ are disjoint from one another,} \\
&= \sum_{i=1}^n \Pr(E \mid F_i) \Pr(F_i).
\end{aligned}$$

**4.24.** There are two urns containing pens and pencils. Urn #1 contains three pens and seven pencils and Urn #2 contains eight pens and four pencils.

- (a) An urn is chosen at random and an object is drawn. What is the probability that it is a pencil?
- (b) An urn is chosen at random and an object is drawn. If the object drawn is a pencil, what is the probability that it came from Urn #1?
- (c) If an urn is chosen at random and two objects are drawn simultaneously, what is the probability that both are pencils?

Solution to Exercise 4.24.

Define events

$$\begin{aligned}
E &= \{\text{Urn \#1 is selected}\}, \\
F &= \{\text{A pencil is selected}\}.
\end{aligned}$$

- (a) We compute

$$\begin{aligned}
\Pr(F) &= \Pr(F \mid E) \Pr(E) + \Pr(F \mid E^c) \Pr(E^c) \\
&= \frac{7}{10} \cdot \frac{1}{2} + \frac{4}{12} \cdot \frac{1}{2} \\
&= \frac{31}{60} \approx 0.517.
\end{aligned}$$

- (b) We compute

$$\begin{aligned}
\Pr(E \mid F) &= \frac{\Pr(F \mid E) \Pr(E)}{\Pr(F)} && \text{Baye's law,} \\
&= \frac{(7/10) \cdot (1/2)}{31/60} && \text{using (a) to get } \Pr(F), \\
&= \frac{21}{31} \approx 0.677.
\end{aligned}$$

- (c) We need slightly different events, so we let

$$\begin{aligned}
E &= \{\text{Urn \#1 is selected}\}, \\
F &= \{\text{First item selected is a pencil}\}, \\
G &= \{\text{Second item selected is a pencil}\}.
\end{aligned}$$



Then

$$\Pr(F \text{ and } G) = \Pr(F) \Pr(G | F).$$

We already know  $\Pr(F) = 31/60$  from (a). To compute  $\Pr(G | F)$ , we do a calculation similar to the calculation in (a). Thus

$$\begin{aligned} \Pr(G | F) &= \Pr(G | F \& E) \Pr(F \& E) + \Pr(G | F \& E^c) \Pr(F \& E^c) \\ &= \Pr(G | F \& E) \Pr(F | E) \Pr(E) + \Pr(G | F \& E^c) \Pr(F | E^c) \Pr(E^c) \\ &= \frac{6}{9} \cdot \frac{7}{10} \cdot \frac{1}{2} + \frac{3}{11} \cdot \frac{4}{12} \cdot \frac{1}{2} \\ &= \frac{46}{165} \approx 0.279. \end{aligned}$$

**4.25.** An urn contains 20 silver coins and 10 gold coins. You are the sixth person in line to randomly draw and keep a coin from the urn.

- (a) What is the probability that you draw a gold coin?
- (b) If you draw a gold coin, what is the probability that the five people ahead of you all drew silver coins?

*Solution to Exercise 4.25.*

(a) It doesn't matter if you are the sixth to draw a coin, or the first, or the last, your chance of getting a gold coin is  $10/30$ , since there are 10 gold coins and 30 coins altogether. (If you had some information about the color of the coins drawn by the people ahead of you, that would change the answer, but the problem does not give you any such information.)

(b) This part is more difficult. We define events:

$$\begin{aligned} E &= \{\text{You draw a gold coin}\}, \\ F &= \{\text{Previous 5 people drew silver coins}\}. \end{aligned}$$

We want to compute  $\Pr(F | E)$  and we will use Baye's law in the form

$$\Pr(F | E) = \frac{\Pr(E | F) \Pr(F)}{\Pr(E)}.$$

As already explained,  $\Pr(E) = 1/3$ . Similarly, it is easy to compute  $\Pr(E | F)$ . The assumption that  $F$  is true means that when you draw your coin, the urn now contains 15 silver coins and 10 gold coins, so your probability of drawing a gold coin is  $\Pr(E | F) = 10/25 = 2/5$ .

Finally, to compute  $\Pr(F)$ , define events  $F_1, \dots, F_5$  by

$$F_i = \{\text{Person } \#i \text{ draws a silver coin}\}.$$

Then

$$\begin{aligned}
\Pr(F) &= \Pr(F_1 \& F_2 \& F_3 \& F_4 \& F_5) \\
&= \Pr(F_1) \cdot \Pr(F_2 \mid F_1) \cdot \Pr(F_3 \mid F_1 \& F_2) \cdot \Pr(F_4 \mid F_1 \& F_2 \& F_3) \\
&\quad \cdot \Pr(F_5 \mid F_1 \& F_2 \& F_3 \& F_4) \\
&= \frac{20}{30} \cdot \frac{19}{29} \cdot \frac{18}{28} \cdot \frac{17}{27} \cdot \frac{16}{26} \\
&= \frac{2584}{23751} \approx 0.109.
\end{aligned}$$

We now have the values needed to solve the problem:

$$\Pr(F \mid E) = \frac{\Pr(E \mid F) \Pr(F)}{\Pr(E)} = \frac{(2/5) \cdot (2584/23751)}{1/3} = \frac{5168}{39585} \approx 0.131.$$

Thus with no other knowledge, there is approximately an 11% chance that the first five coins chosen are silver, but if we know that the sixth coin chosen is gold, then the probability that the first five were silver increases to approximately 13%.

**4.26.** (*The Monty Hall Problem*) Monty Hall gives Dan, a contestant, the choice of three boxes. One box contains a valuable prize and the other two contain nothing. Dan chooses a box, but does not yet open it. Monty Hall then opens one of the other boxes, shows that it is empty, and offers Dan the option of keeping his original box or of switching it for the remaining box. The Monty Hall problem is to figure out Dan's best strategy: "To hold or to switch?"

The answer may depend on the strategy that Monty Hall employs in deciding which box to open when he has a choice, i.e., when Dan initially chooses the prize box and the other two boxes are empty. This problem considers various strategies. (We assume in all cases that Dan is aware of Monty Hall's chosen strategy.)

- (a) Suppose that when Monty Hall has a choice, he randomly opens one of the two empty boxes. Should Dan hold or switch, and what is his probability of winning?
- (b) Suppose that Monty Hall has mentally labeled the boxes 0, 1, and 2, and that if Dan chooses Box  $n$  and if the other two boxes are empty, then Monty Hall opens Box  $n + 1$ . (If  $n = 2$ , then he opens Box 0.) Should Dan hold or switch, and what is his probability of winning?
- (c) Again assume that Monty Hall has mentally labeled the boxes 0, 1, and 2, but now suppose that Monty Hall always opens the lowest-numbered empty box. What is Dan's best strategy and what is his probability of winning? (You may assume that the prize is placed in each box with equal probability.)
- (d) Same questions as in (b) and (c), except that Dan also knows how the boxes are labeled.
- (e) With the same assumptions as in (c), suppose that Dan employs his best strategy and that Monty Hall knows that Dan is employing this strategy.

Can Monty Hall hurt Dan's chances of winning by placing the prize in one box more often than the others? But if he does so and if Dan knows, can Dan do better by changing his strategy?

- (f) Suppose that we return to the scenario in (a), but we give Monty Hall another option, namely he can force Dan to keep the box that Dan initially chose. Now what is Dan's best strategy to win the prize and what is Monty Hall's best strategy to stop Dan?

Solution to Exercise 4.26.

*A solution for this exercise is not currently available.*

**4.27.** Let  $\mathcal{S}$  be a set, let  $A$  be a property of interest, and suppose that for  $m \in \mathcal{S}$ , we have  $\Pr(m \text{ has property } A) = \delta$ . Suppose further that a Monte Carlo algorithm applied to  $m$  and a random number  $r$  satisfy:

- (1) If the algorithm returns **Yes**, then  $m$  definitely has property  $A$ .
- (2) If  $m$  has property  $A$ , then the probability that the algorithm returns **Yes** is at least  $p$ .

Notice that we can restate (1) and (2) as conditional probabilities:

- (1)  $\Pr(m \text{ has property } A \mid \text{algorithm returns Yes}) = 1$ ,
- (2)  $\Pr(\text{algorithm returns Yes} \mid m \text{ has property } A) \geq p$ .

Suppose that we run the algorithm  $N$  times on the number  $m$ , and suppose that the algorithm returns **No** every single time. Derive a lower bound, in terms of  $\delta$ ,  $p$ , and  $N$ , for the probability that  $m$  does not have property  $A$ . (This generalizes the version of the Monte Carlo method that we studied in Section 4.3.3 with  $\delta = 0.01$  and  $p = \frac{1}{2}$ . Be careful to distinguish  $p$  from  $1 - p$  in your calculations.)

Solution to Exercise 4.27.

Let

$$E = \{\text{an element } m \in \mathcal{S} \text{ does not have property } A\}.$$

$$F = \{\text{the algorithm returns No } N \text{ times in a row}\}.$$

We want a lower bound for the conditional probability  $\Pr(E \mid F)$ , that is, the probability that  $m$  does not have property  $A$  despite the fact that the algorithm returned **No**  $N$  times. We compute this probability using Bayes's formula

$$\Pr(E \mid F) = \frac{\Pr(F \mid E) \Pr(E)}{\Pr(F \mid E) \Pr(E) + \Pr(F \mid E^c) \Pr(E^c)}.$$

We are given that the probability of have property  $A$  is  $\delta$ , so

$$\Pr(E) = \Pr(\text{not } A) = 1 - \delta \quad \text{and} \quad \Pr(E^c) = \Pr(A) = \delta.$$

Next consider  $\Pr(F \mid E)$ . If  $m$  does not have property  $A$ , which is our assumption on this conditional probability, then the algorithm always returns **No**, since Property (1) tells us that a **Yes** output forces  $m$  to have property  $A$ . Thus

$$\Pr(\text{No} \mid \text{not } A) = \Pr(A \mid \text{Yes}) = 1,$$

from which it follows that  $\Pr(F \mid E) = \Pr(\text{No} \mid \text{not } A)^N = 1$ .

Finally, we must compute the value of  $\Pr(F \mid E^c)$ . Since the algorithm is run  $N$  independent times, we have

$$\begin{aligned} \Pr(F \mid E^c) &= \Pr(\text{Output is No} \mid m \text{ has property } A)^N \\ &= (1 - \Pr(\text{Output is Yes} \mid m \text{ has property } A))^N \\ &\leq (1 - p)^N \quad \text{from Property (2) of the Monte Carlo method.} \end{aligned}$$

Substituting these values into Bayes's formula, we find that if the algorithm returns **No**  $N$  times in a row, then the probability that the integer  $m$  does not have property  $A$  is

$$\Pr(E \mid F) \geq \frac{1 \cdot (1 - \delta)}{1 \cdot (1 - \delta) + (1 - p)^N \cdot \delta} = \frac{1 - \delta}{1 - \delta + (1 - p)^N \cdot \delta}.$$

If  $\delta$  and  $p$  are not too small and  $N$  is large, this can be approximated by

$$\Pr(E \mid F) \geq 1 - \frac{(1 - p)^N \cdot \delta}{1 - \delta + (1 - p)^N \cdot \delta} \approx 1 - \frac{(1 - p)^N \cdot \delta}{1 - \delta} = 1 - \frac{(1 - p)^N}{\delta^{-1} - 1}.$$

**4.28.** We continue with the setup described in Exercise 4.27.

- Suppose that  $\delta = \frac{9}{10}$  and  $p = \frac{3}{4}$ . If we run the algorithm 25 times on the input  $m$  and always get back **No**, what is the probability that  $m$  does not have property  $A$ ?
- Same question as (a), but this time we run the algorithm 100 times.
- Suppose that  $\delta = \frac{99}{100}$  and  $p = \frac{1}{2}$ . How many times should we run the algorithm on  $m$  to be 99% confident that  $m$  does not have property  $A$ , assuming that every output is **No**?
- Same question as (c), except now we want to be 99.9999% confident.

Solution to Exercise 4.28.

*A solution for this exercise is not currently available.*

**4.29.** If an integer  $n$  is composite, then the Miller–Rabin test has at least a 75% chance of succeeding in proving that  $n$  is composite, while it never misidentifies a prime as being composite. (See Table 3.2 in Section 3.4 for a description of the Miller–Rabin test.) Suppose that we run the Miller–Rabin test  $N$  times on the integer  $n$  and that it fails to prove that  $n$  is composite. Show that the probability that  $n$  is prime satisfies (approximately)

$$\Pr(n \text{ is prime} \mid \text{the Miller-Rabin test fails } N \text{ times}) \geq 1 - \frac{\ln(n)}{4^N}.$$

(*Hint.* Use Exercise 4.27 with appropriate choices of  $A$ ,  $\mathcal{S}$ ,  $\delta$ , and  $p$ . You may also use the estimate from Section 3.4.1 that the probability that  $n$  is prime is approximately  $1/\ln(n)$ .)

Solution to Exercise 4.29.

In Exercise 4.27 we let  $A$  be the property of being composite and we let  $p = \frac{3}{4}$ , since we know that if  $n$  is composite, then the Miller-Rabin test returns **Yes** at least 75% of the time. Further, we have  $\delta \approx 1 - 1/\ln(n)$ , since  $\delta$  is the probability that  $n$  is composite, which is 1 minus the probability that it is prime. The solution to that exercise says that (approximately)

$$\begin{aligned} \Pr(n \text{ is prime} \mid \text{the Miller-Rabin test fails } N \text{ times}) \\ &\geq 1 - \frac{(1-p)^N}{\delta^{-1} - 1} \\ &\approx 1 - \frac{\ln(n) - 1}{4^N} \\ &\approx 1 - \frac{\ln(n)}{4^N}. \end{aligned}$$

**4.30.** Let  $f_X(k)$  be the binomial density function (4.23). Prove directly, using the binomial theorem, that  $\sum_{k=0}^n f_X(k) = 1$ .

Solution to Exercise 4.30.

Let  $q = 1 - p$ , so  $p + q = 1$ . Then we use the binomial theorem to compute

$$\sum_{k=0}^n f_X(k) = \sum_{k=0}^n \binom{n}{k} p^k (1-p)^{n-k} = \sum_{k=0}^n \binom{n}{k} p^k q^{n-k} = (p+q)^n = 1^n = 1.$$

**4.31.** In Example 4.37 we used a differentiation trick to compute the value of the infinite series  $\sum_{n=1}^{\infty} np(1-p)^{n-1}$ . This exercise further develops this useful technique. The starting point is the formula for the geometric series

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x} \quad \text{for } |x| < 1. \quad (4.1)$$

(a) Prove that

$$\sum_{n=1}^{\infty} nx^{n-1} = \frac{1}{(1-x)^2} \quad (4.2)$$

by differentiating both sides of (4.57) with respect to  $x$ . For which  $x$  does the left-hand side of (4.58) converge? (*Hint.* Use the ratio test.)

(b) Differentiate again to prove that

$$\sum_{n=2}^{\infty} n(n-1)x^{n-2} = \frac{2}{(1-x)^3}. \quad (4.3)$$

(c) More generally, prove that for every  $k \geq 0$ ,

$$\sum_{n=0}^{\infty} \binom{n+k}{k} x^n = \frac{1}{(1-x)^{k+1}}. \quad (4.4)$$

(Hint. Use induction on  $k$ .)

(d) Prove that

$$\sum_{n=0}^{\infty} n^2 x^n = \frac{x + x^2}{(1-x)^3}. \quad (4.5)$$

(Hint. Multiply (4.58) by  $x$  and (4.59) by  $x^2$  and then add them together.)

(e) Find a formula for

$$\sum_{n=0}^{\infty} n^3 x^n. \quad (4.6)$$

(f) Prove that for every value of  $k$  there is a polynomial  $F_k(x)$  such that

$$\sum_{n=0}^{\infty} n^k x^n = \frac{F_k(x)}{(1-x)^{k+1}}. \quad (4.7)$$

(Hint. Use induction on  $k$ .) Compute the polynomials  $F_0(x)$ ,  $F_1(x)$ , and  $F_2(x)$ .

(g) Prove that the polynomial  $F_k(x)$  in (f) has degree  $k$ .

Solution to Exercise 4.31.

(a) Term-by-term differentiation gives the formula. We compute

$$\rho = \lim_{n \rightarrow \infty} \frac{|(n+1)x^{n+1}|}{|nx^n|} = \lim_{n \rightarrow \infty} \frac{n+1}{n} |x| = |x|.$$

The ratio test tells us that the series converges for  $|x| < 1$  and diverges for  $|x| > 1$ . And the series clearly also diverges for  $|x| = 1$ .

(b) Term-by-term differentiation of (a) gives the formula.

(c) Differentiating  $k$  times gives

$$\sum_{n=0}^{\infty} n(n-1)(n-2) \cdots (n-k+1) x^{n-k} = \frac{1 \cdot 2 \cdot 3 \cdots k}{(1-x)^{k+1}}.$$

(If one wants to be formal, one can prove this formula by induction on  $k$ .) Now divide both sides by  $k!$  and use the definition of the combinatorial symbol to get

$$\sum_{n=k}^{\infty} \binom{n}{k} x^{n-k} = \frac{1}{(1-x)^{k+1}}.$$

(Notice that we only need to start the summation with  $n = k$ , since terms with  $n = 0, 1, \dots, k-1$  give 0.) Finally, in the summation on the left, replace  $n$  by  $n+k$ , so now the sum starts at  $n = 0$ . This gives

$$\sum_{n=0}^{\infty} \binom{n+k}{k} x^n = \frac{1}{(1-x)^{k+1}}.$$

(d) Following the hint, we first compute

$$x \sum_{n=1}^{\infty} n x^{n-1} + x^2 \sum_{n=2}^{\infty} n(n-1) x^{n-2} = \sum_{n=0}^{\infty} (n + n(n-1)) x^n = \sum_{n=0}^{\infty} n^2 x^n.$$

Then, according to our results in (a) and (b), this is also equal to

$$\frac{x}{(1-x)^2} + \frac{2x^2}{(1-x)^3} = \frac{x+x^2}{(1-x)^3}.$$

(e) One way to do this is to differentiate (b) and then combine various quantities to get the desired result. An easier method is to differentiate both sides of (d). Thus

$$\begin{aligned} \frac{d}{dx} \left( \sum_{n=0}^{\infty} n^2 x^n \right) &= \frac{d}{dx} \left( \frac{x+x^2}{(1-x)^3} \right) \\ \sum_{n=0}^{\infty} n^3 x^{n-1} &= \frac{1+4x+x^2}{(1-x)^4}. \end{aligned}$$

Multiplying both sides by  $x$  gives the desired result,

$$\sum_{n=0}^{\infty} n^3 x^n = \frac{x+4x^2+x^3}{(1-x)^4}.$$

(f, g) From the geometric series we have  $F_0(x) = 1$ , and (a) and (d) give  $F_1(x) = x$  and  $F_2(x) = x + x^2$ . Now assume that

$$\sum_{n=0}^{\infty} n^k x^n = \frac{F_k(x)}{(1-x)^{k+1}}$$

is true for  $k$ , where  $F_k(x)$  is a polynomial of degree  $k$ . Differentiating both sides and using the differentiation rule for quotients yields

$$\begin{aligned} \sum_{n=0}^{\infty} n^{k+1} x^{n-1} &= \frac{(1-x)^{k+1} F'_k(x) - (k+1)(1-x)^k (-1) F_k(x)}{(1-x)^{2k+2}} \\ &= \frac{(1-x) F'_k(x) + (k+1) F_k(x)}{(1-x)^{k+2}} \end{aligned}$$

Multiplying both sides by  $x$  gives

$$\sum_{n=0}^{\infty} n^{k+1} x^n = \frac{(x - x^2)F'_k(x) + (k+1)xF_k(x)}{(1-x)^{k+2}},$$

so the desired formula is true with

$$F_{k+1}(x) = (x - x^2)F'_k(x) + (k+1)xF_k(x).$$

Since the degree of  $F'_k(x)$  is one smaller than the degree of  $F_k(x)$ , we also see that

$$\deg F_{k+1}(x) = 1 + \deg F_k(x).$$

Since  $\deg F_0(x) = 0$ , we conclude that  $\deg F_k(x) = k$ .

**4.32.** In each case, compute the expectation of the random variable  $X$ .

- (a) The values of  $X$  are uniformly distributed on the set  $\{0, 1, 2, \dots, N-1\}$ . (See Example 4.28.)
- (b) The values of  $X$  are uniformly distributed on the set  $\{1, 2, \dots, N\}$ .
- (c) The values of  $X$  are uniformly distributed on the set  $\{1, 3, 7, 11, 19, 23\}$ .
- (d)  $X$  is a random variable with a binomial density function (see (4.23) on page 221).

Solution to Exercise 4.32.

(a)

$$\begin{aligned} E(X) &= 0 \cdot \frac{1}{N} + 1 \cdot \frac{1}{N} + 2 \cdot \frac{1}{N} + \cdots + (N-1) \cdot \frac{1}{N} \\ &= \frac{0 + 1 + 2 + \cdots + (N-1)}{N} \\ &= \frac{\frac{1}{2}(N-1)N}{N} \\ &= \frac{N-1}{2}. \end{aligned}$$

(b)

$$\begin{aligned} E(X) &= 1 \cdot \frac{1}{N} + 2 \cdot \frac{1}{N} + 3 \cdot \frac{1}{N} + \cdots + N \cdot \frac{1}{N} \\ &= \frac{1 + 2 + 3 + \cdots + N}{N} \\ &= \frac{\frac{1}{2}N(N+1)}{N} \\ &= \frac{N+1}{2}. \end{aligned}$$

(c)



$$E(X) = \frac{1 + 3 + 7 + 11 + 19 + 23}{6} = \frac{64}{6} = \frac{32}{3}.$$

(d)

$$\begin{aligned} E(X) &= \sum_{k=0}^n k \cdot f_X(k) \\ &= \sum_{k=0}^n k \binom{n}{k} p^k (1-p)^{n-k} \\ &= (1-p)^n \sum_{k=0}^n k \binom{n}{k} \left(\frac{p}{1-p}\right)^k. \end{aligned}$$

If we let  $x = p/(1-p)$ , then we need to compute the value of the sum

$$\sum_{k=0}^n k \binom{n}{k} x^k.$$

To do this, we start with the binomial theorem

$$\sum_{k=0}^n \binom{n}{k} x^k = (x+1)^n$$

and differentiate both sides with respect to  $x$  to get

$$\sum_{k=0}^n k \binom{n}{k} x^{k-1} = n(x+1)^{n-1}.$$

Now multiply both sides by  $x$  to get

$$\sum_{k=0}^n k \binom{n}{k} x^k = nx(x+1)^{n-1}.$$

This gives the value

$$E(X) = (1-p)^n \cdot n \cdot \frac{p}{1-p} \cdot \left(\frac{p}{1-p} + 1\right)^{n-1} = (1-p)^n \cdot n \cdot \frac{p}{1-p} \cdot \left(\frac{1}{1-p}\right)^{n-1} = np.$$

This makes sense, since if we perform the experiment  $n$  times and have a probability  $p$  of succeeding each time, we would expect to succeed, on average, a total of  $np$  times.

**4.33.** Let  $X$  be a random variable on the probability space  $\Omega$ . It might seem more natural to define the expected value of  $X$  by the formula

$$\sum_{\omega \in \Omega} X(\omega) \cdot \Pr(\omega). \quad (4.8)$$

Prove that the formula (4.64) gives the same value as equation (4.27) on page 225, which we used in the text to define  $E(X)$ .

Solution to Exercise 4.33.

We compute (the key step comes in the middle where we reverse the order of summation):

$$\begin{aligned}
 E(X) &= \sum_{i=1}^n x_i \cdot f_X(x_i) \\
 &= \sum_{i=1}^n x_i \cdot \Pr(X = x_i) \\
 &= \sum_{i=1}^n x_i \Pr\{\omega \in \Omega : X(\omega) = x_i\} \\
 &= \sum_{i=1}^n x_i \sum_{\substack{\omega \in \Omega \\ X(\omega) = x_i}} \Pr(\omega) \\
 &= \sum_{\omega \in \Omega} \Pr(\omega) \sum_{\substack{1 \leq i \leq n \\ x_i = X(\omega)}} x_i \\
 &= \sum_{\omega \in \Omega} \Pr(\omega) \cdot X(\omega),
 \end{aligned}$$

where for the final equality we use that fact that  $x_1, \dots, x_n$  are distinct, so each  $X(\omega)$  is equal to exactly one of the  $x_i$  values.

## Section. Collision algorithms and the birthday paradox

- 4.34.** (a) In a group of 23 strangers, what is the probability that at least two of them have the same birthday? How about if there are 40 strangers? In a group of 200 strangers, what is the probability that one of them has the same birthday as your birthday? (*Hint.* See the discussion in Section 4.4.1.)
- (b) Suppose that there are  $N$  days in a year (where  $N$  could be any number) and that there are  $n$  people. Develop a general formula, analogous to (4.28), for the probability that at least two of them have the same birthday. (*Hint.* Do a calculation similar to the proof of (4.28) in the collision theorem (Theorem 4.38), but note that the formula is a bit different because the birthdays are being selected from a single list of  $N$  days.)
- (c) Find a lower bound of the form

$$\Pr(\text{at least one match}) \geq 1 - e^{-(\text{some function of } n \text{ and } N)}$$

for the probability in (b), analogous to the estimate (4.29).

Solution to Exercise 4.34.

We start by doing (b).

$$\begin{aligned}
\Pr\left(\begin{array}{l} \text{at least one match} \\ \text{in } n \text{ attempts} \end{array}\right) &= 1 - \Pr\left(\begin{array}{l} \text{all } n \text{ birthdays} \\ \text{are different} \end{array}\right) \\
&= 1 - \prod_{i=1}^n \Pr\left(\begin{array}{l} i^{\text{th}} \text{ birthday is different} \\ \text{from all of the} \\ \text{previous } i-1 \text{ birthdays} \end{array}\right) \\
&= 1 - \prod_{i=1}^n \frac{N-(i-1)}{N} \\
&= 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{N}\right).
\end{aligned}$$

Then the answer to the first part of (a) is obtained by setting  $N = 365$  and  $n = 23$ , which gives

$$(a) \quad \Pr(\text{match}) = 1 - \prod_{i=1}^{22} \left(1 - \frac{i}{365}\right) \approx 50.73\%.$$

Similarly,  $N = 365$  and  $n = 40$  gives the answer to the second part of (a),

$$(b) \quad \Pr(\text{match}) = 1 - \prod_{i=1}^{39} \left(1 - \frac{i}{365}\right) \approx 89.12\%.$$

The final part of (a) is

$$\begin{aligned}
\Pr(\text{someone has your birthday}) &= 1 - \Pr(\text{no one has your birthday}) \\
&= 1 - \Pr(\text{one person does not have your birthday})^{200} \\
&= 1 - \left(\frac{364}{365}\right)^{200} \\
&\approx 42.23\%.
\end{aligned}$$

For (c) we use the lower bound  $e^{-x} \geq 1 - x$  with  $x = i/N$  to compute

$$\begin{aligned}
\Pr\left(\begin{array}{l} \text{at least one match} \\ \text{in } n \text{ attempts} \end{array}\right) &= 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{N}\right) \\
&\geq 1 - \prod_{i=1}^{n-1} e^{-i/N} \\
&= 1 - e^{-(1+2+\cdots+(n-1))/N} \\
&= 1 - e^{-(n-1)n/2N} \\
&\approx 1 - e^{-n^2/2N}.
\end{aligned}$$

Notice that we have used the well known formula

$$1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2}.$$

**4.35.** A deck of cards is shuffled and the top eight cards are turned over.

- (a) What is the probability that the king of hearts is visible?
- (b) A second deck is shuffled and its top eight cards are turned over. What is the probability that a visible card from the first deck matches a visible card from the second deck? (Note that this is slightly different from Example 4.39 because the cards in the second deck are not being replaced.)

Solution to Exercise 4.35.

*A solution for this exercise is not currently available.*

**4.36.** (a) Prove that

$$e^{-x} \geq 1 - x \quad \text{for all values of } x.$$

(*Hint.* Look at the graphs of  $e^{-x}$  and  $1 - x$ , or use calculus to compute the minimum of the function  $f(x) = e^{-x} - (1 - x)$ .)

- (b) Prove that for all  $a > 1$ , the inequality

$$e^{-ax} \leq (1 - x)^a + \frac{1}{2}ax^2 \quad \text{is valid for all } 0 \leq x \leq 1.$$

(This is a challenging problem.)

- (c) We used the inequality in (a) during the proof of the lower bound (4.29) in the collision theorem (Theorem 4.38). Use (b) to prove that

$$\Pr(\text{at least one red}) \leq 1 - e^{-mn/N} + \frac{mn^2}{2N^2}.$$

Thus if  $N$  is large and  $m$  and  $n$  are not much larger than  $\sqrt{N}$ , then the estimate

$$\Pr(\text{at least one red}) \approx 1 - e^{-mn/N}$$

is quite accurate. (*Hint.* Use (b) with  $a = m$  and  $x = n/N$ .)

Solution to Exercise 4.36.

(a) Let  $f(x) = e^{-x} - 1 + x$ . Then  $f(0) = f'(0) = 0$ . Then generalized mean value theorem says that

$$f(x) = f(0) + f'(0)x + \frac{1}{2}f''(z)x^2 \quad \text{for some } 0 \leq z \leq x,$$

so we find that  $f(x) = \frac{1}{2}e^{-z}x^2 \geq 0$ . This is the desired inequality.

- (b) Let

$$f(x) = (1 - x)^a + \frac{1}{2}ax^2 - e^{-ax}.$$

Since  $f(0) = 0$ , it suffices to prove that

$$f'(x) = -a(1-x)^{a-1} + ax + ae^{-ax}$$

is positive for  $0 < x < 1$ . We can divide by  $a$ , and for notational convenience, we let  $a = b + 1$ . So we need to prove that

$$g(x) = -(1-x)^b + x + e^{-(b+1)x}$$

is positive for  $0 < x < 1$  and  $b > 0$ .

From (a) we know that  $e^{-x} > 1 - x$ , so raising both sides to the  $b^{\text{th}}$  power and multiplying by  $-1$  gives

$$-(1-x)^b > -e^{-bx}.$$

Substituting this into  $g(x)$ , we find that

$$g(x) > -e^{-bx} + x + e^{-(b+1)x} = x - e^{-bx}(1 - e^{-x}).$$

It is clear that this last expression is increasing as  $b$  increases. (To be more formal, its derivative with respect to  $b$  is  $be^{-bx}(1 - e^{-x})$ , which is strictly positive for  $0 < x < 1$ .) Hence the expression is minimized when  $b = 0$ , so we get

$$g(x) > x - (1 - e^{-x}) = e^{-x} - (1 - x).$$

Using (a) again gives  $g(x) > 0$ .

Remark: It appears to be true numerically that  $f(x) \geq 0$  provided that  $a > 0.8526055\dots$ , where  $c = 0.8526055\dots$  is the unique real solution to  $ce^c = 2$ .

(c) We have

$$\begin{aligned} \Pr\left(\begin{array}{c} \text{at least} \\ \text{one red} \end{array}\right) &= 1 - \left(1 - \frac{n}{N}\right)^m && \text{from the Collision Theorem} \\ &\leq 1 - \left(e^{-mn/N} - \frac{mn^2}{2N^2}\right) && \text{use (b) with } a = m \text{ and } x = \frac{n}{N}. \end{aligned}$$

**4.37.** Solve the discrete logarithm problem  $10^x = 106$  in the finite field  $\mathbb{F}_{811}$  by finding a collision among the random powers  $10^i$  and  $106 \cdot 10^i$  that are listed in Table 4.17.

Solution to Exercise 4.37.

From Table 4.17 we see that

$$10^{234} = 106 \cdot 10^{399} = 304 \quad \text{in } \mathbb{F}_{811}.$$

Hence

$$10^{234} \cdot 10^{-399} = 10^{-165} = 10^{645} = 106 \quad \text{in } \mathbb{F}_{811}.$$

$i$	$h^i$	$a \cdot h^i$	$i$	$h^i$	$a \cdot h^i$	$i$	$h^i$	$a \cdot h^i$	$i$	$h^i$	$a \cdot h^i$
116	96	444	519	291	28	791	496	672	406	801	562
497	326	494	286	239	193	385	437	95	745	194	289
225	757	764	298	358	642	178	527	714	234	304	595
233	517	465	500	789	101	471	117	237	556	252	760
677	787	700	272	24	111	42	448	450	326	649	670
622	523	290	307	748	621	258	413	795	399	263	304

Table 4.12: Data for Exercise 4.37,  $h = 10$ ,  $a = 106$ ,  $p = 811$ Section. Pollard's  $\rho$  method

**4.38.** Table 4.18 gives some of the computations for the solution of the discrete logarithm problem

$$11^t = 41387 \quad \text{in } \mathbb{F}_{81799} \quad (4.9)$$

using Pollard's  $\rho$  method. (It is similar to Table 4.11 in Example 4.51.) Use the data in Table 4.18 to solve (4.65).

Solution to Exercise 4.38.

$$\begin{aligned}
 x_{308} &= x_{154} = 15386 \quad \text{in } \mathbb{F}_{81799}. \\
 \alpha_{154} &= 81756, \quad \beta_{154} = 9527, \quad \gamma_{154} = 67782, \quad \delta_{154} = 28637. \\
 11^{81756} \cdot 41387^{9527} &= 11^{67782} \cdot 41387^{28637} \quad \text{in } \mathbb{F}_{81799}. \\
 11^{13974} &= 41387^{19110} \quad \text{in } \mathbb{F}_{81799}. \\
 \gcd(19110, 81798) &= 6. \\
 81340 \cdot 19110 &\equiv 6 \pmod{81798}. \\
 11^{13974 \cdot 81340} &= 11^{1136645160} = 11^{61950} = 41387^6 \quad \text{in } \mathbb{F}_{81799}. \\
 \frac{61950}{6} &= 10325, \quad \frac{81798}{6} = 13633. \\
 \log_{11}(41387) &\in \{10325 + 13633 \cdot k : 0 \leq k < 6\} \\
 &= \{10325, 23958, 37591, 51224, 64857, 78490\}. \\
 11^{10325} &= 73192, \quad 11^{23958} = 40412, \quad 11^{37591} = 49019, \quad 11^{51224} = 8607, \\
 \boxed{11^{64857} = 41387}, \quad &11^{78490} = 32780.
 \end{aligned}$$

**4.39.** Table 4.19 gives some of the computations for the solution of the discrete logarithm problem

$$7^t = 3018 \quad \text{in } \mathbb{F}_{7963} \quad (4.10)$$

$i$	$x_i$	$y_i$	$\alpha_i$	$\beta_i$	$\gamma_i$	$\delta_i$
0	1	1	0	0	0	0
1	11	121	1	0	2	0
2	121	14641	2	0	4	0
3	1331	42876	3	0	12	2
4	14641	7150	4	0	25	4
$\vdots$						
151	4862	33573	40876	45662	29798	73363
152	23112	53431	81754	9527	37394	48058
153	8835	23112	81755	9527	67780	28637
154	15386	15386	81756	9527	67782	28637

Table 4.13: Computations to solve  $11^t = 41387$  in  $\mathbb{F}_{81799}$  for Exercise 4.38

using Pollard's  $\rho$  method. (It is similar to Table 4.11 in Example 4.51.) Extend Table 4.19 until you find a collision (we promise that it won't take too long) and then solve (4.66).

Solution to Exercise 4.39.

Extending the table:

$i$	$x_i$	$y_i$	$\alpha_i$	$\beta_i$	$\gamma_i$	$\delta_i$
87	1329	1494	6736	7647	3148	3904
88	1340	1539	6737	7647	3150	3904
89	1417	4767	6738	7647	6302	7808
90	1956	1329	6739	7647	4642	7655
91	5729	1417	6740	7647	4644	7655
92	2449	5729	6740	7648	4646	7655
93	1217	1217	6741	7648	4647	7656

$$\begin{aligned}
x_{186} &= x_{93} = 1217 \quad \text{in } \mathbb{F}_{7963}. \\
\alpha_{93} &= 6741, \quad \beta_{93} = 7648, \quad \gamma_{93} = 4647, \quad \delta_{93} = 7656. \\
7^{6741} \cdot 3018^{7648} &= 7^{4647} \cdot 3018^{7656} \quad \text{in } \mathbb{F}_{7963}. \\
7^{2094} &= 3018^8 \quad \text{in } \mathbb{F}_{7963}. \\
7^{2094} &= 3018^8 \quad \text{in } \mathbb{F}_{7963}. \\
\gcd(8, 7962) &= 2. \\
6967 \cdot 8 &\equiv 2 \pmod{7962}. \\
7^{2094 \cdot 6967} &= 7^{14588898} = 7^{2514} = 3018^2 \quad \text{in } \mathbb{F}_{7963}. \\
\frac{2514}{2} &= 1257, \quad \frac{7962}{2} = 3981. \\
\log_7(3018) &\in \{1257 + 3981 \cdot k : 0 \leq k < 2\} = \{1257, 5238\}. \\
7^{1257} &= 4945, \quad 7^{5238} = 3018.
\end{aligned}$$

$i$	$x_i$	$y_i$	$\alpha_i$	$\beta_i$	$\gamma_i$	$\delta_i$
0	1	1	0	0	0	0
1	7	49	1	0	2	0
2	49	2401	2	0	4	0
3	343	6167	3	0	6	0
4	2401	1399	4	0	7	1
$\vdots$						
87	1329	1494	6736	7647	3148	3904
88	1340	1539	6737	7647	3150	3904
89	1417	4767	6738	7647	6302	7808
90	1956	1329	6739	7647	4642	7655

Table 4.14: Computations to solve  $7^t = 3018$  in  $\mathbb{F}_{7963}$  for Exercise 4.39

**4.40.** Write a computer program implementing Pollard's  $\rho$  method for solving the discrete logarithm problem and use it to solve each of the following:

- (a)  $2^t = 2495$  in  $\mathbb{F}_{5011}$ .
- (b)  $17^t = 14226$  in  $\mathbb{F}_{17959}$ .
- (c)  $29^t = 5953042$  in  $\mathbb{F}_{15239131}$ .

*Solution to Exercise 4.40.*

- (a)  $\boxed{2^{3351} = 2495}.$
- (b)  $\boxed{17^{14557} = 14226}.$
- (c)  $\boxed{29^{2528453} = 5953042}.$



**4.41.** Evaluate the integral  $I = \int_0^\infty t^2 e^{-t^2/2} dt$  appearing in the proof of Theorem 4.47. (*Hint.* Write  $I^2$  as an iterated integral,

$$I^2 = \int_0^\infty \int_0^\infty x^2 e^{-x^2/2} \cdot y^2 e^{-y^2/2} dx dy,$$

and switch to polar coordinates.)

Solution to Exercise 4.41.

Following the hint, we have

$$\begin{aligned} I^2 &= \int_0^\infty \int_0^\infty x^2 e^{-x^2/2} y^2 e^{-y^2/2} dx dy \\ &= \int_0^\infty \int_0^\infty x^2 y^2 e^{-(x^2+y^2)/2} dx dy \\ &= \int_0^\infty \int_0^{\pi/2} (r \sin \theta)^2 (r \cos \theta)^2 e^{-r^2/2} r dr d\theta \\ &= \left( \int_0^{\pi/2} \sin^2 \theta \cos^2 \theta d\theta \right) \left( \int_0^\infty r^5 e^{-r^2/2} dr \right). \end{aligned}$$

Each of these integrals is now a moderately hard freshman calculus exercise. For the first one we can use

$$\sin^2 \theta \cos^2 \theta = (\sin \theta \cos \theta)^2 = \left( \frac{1}{2} \sin(2\theta) \right)^2 = \frac{1}{4} \cdot \frac{1 - \cos(4\theta)}{2}.$$

Then

$$\int_0^{\pi/2} \sin^2 \theta \cos^2 \theta d\theta = \int_0^{\pi/2} \frac{1 - \cos(4\theta)}{8} d\theta = \frac{\theta}{8} - \frac{\sin(4\theta)}{32} \Big|_0^{\pi/2} = \frac{\pi}{16}.$$

For the second integral we substitute  $r^2 = z$  and then integrate by parts twice. Thus

$$\begin{aligned} \int_0^\infty r^5 e^{-r^2/2} dr &= \int_0^\infty z^2 e^{-z/2} \frac{1}{2} dz \\ &= -z^2 e^{-z/2} \Big|_0^\infty + 2 \int_0^\infty z e^{-z/2} dz \\ &= 2 \int_0^\infty z e^{-z/2} dz \\ &= -4z e^{-z/2} \Big|_0^\infty + 4 \int_0^\infty e^{-z/2} dz \\ &= 4 \int_0^\infty e^{-z/2} dz \\ &= -8e^{-z/2} \Big|_0^\infty = 8. \end{aligned}$$

Hence  $I^2 = \pi/16 \cdot 8 = \pi/2$ , so  $I = \sqrt{\pi/2}$ .

## Section. Information theory

**4.42.** Consider the cipher that has three keys, three plaintexts, and four ciphertexts that are combined using the following encryption table (which is similar to Table 4.12 used in Example 4.53 on page 246).

	$m_1$	$m_2$	$m_3$
$k_1$	$c_2$	$c_4$	$c_1$
$k_2$	$c_1$	$c_3$	$c_2$
$k_3$	$c_3$	$c_1$	$c_2$

Suppose further that the plaintexts and keys are used with the following probabilities:

$$f(m_1) = f(m_2) = \frac{2}{5}, \quad f(m_3) = \frac{1}{5}, \quad f(k_1) = f(k_2) = f(k_3) = \frac{1}{3}.$$

- Compute  $f(c_1)$ ,  $f(c_2)$ ,  $f(c_3)$ , and  $f(c_4)$ .
- Compute  $f(c_1 | m_1)$ ,  $f(c_1 | m_2)$ , and  $f(c_1 | m_3)$ . Does this cryptosystem have perfect secrecy?
- Compute  $f(c_2 | m_1)$  and  $f(c_3 | m_1)$ .
- Compute  $f(k_1 | c_3)$  and  $f(k_2 | c_3)$ .

Solution to Exercise 4.42.

*A solution for this exercise is not currently available.*

**4.43.** Suppose that a shift cipher is employed such that each key, i.e., each shift amount from 0 to 25, is used with equal probability and such that a new key is chosen to encrypt each successive letter. Show that this cryptosystem has perfect secrecy by filling in the details of the following steps.

- Show that  $\sum_{k \in \mathcal{K}} f_M(d_k(c)) = 1$  for every ciphertext  $c \in \mathcal{C}$ .
- Compute the ciphertext density function  $f_C$  using the formula

$$f_C(c) = \sum_{k \in \mathcal{K}} f_K(k) f_M(d_k(c)).$$

- Compare  $f_C(c)$  to  $f_{C|M}(c | m)$ .

Solution to Exercise 4.43.

*A solution for this exercise is not currently available.*

**4.44.** Suppose that a cryptosystem has the same number of plaintexts as it does ciphertexts ( $\#\mathcal{M} = \#\mathcal{C}$ ). Prove that for any given key  $k \in \mathcal{K}$  and any given ciphertext  $c \in \mathcal{C}$ , there is a unique plaintext  $m \in \mathcal{M}$  that encrypts to  $c$  using the key  $k$ . (We used this fact during the proof of Theorem 4.55. Notice that the proof does not require the cryptosystem to have perfect secrecy; all that is needed is that  $\#\mathcal{M} = \#\mathcal{C}$ .)

Solution to Exercise 4.44.

Fix  $k \in \mathcal{K}$ . The encryption map  $e_k : \mathcal{M} \rightarrow \mathcal{C}$  is injective by definition of a cryptosystem, so our assumption that  $\#\mathcal{M} = \#\mathcal{C}$  implies that  $e_k$  is also surjective, and hence is a bijective map from  $\mathcal{M}$  to  $\mathcal{C}$ . This is equivalent to the assertion that for every  $c \in \mathcal{C}$ , there is a unique  $m \in \mathcal{M}$  satisfying  $e_k(m) = c$ , which is the desired result.

**4.45.** Let  $\mathcal{S}_{m,c} = \{k \in \mathcal{K} : e_k(m) = c\}$  be the set used during the proof of Theorem 4.55. Prove that if  $c \neq c'$ , then  $\mathcal{S}_{m,c} \cap \mathcal{S}_{m,c'} = \emptyset$ . (Prove this for any cryptosystem; it is not necessary to assume perfect secrecy.)

Solution to Exercise 4.45.

Suppose that  $k \in \mathcal{S}_{m,c} \cap \mathcal{S}_{m,c'}$ . Then  $c = e_k(m) = c'$ . Hence  $\mathcal{S}_{m,c} \cap \mathcal{S}_{m,c'} \neq \emptyset$  implies that  $c = c'$ .

**4.46.** Suppose that a cryptosystem satisfies  $\#\mathcal{K} = \#\mathcal{M} = \#\mathcal{C}$  and that it has perfect secrecy. Prove that every ciphertext is used with equal probability and that every plaintext is used with equal probability. (*Hint.* We proved one of these during the course of proving Theorem 4.55. The proof of the other is similar.)

Solution to Exercise 4.46.

*A solution for this exercise is not currently available.*

**4.47.** Prove the “only if” part of Theorem 4.55, i.e., prove that if a cryptosystem with an equal number of keys, plaintexts, and ciphertexts satisfies conditions (a) and (b) of Theorem 4.55, then it has perfect secrecy.

Solution to Exercise 4.47.

*A solution for this exercise is not currently available.*

**4.48.** Let  $X$  be an experiment (random variable) with outcomes  $x_1, \dots, x_n$  occurring with probabilities  $p_1, \dots, p_n$ , and similarly let  $Y$  be an experiment with outcomes  $y_1, \dots, y_m$  occurring with probabilities  $q_1, \dots, q_m$ . Consider the experiment  $Z$  consisting of first performing  $X$  and then performing  $Y$ . Thus the outcomes of  $Z$  are the  $mn$  pairs  $(x_i, y_j)$  occurring with probabilities  $p_i q_j$ . Use the formula for entropy (4.51) to prove that

$$H(Z) = H(X) + H(Y).$$

Thus entropy is additive on independent compound events, which is a special case of Property **H**<sub>3</sub> on page 250.

Solution to Exercise 4.48.

Using the formula for entropy, we compute

$$\begin{aligned}
H(Z) &= - \sum_{i=1}^n \sum_{j=1}^m p_i q_j \log(p_i q_j) \\
&= - \sum_{i=1}^n \sum_{j=1}^m p_i q_j (\log p_i + \log q_j) \\
&= - \sum_{i=1}^m p_i \log p_i \sum_{j=1}^n q_j - \sum_{i=1}^n p_i \sum_{j=1}^m q_j \log q_j \\
&= H(X) \cdot 1 + 1 \cdot H(Y).
\end{aligned}$$

**4.49.** Let  $F(t)$  be a twice differentiable function with the property that  $F''(t) < 0$  for all  $x$  in its domain. Prove that  $F$  is concave in the sense of (4.52). Conclude in particular that the function  $F(t) = \log t$  is concave for all  $t > 0$ .

Solution to Exercise 4.49.

*A solution for this exercise is not currently available.*

**4.50.** Use induction to prove Jensen's inequality (Theorem 4.59).

Solution to Exercise 4.50.

The case  $n = 2$  is true by definition of concavity. Assume now that it is true for  $n$ . The idea is to combine two of the terms in the sum  $\alpha_1 t_1 + \cdots + \alpha_n t_n + \alpha_{n+1} t_{n+1}$  into one term, say the last two. In other words, we want to write

$$\alpha_n t_n + \alpha_{n+1} t_{n+1} \quad \text{as} \quad \beta_n y_n,$$

but we need to make sure that  $\alpha_1 + \alpha_2 + \cdots + \alpha_{n-1} + \beta_n = 1$ . So we need to take  $\beta_n = \alpha_n + \alpha_{n+1}$ , which means that we need to take

$$y_n = \frac{\alpha_n t_n + \alpha_{n+1} t_{n+1}}{\alpha_n + \alpha_{n+1}}.$$

With this choice of  $\beta_n$  and  $y_n$ , we have  $\alpha_1 + \cdots + \alpha_{n-1} + \beta_n = 1$ , so we can apply the induction hypothesis to conclude that

$$f(\alpha_1 t_1 + \cdots + \alpha_{n-1} t_{n-1} + \beta_n y_n) \leq \alpha_1 f(t_1) + \cdots + \alpha_{n-1} f(t_{n-1}) + \beta_n f(y_n).$$

We are also going to apply the induction hypothesis to  $f(y_n)$ . We can write  $y_n$  as

$$y_n = \frac{\alpha_n}{\alpha_n + \alpha_{n+1}} t_n + \frac{\alpha_{n+1}}{\alpha_n + \alpha_{n+1}} t_{n+1} = \gamma t_n + \delta t_{n+1},$$

where notice that  $\gamma$  and  $\delta$  satisfy  $\gamma + \delta = 1$ . Hence the induction hypothesis tells us that

$$f(y_n) = f(\gamma t_n + \delta t_{n+1}) \leq \gamma f(t_n) + \delta f(t_{n+1}).$$

Now multiplying both sides by  $\beta_n$  and substituting in the values  $\gamma$ ,  $\delta$ , and  $\beta_n$  yields

$$\beta_n f(y_n) \leq \beta_n \gamma f(t_n) + \beta_n \delta f(t_{n+1}) = \alpha_n f(t_n) + \alpha_{n+1} f(t_{n+1}).$$

Finally, substituting this in above gives the desired inequality

$$f(\alpha_1 t_1 + \cdots + \alpha_n t_n + \alpha_{n+1} t_{n+1}) \leq \alpha_1 f(t_1) + \cdots + \alpha_n f(t_n) + \alpha_{n+1} f(t_{n+1}).$$

The induction proof that there is equality if and only if all of the  $t_i$ 's are equal is similar.

**4.51.** Let  $X$  and  $Y$  be independent random variables.

- (a) Prove that the equivocation  $H(X | Y)$  is equal to the entropy  $H(X)$ .
- (b) If  $H(X | Y) = H(X)$ , is it necessarily true that  $X$  and  $Y$  are independent?

Solution to Exercise 4.51.

Independence means that  $f(x | y) = f(x)$ , so

$$\begin{aligned} H(X | Y) &= - \sum_{x,y} f(y) f(x | y) \log f(x | y) \\ &= - \sum_{x,y} f(y) f(x) \log f(x) \\ &= - \sum_y f(y) \sum_x f(x) \log f(x) \\ &= 1 \cdot H(X). \end{aligned}$$

For the converse, notice that

$$\begin{aligned} H(X) &= - \sum_x f(x) \log f(x) \\ &= - \sum_x \left( \sum_y f(x, y) \right) \log f(x) \\ &= - \sum_{x,y} f(y) f(x | y) \log f(x), \end{aligned}$$

so

$$\begin{aligned} H(X) - H(X | Y) &= - \sum_{x,y} f(y) f(x | y) \log \frac{f(x)}{f(x | y)} \\ &= - \sum_{x,y} f(x, y) \log \frac{f(x) f(y)}{f(x, y)}. \end{aligned}$$

It is likely that one could come up with dependent random variables  $X$  and  $Y$  making this quantity vanish.

**4.52.** Suppose a cryptosystem has two keys,  $\mathcal{K} = \{k_1, k_2\}$ , each of which is equally likely to be used, and suppose that it has three plaintexts  $\mathcal{M} = \{m_1, m_2, m_3\}$  that occur with probabilities  $f(m_1) = \frac{1}{2}$ ,  $f(m_2) = \frac{1}{4}$ , and  $f(m_3) = \frac{1}{4}$ .

- (a) Create an encryption function for this cipher, similar to Example 4.53, such that there are three ciphertexts  $\mathcal{C} = \{c_1, c_2, c_3\}$  and such that the ciphertext  $c_1$  occurs with probability  $\frac{1}{2}$ . (There is more than one correct answer to this problem.)
- (b) Compute the entropies  $H(K)$ ,  $H(M)$ , and  $H(C)$  of your encryption scheme in (a).
- (c) Compute the key equivocation  $H(K | C)$ .
- (d) Use your answer in (c) to explain why each ciphertext leaks information.

Solution to Exercise 4.52.

*A solution for this exercise is not currently available.*

**4.53.** Suppose that the key equivocation of a certain cryptosystem vanishes, i.e., suppose that  $H(K | C) = 0$ . Prove that even a single observed ciphertext uniquely determines which key was used.

Solution to Exercise 4.53.

*A solution for this exercise is not currently available.*

**4.54.** Write a computer program that reads a text file and performs the following tasks:

- [1] Convert all alphabetic characters to lowercase and convert all strings of consecutive nonalphabetic characters to a single space. (The reason for leaving in a space is that when you count bigrams and trigrams, you will want to know where words begin and end.)
- [2] Count the frequency of each letter a-to-z, print a frequency table, and use your frequency table to estimate the entropy of a single letter in English, as we did in Section 4.6.3 using Table 1.3.
- [3] Count the frequency of each bigram aa, ab, ..., zz, being careful to include only bigrams that appear within words. (As an alternative, also allow bigrams that either start or end with a space, in which case there are  $27^2 - 1 = 728$  possible bigrams.) Print a frequency table of the 25 most common bigrams and their probabilities, and use your full frequency table to estimate the entropy of bigrams in English. In the notation of Section 4.6.3, this is the quantity  $H(L^2)$ . Compare  $\frac{1}{2}H(L^2)$  with the value of  $H(L)$  from step [1].
- [4] Repeat [3], but this time with trigrams. Compare  $\frac{1}{3}H(L^3)$  with the values of  $H(L)$  and  $\frac{1}{2}H(L^2)$  from [2] and [3]. (Note that for this part, you will need a large quantity of text in order to get some reasonable frequencies.)

Try running your program on some long blocks of text. For example, the following noncopyrighted material is available in the form of ordinary text files from Project Gutenberg at <http://www.gutenberg.net/>. To what extent

are the letter frequencies similar and to what extent do they differ in these different texts?

- (a) *Alice's Adventures in Wonderland* by Lewis Carroll,  
<http://www.gutenberg.net/etext/11>
- (b) *Relativity: the Special and General Theory* by Albert Einstein,  
<http://www.gutenberg.net/etext/5001>
- (c) The Old Testament (translated from the original Hebrew, of course!),  
<http://www.gutenberg.net/etext/1609>
- (d) *20000 Lieues Sous Les Mers* (20000 Leagues Under the Sea) by Jules Verne, <http://www.gutenberg.net/etext/5097>. Note that this one is a little trickier, since first you will need to convert all of the letters to their unaccented forms.

## Chapter 5

# Elliptic Curves and Cryptography

### Exercises for Chapter 5

Section. Elliptic curves

**5.1.** Let  $E$  be the elliptic curve  $E : Y^2 = X^3 - 2X + 4$  and let  $P = (0, 2)$  and  $Q = (3, -5)$ . (You should check that  $P$  and  $Q$  are on the curve  $E$ .)

- (a) Compute  $P \oplus Q$ .
- (b) Compute  $P \oplus P$  and  $Q \oplus Q$ .
- (c) Compute  $P \oplus P \oplus P$  and  $Q \oplus Q \oplus Q$ .

Solution to Exercise 5.1.

- (a)  $P \oplus Q = (22/9, 100/27)$ .
- (b)  $P \oplus P = Q \oplus Q = (1/4, -15/8)$ .
- (c)  $P \oplus P \oplus P = (240, 3718)$  and  $Q \oplus Q \oplus Q = (-237/121, -845/1331)$ .

**5.2.** Check that the points  $P = (-1, 4)$  and  $Q = (2, 5)$  are points on the elliptic curve  $E : Y^2 = X^3 + 17$ .

- (a) Compute the points  $P \oplus Q$  and  $P \ominus Q$ .
- (b) Compute the points  $2P$  and  $2Q$ .

(*Bonus.* How many points with integer coordinates can you find on  $E$ ?)

Solution to Exercise 5.2.

- (a)  $P + Q = (-\frac{8}{9}, -\frac{109}{27})$  and  $P - Q = (8, 23)$ .
- (b)  $2P = (\frac{137}{64}, -\frac{2651}{512})$  and  $2Q = (-\frac{64}{25}, \frac{59}{125})$

*Bonus.* This curve has 16 points with integer coordinates, including one that is quite large. This is somewhat surprising number. The points are  $(-2, \pm 3)$ ,  $(-1, \pm 4)$ ,  $(2, \pm 5)$ ,  $(4, \pm 9)$ ,  $(8, \pm 23)$ ,  $(43, \pm 282)$ ,  $(52, \pm 375)$ ,  $(5234, \pm 378661)$ . There are no others, but that's not so easy to prove.



**5.3.** Suppose that the cubic polynomial  $X^3 + AX + B$  factors as

$$X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3).$$

Prove that  $4A^3 + 27B^2 = 0$  if and only if two (or more) of  $e_1$ ,  $e_2$ , and  $e_3$  are the same. (*Hint.* Multiply out the right-hand side and compare coefficients to relate  $A$  and  $B$  to  $e_1$ ,  $e_2$ , and  $e_3$ .)

Solution to Exercise 5.3.

We have

$$X^3 + AX + B = X^3 - (e_1 + e_2 + e_3)X^2 + (e_1e_2 + e_1e_3 + e_2e_3)X - e_1e_2e_3,$$

and comparing the coefficients gives three relations

$$\begin{aligned} e_1 + e_2 + e_3 &= 0, \\ e_1e_2 + e_1e_3 + e_2e_3 &= A, \\ e_1e_2e_3 &= B. \end{aligned}$$

Suppose first that two of the  $e_i$  are the same, say  $e_2 = e_3$ . Then we get

$$e_1 + 2e_2 = 0, \quad 2e_1e_2 + e_2^2 = A, \quad e_1e_2^2 = B.$$

So  $e_1 = -2e_2$ , and substituting this into the second and third equations gives

$$-3e_2^2 = A \quad \text{and} \quad -2e_2^3 = B.$$

Hence

$$4A^3 + 27B^2 = 4(-3e_2^2)^3 + 27(-2e_2^3)^2 = 0.$$

Conversely, suppose that  $4A^3 + 27B^2 = 0$ . Substituting the expressions for  $A$  and  $B$  from above and multiplying it out gives the rather complicated expression

$$\begin{aligned} 4A^3 + 27B^2 &= (4e_2^3 + 12e_3e_2^2 + 12e_3^2e_2 + 4e_3^3)e_1^3 + (12e_3e_2^3 + 51e_3^2e_2^2 + 12e_3^3e_2)e_1^2 \\ &\quad + (12e_3^2e_2^3 + 12e_3^3e_2^2)e_1 \\ &\quad + 4e_3^3e_2^3. \end{aligned}$$

Next we substitute  $e_1 = -e_2 - e_3$  to get

$$4A^3 + 27B^2 = -4e_2^6 - 12e_3e_2^5 + 3e_3^2e_2^4 + 26e_3^3e_2^3 + 3e_3^4e_2^2 - 12e_3^5e_2 - 4e_3^6.$$

We'd like to know that this last expression vanishes if any two of the  $e_i$  are the same. It is not hard to check that it is a multiple of  $e_2 - e_3$ , and indeed a multiple of  $(e_2 - e_3)^2$ . But we'd also like it to vanish when  $e_3 = e_1$ , which is the same as when  $e_3 = -e_2 - e_3$ . So we check and find that the expression is divisible by  $e_2 + 2e_3$ , and in fact it is divisible by  $(e_2 + 2e_3)^2$ . Similarly, it is divisible by  $(e_3 + 2e_2)^2$ . So we find that

$$4A^3 + 27B^2 = -(e_2 - e_3)^2(e_2 + 2e_3)^2(e_3 + 2e_2)^2.$$

Hence using the fact that  $e_1 + e_2 + e_3 = 0$ , we find that

$$4A^3 + 27B^2 \text{ if and only if } (e_2 - e_3)^2(e_1 - e_3)^2(e_1 - e_2)^2 = 0,$$

**5.4.** Sketch each of the following curves, as was done in Figure 5.1 on page 280.

(a)  $E : Y^2 = X^3 - 7X + 3.$

(b)  $E : Y^2 = X^3 - 7X + 9.$

(c)  $E : Y^2 = X^3 - 7X - 12.$

(d)  $E : Y^2 = X^3 - 3X + 2.$

(e)  $E : Y^2 = X^3.$

Notice that the curves in (d) and (e) have  $\Delta_E = 0$ , so they are not elliptic curves. How do their pictures differ from the pictures in (a), (b), and (c)? Each of the curves (d) and (e) has one point that is somewhat unusual. These unusual points are called *singular points*.

**Section. Elliptic curves over finite fields**

**5.5.** For each of the following elliptic curves  $E$  and finite fields  $\mathbb{F}_p$ , make a list of the set of points  $E(\mathbb{F}_p)$ .

(a)  $E : Y^2 = X^3 + 3X + 2$  over  $\mathbb{F}_7$ .

(b)  $E : Y^2 = X^3 + 2X + 7$  over  $\mathbb{F}_{11}$ .

(c)  $E : Y^2 = X^3 + 4X + 5$  over  $\mathbb{F}_{11}$ .

(d)  $E : Y^2 = X^3 + 9X + 5$  over  $\mathbb{F}_{11}$ .

(e)  $E : Y^2 = X^3 + 9X + 5$  over  $\mathbb{F}_{13}$ .

Solution to Exercise 5.5.

(a)  $\#E(\mathbb{F}_7) = 9$

$$E(\mathbb{F}_7) = \{\mathcal{O}, (0, 3), (0, 4), (2, 3), (2, 4), (4, 1), (4, 6), (5, 3), (5, 4)\}$$

(b)  $\#E(\mathbb{F}_{11}) = 7$

$$E(\mathbb{F}_{11}) = \{\mathcal{O}, (6, 2), (6, 9), (7, 1), (7, 10), (10, 2), (10, 9)\}$$

(c)  $\#E(\mathbb{F}_{11}) = 8$

$$E(\mathbb{F}_{11}) = \{\mathcal{O}, (0, 4), (0, 7), (3, 0), (6, 5), (6, 6), (9, 0), (10, 0)\}$$

(d)  $\#E(\mathbb{F}_{11}) = 14$

$$E(\mathbb{F}_{11}) = \{\mathcal{O}, (0, 4), (0, 7), (1, 2), (1, 9), (2, 3), (2, 8), (3, 2), (3, 9), (6, 0), (7, 2), (7, 9), (9, 1), (9, 10)\}$$

(e)  $\#E(\mathbb{F}_{13}) = 9$

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (4, 1), (4, 12), (8, 2), (8, 11), (9, 3), (9, 10), (10, 4), (10, 9)\}$$

**5.6.** Make an addition table for  $E$  over  $\mathbb{F}_p$ , as we did in Table 5.1.

(a)  $E : Y^2 = X^3 + X + 2$  over  $\mathbb{F}_5$ .

(b)  $E : Y^2 = X^3 + 2X + 3$  over  $\mathbb{F}_7$ .

(c)  $E : Y^2 = X^3 + 2X + 5$  over  $\mathbb{F}_{11}$ .

You may want to write a computer program for (c), since  $E(\mathbb{F}_{11})$  has a lot of points!

*Solution to Exercise 5.6.*

(a)  $E(\mathbb{F}_5) = \{\mathcal{O}, (1, 2), (1, 3), (4, 0)\}$ .

	$\mathcal{O}$	(1, 2)	(1, 3)	(4, 0)
$\mathcal{O}$	$\mathcal{O}$	(1, 2)	(1, 3)	(4, 0)
(1, 2)	(1, 2)	(4, 0)	$\mathcal{O}$	(1, 3)
(1, 3)	(1, 3)	$\mathcal{O}$	(4, 0)	(1, 2)
(4, 0)	(4, 0)	(1, 3)	(1, 2)	$\mathcal{O}$

(b)  $E(\mathbb{F}_7) = \{\mathcal{O}, (2, 1), (2, 6), (3, 1), (3, 6), (6, 0)\}$ .

	$\mathcal{O}$	(2, 1)	(2, 6)	(3, 1)	(3, 6)	(6, 0)
$\mathcal{O}$	$\mathcal{O}$	(2, 1)	(2, 6)	(3, 1)	(3, 6)	(6, 0)
(2, 1)	(2, 1)	(3, 6)	$\mathcal{O}$	(2, 6)	(6, 0)	(3, 1)
(2, 6)	(2, 6)	$\mathcal{O}$	(3, 1)	(6, 0)	(2, 1)	(3, 6)
(3, 1)	(3, 1)	(2, 6)	(6, 0)	(3, 6)	$\mathcal{O}$	(2, 1)
(3, 6)	(3, 6)	(6, 0)	(2, 1)	$\mathcal{O}$	(3, 1)	(2, 6)
(6, 0)	(6, 0)	(3, 1)	(3, 6)	(2, 1)	(2, 6)	$\mathcal{O}$

(c)  $E(\mathbb{F}_{11}) = \{\mathcal{O}, (0, 4), (0, 7), (3, 4), (3, 7), (4, 0), (8, 4), (8, 7), (9, 2), (9, 9)\}$ .

	$\mathcal{O}$	(0, 4)	(0, 7)	(3, 4)	(3, 7)	(4, 0)	(8, 4)	(8, 7)	(9, 2)	(9, 9)
$\mathcal{O}$	$\mathcal{O}$	(0, 4)	(0, 7)	(3, 4)	(3, 7)	(4, 0)	(8, 4)	(8, 7)	(9, 2)	(9, 9)
(0, 4)	(0, 4)	(9, 2)	$\mathcal{O}$	(8, 7)	(9, 9)	(8, 4)	(3, 7)	(4, 0)	(3, 4)	(0, 7)
(0, 7)	(0, 7)	$\mathcal{O}$	(9, 9)	(9, 2)	(8, 4)	(8, 7)	(4, 0)	(3, 4)	(0, 4)	(3, 7)
(3, 4)	(3, 4)	(8, 7)	(9, 2)	(8, 4)	$\mathcal{O}$	(9, 9)	(0, 7)	(3, 7)	(4, 0)	(0, 4)
(3, 7)	(3, 7)	(9, 9)	(8, 4)	$\mathcal{O}$	(8, 7)	(9, 2)	(3, 4)	(0, 4)	(0, 7)	(4, 0)
(4, 0)	(4, 0)	(8, 4)	(8, 7)	(9, 9)	(9, 2)	$\mathcal{O}$	(0, 4)	(0, 7)	(3, 7)	(3, 4)
(8, 4)	(8, 4)	(3, 7)	(4, 0)	(0, 7)	(3, 4)	(0, 4)	(9, 2)	$\mathcal{O}$	(9, 9)	(8, 7)
(8, 7)	(8, 7)	(4, 0)	(3, 4)	(3, 7)	(0, 4)	(0, 7)	$\mathcal{O}$	(9, 9)	(8, 4)	(9, 2)
(9, 2)	(9, 2)	(3, 4)	(0, 4)	(4, 0)	(0, 7)	(3, 7)	(9, 9)	(8, 4)	(8, 7)	$\mathcal{O}$
(9, 9)	(9, 9)	(0, 7)	(3, 7)	(0, 4)	(4, 0)	(3, 4)	(8, 7)	(9, 2)	$\mathcal{O}$	(8, 4)

**5.7.** Let  $E$  be the elliptic curve

$$E : y^2 = x^3 + x + 1.$$

Compute the number of points in the group  $E(\mathbb{F}_p)$  for each of the following primes:

(a)  $p = 3$ .      (b)  $p = 5$ .      (c)  $p = 7$ .      (d)  $p = 11$ .

In each case, also compute the trace of Frobenius

$$t_p = p + 1 - \#E(\mathbb{F}_p)$$

and verify that  $|t_p|$  is smaller than  $2\sqrt{p}$ .

*Solution to Exercise 5.7.*

$p$	$\#E(\mathbb{F}_p)$	$t_p$	$2\sqrt{p}$
3	4	0	3.46
5	9	-3	4.47
7	5	3	5.29
11	14	-2	6.63
13	18	-4	7.21
17	18	0	8.25

Section. The elliptic curve discrete logarithm problem

**5.8.** Let  $E$  be the elliptic curve

$$E : y^2 = x^3 + x + 1$$

and let  $P = (4, 2)$  and  $Q = (0, 1)$  be points on  $E$  modulo 5. Solve the elliptic curve discrete logarithm problem for  $P$  and  $Q$ , that is, find a positive integer  $n$  such that  $Q = nP$ .

*Solution to Exercise 5.8.*

We compute the multiples of  $P$ :

$$\begin{aligned} P = (4, 2), \quad 2P = (3, 4), \quad 3P = (2, 4), \quad 4P = (0, 4), \quad \boxed{5P = (0, 1)} \\ 6P = (2, 1), \quad 7P = (3, 1), \quad 8P = (4, 3), \quad 9P = \mathcal{O}. \end{aligned}$$

Thus  $\log_P(Q) = 5$  in  $E(\mathbb{F}_5)$ . It turns out that  $E(\mathbb{F}_5)$  contains 9 points, and the multiples of  $P$  give all of them.

**5.9.** Let  $E$  be an elliptic curve over  $\mathbb{F}_p$  and let  $P$  and  $Q$  be points in  $E(\mathbb{F}_p)$ . Assume that  $Q$  is a multiple of  $P$  and let  $n_0 > 0$  be the smallest solution to  $Q = nP$ . Also let  $s > 0$  be the smallest solution to  $sP = \mathcal{O}$ . Prove that every solution to  $Q = nP$  looks like  $n_0 + is$  for some  $i \in \mathbb{Z}$ . (*Hint.* Write  $n$  as  $n = is + r$  for some  $0 \leq r < s$  and determine the value of  $r$ .)

*Solution to Exercise 5.9.*

Following the hint, we write  $n$  as  $n = is + r$  for some  $0 \leq r < s$ . Then

$$Q = nP = (is + r)P = i(sP) + rP = i\mathcal{O} + rP = rP,$$

since by definition  $sP = \mathcal{O}$ . But  $n_0P$  is the smallest multiple of  $P$  that is equal to  $Q$ , so we must have  $r \geq n_0$ . If  $r = n_0$ , we're done, so suppose instead that  $r > n_0$ .

Then

$$\mathcal{O} = Q - Q = rP - n_0P = (r - n_0)P,$$

and we know that  $sP$  is the smallest (nonzero) multiple of  $P$  that is equal to  $\mathcal{O}$ , so  $r - n_0 \geq s$ . But this contradicts  $r < s$ . Hence  $r = n_0$ , which proves that  $n = is + n_0$ .

**5.10.** Use the double-and-add algorithm (Table 5.3) to compute  $nP$  in  $E(\mathbb{F}_p)$  for each of the following curves and points, as we did in Figure 5.4.

- (a)  $E : Y^2 = X^3 + 23X + 13$ ,  $p = 83$ ,  $P = (24, 14)$ ,  $n = 19$ ;
- (b)  $E : Y^2 = X^3 + 143X + 367$ ,  $p = 613$ ,  $P = (195, 9)$ ,  $n = 23$ ;
- (c)  $E : Y^2 = X^3 + 1828X + 1675$ ,  $p = 1999$ ,  $P = (1756, 348)$ ,  $n = 11$ ;
- (d)  $E : Y^2 = X^3 + 1541X + 1335$ ,  $p = 3221$ ,  $P = (2898, 439)$ ,  $n = 3211$ .

Solution to Exercise 5.10.

(a) Solution:  $19 * (24, 14) = (24, 69)$ .

Step $i$	$n$	$Q = 2^i P$	$R$
0	19	(24, 14)	$\mathcal{O}$
1	9	(30, 8)	(24, 14)
2	4	(24, 69)	(30, 75)
3	2	(30, 75)	(30, 75)
4	1	(24, 14)	(30, 75)
5	0	(30, 8)	(24, 69)

Compute  $19 \cdot (24, 14)$  on  $Y^2 = X^3 + 23X + 13$  modulo 83.

(b) Solution:  $23 * (195, 9) = (485, 573)$ .

Step $i$	$n$	$Q = 2^i P$	$R$
0	23	(195, 9)	$\mathcal{O}$
1	11	(407, 428)	(195, 9)
2	5	(121, 332)	(182, 355)
3	2	(408, 110)	(194, 565)
4	1	(481, 300)	(194, 565)
5	0	(401, 150)	(485, 573)

Compute  $23 \cdot (195, 9)$  on  $Y^2 = X^3 + 143X + 367$  modulo 613

(c) Solution:  $11 * (1756, 348) = (1068, 1540)$ .

Step $i$	$n$	$Q = 2^i P$	$R$
0	11	(1756, 348)	$\mathcal{O}$
1	5	(1526, 1612)	(1756, 348)
2	2	(1657, 1579)	(1362, 998)
3	1	(1849, 225)	(1362, 998)
4	0	(586, 959)	(1068, 1540)

Compute  $11 \cdot (1756, 348)$  on  $Y^2 = X^3 + 1828X + 1675$  modulo 1999

(d) Solution:  $3211 * (2898, 439) = (243, 1875)$ .

Step $i$	$n$	$Q = 2^i P$	$R$
0	3211	(2898, 439)	$\mathcal{O}$
1	1605	(2964, 2977)	(2898, 439)
2	802	(1372, 2349)	(781, 2494)
3	401	(2956, 1288)	(781, 2494)
4	200	(1045, 1606)	(341, 1727)
5	100	(770, 285)	(341, 1727)
6	50	(2589, 1698)	(341, 1727)
7	25	(2057, 2396)	(341, 1727)
8	12	(1017, 828)	(2117, 1162)
9	6	(1988, 1949)	(2117, 1162)
10	3	(1397, 1477)	(2117, 1162)
11	1	(420, 1274)	(2362, 757)
12	0	(2583, 2597)	(243, 1875)

Compute  $3211 \cdot (2898, 439)$  on  $Y^2 = X^3 + 1541X + 1335$  modulo 3221

**5.11.** Convert the proof of Proposition 5.18 into an algorithm and use it to write each of the following numbers  $n$  as a sum of positive and negative powers of 2 with at most  $\frac{1}{2}[\log n] + 1$  nonzero terms. Compare the number of nonzero terms in the binary expansion of  $n$  with the number of nonzero terms in the ternary expansion of  $n$ .

(a) 349. (b) 9337. (c) 38728. (d) 8379483273489.

Solution to Exercise 5.11.

(a) Binary expansion has 6 terms. Ternary expansion has 5 terms.

$$\begin{aligned} 349 &= +2^1 + 2^3 + 2^4 + 2^5 + 2^7 + 2^9 \\ &= +2^1 - 2^3 - 2^6 - 2^8 + 2^{10} \end{aligned}$$

(b) Binary expansion has 7 terms. Ternary expansion has 5 terms.

$$\begin{aligned} 9337 &= +2^1 + 2^4 + 2^5 + 2^6 + 2^7 + 2^{11} + 2^{14} \\ &= +2^1 - 2^4 + 2^8 + 2^{11} + 2^{14} \end{aligned}$$

(c) Binary expansion has 7 terms. Ternary expansion has 6 terms.

$$\begin{aligned} 38728 &= +2^4 + 2^7 + 2^9 + 2^{10} + 2^{11} + 2^{13} + 2^{16} \\ &= +2^4 + 2^7 - 2^9 - 2^{12} + 2^{14} + 2^{16} \end{aligned}$$

(d) Binary expansion has 21 terms. Ternary expansion has 10 terms.

$$\begin{aligned} 8379483273489 &= +2^1 + 2^5 + 2^9 + 2^{12} + 2^{13} + 2^{14} + 2^{16} + 2^{17} + 2^{18} + 2^{19} \\ &\quad + 2^{20} + 2^{21} + 2^{33} + 2^{34} + 2^{35} + 2^{36} + 2^{37} + 2^{40} + 2^{41} \\ &\quad + 2^{42} + 2^{43} \\ &= +2^1 + 2^5 + 2^9 - 2^{12} - 2^{15} + 2^{22} - 2^{33} + 2^{38} - 2^{40} + 2^{44} \end{aligned}$$

**5.12.** In Section 4.5 we gave an abstract description of Pollard's  $\rho$  method, and in Section 4.5.2 we gave an explicit version to solve the discrete logarithm problem in  $\mathbb{F}_p$ . Adapt this material to create a Pollard  $\rho$  algorithm to solve the ECDLP.

*Solution to Exercise 5.12.*

We want to find  $n$  so that  $Q = nP$ , where  $P, Q \in E(\mathbb{F}_p)$  are given. We also assume that we know an integer  $N$  such that  $NP = \mathcal{O}$  and  $NQ = \mathcal{O}$ . For example, we can take  $N = \#E(\mathbb{F}_p)$ . To apply Pollard's method, we need a function  $f : E(\mathbb{F}_p) \rightarrow E(\mathbb{F}_p)$  that mixes up the points reasonably well. Following the ideas from Section 4.5.2, we define

$$f : E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_p), \quad f(T) = \begin{cases} P + T & \text{if } 0 \leq x_T < p/3, \\ 2T & \text{if } p/3 \leq x_T < 2p/3, \\ Q + T & \text{if } 2p/3 \leq x_T < p. \end{cases}$$

Then after  $i$  steps, we have

$$f^i(\mathcal{O}) = \alpha_i P + \beta_i Q \quad \text{and} \quad f^{2i}(\mathcal{O}) = \gamma_i P + \delta_i Q$$

for certain integer values of  $\alpha_i, \beta_i, \gamma_i, \delta_i$ . We can keep track of the values of  $\alpha_i, \beta_i, \gamma_i, \delta_i$  just as we did in Section 4.5.2. Note that the values of  $\alpha_i, \beta_i, \gamma_i, \delta_i$  should be computed modulo  $N$ , which prevents them from getting too big.

After  $\mathcal{O}(\sqrt{N})$  steps, we expect to find a match

$$f^i(\mathcal{O}) = f^{2i}(\mathcal{O}).$$

This means that

$$(\alpha_i - \gamma_i)P = (\delta_i - \beta_i)Q \quad \text{in } E(\mathbb{F}_p).$$

If  $\gcd(\delta_i - \beta_i, N) = 1$ , we can multiply both sides by

$$(\delta_i - \beta_i)^{-1} \bmod N$$

to express  $Q$  as a multiple of  $P$ . More generally, we can use the same sort of calculation described in Section 4.5.2 to find  $\gcd(\delta_i - \beta_i, N)$  possible values of  $n$ , and then we can test each of them to see if  $nP$  is equal to  $Q$ . (In practice,  $N$  will be prime, or at worst a small multiple of a large prime, so there will be few cases to check.)

**Section. Elliptic curve cryptography**

**5.13.** Alice and Bob agree to use elliptic Diffie–Hellman key exchange with the prime, elliptic curve, and point

$$p = 2671, \quad E : Y^2 = X^3 + 171X + 853, \quad P = (1980, 431) \in E(\mathbb{F}_{2671}).$$

- (a) Alice sends Bob the point  $Q_A = (2110, 543)$ . Bob decides to use the secret multiplier  $n_B = 1943$ . What point should Bob send to Alice?
- (b) What is their secret shared value?
- (c) How difficult is it for Eve to figure out Alice's secret multiplier  $n_A$ ? If you know how to program, use a computer to find  $n_A$ .
- (d) Alice and Bob decide to exchange a new piece of secret information using the same prime, curve, and point. This time Alice sends Bob only the  $x$ -coordinate  $x_A = 2$  of her point  $Q_A$ . Bob decides to use the secret multiplier  $n_B = 875$ . What single number modulo  $p$  should Bob send to Alice, and what is their secret shared value?

Solution to Exercise 5.13.

(a) Bob sends  $B = g^b = 2^{871} \equiv 805 \pmod{1373}$  to Alice. Their shared value (a) Bob sends the point  $Q_B = 1943P = \boxed{(1432, 667)} \in E(\mathbb{F}_{2671})$  to Alice.

(b) Their secret shared value is the  $x$ -coordinate  $\boxed{x=2424}$  of the point

$$n_B Q_A = 1943(2110, 543) = (2424, 911) \in E(\mathbb{F}_{2671}).$$

(c) By hand, it takes a long time to find  $n_A$ . But  $p$  is small enough that it's not too hard on a computer. Alice's secret value was  $n_A = 2045$ , but it turns out that the point  $P$  has order 1319, so in the smallest value that works is  $\boxed{n_A = 726}$ , since  $726P = (2110, 543) = Q_A \in E(\mathbb{F}_{2671})$ .

(d) Bob computes  $Q_B = 875P = (161, 2040) \in E(\mathbb{F}_{2671})$ , but he sends Alice only the  $x$ -coordinate  $\boxed{x_B = 161}$ . In order to find the shared value, Bob computes

$$\begin{aligned} y_A^2 &= x_A^3 + 171x_A + 853 = 2^3 + 171 \cdot 2 + 853 = 1203, \\ y_A &= 1203^{(2671+1)/4} = 1203^{668} \equiv 2575 \pmod{2671}, \\ n_B(x_A, y_A) &= 875(2, 2575) = (1708, 1419) \in E(\mathbb{F}_{2671}). \end{aligned}$$

The shared value is the  $x$ -coordinate  $\boxed{x = 1708}$ .

**5.14.** Exercise 2.10 on page 107 describes a multistep public key cryptosystem based on the discrete logarithm problem for  $\mathbb{F}_p$ . Describe a version of this cryptosystem that uses the elliptic curve discrete logarithm problem. (You may assume that Alice and Bob know the order of the point  $P$  in the group  $E(\mathbb{F}_p)$ , i.e., they know the smallest integer  $N \geq 1$  with the property that  $NP = \mathcal{O}$ .)

Solution to Exercise 5.14.

*A solution for this exercise is not currently available.*

**5.15.** A shortcoming of using an elliptic curve  $E(\mathbb{F}_p)$  for cryptography is the fact that it takes two coordinates to specify a point in  $E(\mathbb{F}_p)$ . However, as discussed briefly at the end of Section 5.4.2, the second coordinate actually conveys very little additional information.



- (a) Suppose that Bob wants to send Alice the value of a point  $R \in E(\mathbb{F}_p)$ . Explain why it suffices for Bob to send Alice the  $x$ -coordinate of  $R = (x_R, y_R)$  together with the single bit

$$\beta_R = \begin{cases} 0 & \text{if } 0 \leq y_R < \frac{1}{2}p, \\ 1 & \text{if } \frac{1}{2}p < y_R < p. \end{cases}$$

(You may assume that Alice is able to efficiently compute square roots modulo  $p$ . This is certainly true, for example, if  $p \equiv 3 \pmod{4}$ ; see Proposition 2.27.)

- (b) Alice and Bob decide to use the prime  $p = 1123$  and the elliptic curve

$$E : Y^2 = X^3 + 54X + 87.$$

Bob sends Alice the  $x$ -coordinate  $x = 278$  and the bit  $\beta = 0$ . What point is Bob trying to convey to Alice? What about if instead Bob had sent  $\beta = 1$ ?

Solution to Exercise 5.15.

(a) Alice computes  $x_R^3 + Ax_R + B$ . This quantity has two square roots, say  $b$  and  $p - b$ . One of  $b$  or  $p - b$  is between 0 and  $\frac{1}{2}p$ , the other is between  $\frac{1}{2}p$  and  $p$ . So the value of  $\beta_R$  tells Alice exactly which square root to take for  $y_R$ .

(b) First compute  $u = 278^3 + 54 \cdot 278 + 87 \equiv 216 \pmod{1123}$ . Then compute  $u^{(1123+1)/4} \equiv 487 \pmod{1123}$ . So the two possible points are  $(278, 487)$  and  $(278, 636)$ , since  $636 = 1123 - 487$ . From the way that  $\beta$  is chosen, we have

$$\boxed{\beta = 0 \implies R = (278, 487)} \quad \text{and} \quad \boxed{\beta = 1 \implies R = (278, 636)}$$

**5.16.** The Menezes–Vanstone variant of the elliptic ElGamal public key cryptosystem improves message expansion while avoiding the difficulty of directly attaching plaintexts to points in  $E(\mathbb{F}_p)$ . The MV-ElGamal cryptosystem is described in Table 5.12 on page 343.

- (a) The last line of Table 5.12 claims that  $m'_1 = m_1$  and  $m'_2 = m_2$ . Prove that this is true, so the decryption process does work.  
 (b) What is the message expansion of MV-ElGamal?  
 (c) Alice and Bob agree to use

$$p = 1201, \quad E : Y^2 = X^3 + 19X + 17, \quad P = (278, 285) \in E(\mathbb{F}_p),$$

for MV-ElGamal. Alice's secret value is  $n_A = 595$ . What is her public key? Bob sends Alice the encrypted message  $((1147, 640), 279, 1189)$ . What is the plaintext?

Solution to Exercise 5.16.

(a) Suppose that Bob has encrypted the plaintext  $(m_1, m_2)$  using the random number  $k$  as described in Table 5.12 and that he sends Alice his ciphertext  $(R, c_1, c_2)$ . Alice's first step is to compute  $T = n_A R$ . However, using the definition of  $R$ ,  $S$  and  $Q_A$ , we see that Alice is actually computing

$$T = n_A R = n_A(kP) = k(n_A P) = kQ_A = S.$$

Thus  $x_S = x_T$  and  $y_S = y_T$ , so Alice's second step yields

$$\begin{aligned} m'_1 &\equiv x_T^{-1} c_1 \equiv x_S^{-1}(x_S m_1) \equiv m_1 \pmod{p}, \\ m'_2 &\equiv y_T^{-1} c_2 \equiv y_S^{-1}(y_S m_2) \equiv m_2 \pmod{p}. \end{aligned}$$

This shows that Alice recovers Bob's plaintext. Notice how she uses her secret multiplier  $n_A$  during the decryption process.

(b) The plaintext  $(m_1, m_2)$  consists of two numbers modulo  $p$ . The ciphertext  $(R, c_1, c_2)$  consists of four numbers modulo  $p$ , since  $R$  has two coordinates. So the message expansion ratio is  $\boxed{2\text{-to-1}}$ . This can be improved if Bob sends only the  $x$ -coordinate of  $R$ , plus one extra bit to enable Alice to determine the correct  $y$ -coordinate. In that case, the cipher text is three numbers modulo  $p$  (plus one bit), so the message expansion ratio is approximately  $\boxed{3\text{-to-2}}$ .

(c) Alice public key is  $Q_A = n_A P = 595 \cdot (278, 285) = \boxed{(1104, 492)}$ . To decrypt, Alice computes  $T = n_A(1147, 640) = 595(1147, 640) = (942, 476)$ . She then computes  $x_T^{-1} c_1 = 941^{-1} \cdot 279 \equiv 509 \pmod{1201}$  and  $y_T^{-1} c_2 = 476^{-1} \cdot 1189 \equiv 767 \pmod{1201}$ . So the plaintext is  $\boxed{(509, 767)}$ .

**5.17.** This exercise continues the discussion of the MV-ElGamal cryptosystem described in Table 5.12 on page 343.

- (a) Eve knows the elliptic curve  $E$  and the ciphertext values  $c_1$  and  $c_2$ . Show how Eve can use this knowledge to write down a polynomial equation (modulo  $p$ ) that relates the two pieces  $m_1$  and  $m_2$  of the plaintext. In particular, if Eve can figure out one piece of the plaintext, then she can recover the other piece by finding the roots of a certain polynomial modulo  $p$ .
- (b) Alice and Bob exchange a message using MV-ElGamal with the prime, elliptic curve, and point in Exercise 5.16(c). Eve intercepts the ciphertext  $((269, 339), 814, 1050)$  and, through other sources, she discovers that the first part of the plaintext is  $m_1 = 1050$ . Use your algorithm in (a) to recover the second part of the plaintext.

Solution to Exercise 5.17.

- (a) Eve knows the equation of the elliptic curve,

$$E : Y^2 = X^3 + AX + B.$$

The coordinates of the point  $S \in E(\mathbb{F}_p)$  satisfy

$$x_S \equiv m_1^{-1}c_1 \pmod{p},$$

$$y_S \equiv m_2^{-1}c_2 \pmod{p},$$

and the point  $(x_S, y_S)$  satisfies the equation for  $E$ , so Eve knows that

$$(m_2^{-1}c_2)^2 \equiv (m_1^{-1}c_1)^3 + A(m_1^{-1}c_1) + B \pmod{p}.$$

Eve clears denominators by multiplying by  $m_1^3m_2^2$ , so

$$c_2^2m_1^3 \equiv c_1^3m_2^2 + Ac_1m_1^2m_2^2 + Bm_1^3m_2^2 \pmod{p}.$$

Thus  $(m_1, m_2)$  is a solution to the congruence

$$c_2^2u^3 \equiv c_1^3v^2 + Ac_1u^2v^2 + Bu^3v^2 \pmod{p},$$

so in particular, if Eve knows either  $m_1$  or  $m_2$ , then she can find the other one by substituting in the known value and finding the roots modulo  $p$  of the resulting polynomial.

(b)  $m_2 = 179$ . A solution for this exercise is not currently available.

**Section. Lenstra's elliptic curve factorization algorithm**

**5.18.** Use the elliptic curve factorization algorithm to factor each of the numbers  $N$  using the given elliptic curve  $E$  and point  $P$ .

- (a)  $N = 589$ ,  $E : Y^2 = X^3 + 4X + 9$ ,  $P = (2, 5)$ .  
 (b)  $N = 26167$ ,  $E : Y^2 = X^3 + 4X + 128$ ,  $P = (2, 12)$ .  
 (c)  $N = 1386493$ ,  $E : Y^2 = X^3 + 3X - 3$ ,  $P = (1, 1)$ .  
 (d)  $N = 28102844557$ ,  $E : Y^2 = X^3 + 18X - 453$ ,  $P = (7, 4)$ .

Solution to Exercise 5.18.

(a)

$n$	$n! \cdot P \bmod 589$
1	$P = (2, 5)$
2	$2! \cdot P = (564, 156)$
3	$3! \cdot P = (33, 460)$
4	$4! \cdot P = (489, 327)$

Factorial multiples of  $P$  on  $Y^2 = X^3 + 4X + 9$  modulo 589

Computation of  $5! \cdot P$  gives  $589 = 19 \cdot 31$ .

(b)

$n$	$n! \cdot P \bmod 26167$
1	$P = (2, 12)$
2	$2! \cdot P = (23256, 1930)$
3	$3! \cdot P = (21778, 1960)$
4	$4! \cdot P = (22648, 14363)$
5	$5! \cdot P = (5589, 11497)$
6	$6! \cdot P = (7881, 16198)$

Public Parameter Creation	
A trusted party chooses and publishes a (large) prime $p$ , an elliptic curve $E$ over $\mathbb{F}_p$ , and a point $P$ in $E(\mathbb{F}_p)$ .	
Alice	Bob
Key Creation	
Chooses a secret multiplier $n_A$ . Computes $Q_A = n_A P$ . Publishes the public key $Q_A$ .	
Encryption	
	Chooses plaintext values $m_1$ and $m_2$ modulo $p$ . Chooses a random number $k$ . Computes $R = kP$ . Computes $S = kQ_A$ and writes it as $S = (x_S, y_S)$ . Sets $c_1 \equiv x_S m_1 \pmod{p}$ and $c_2 \equiv y_S m_2 \pmod{p}$ . Sends ciphertext $(R, c_1, c_2)$ to Alice.
Decryption	
Computes $T = n_A R$ and writes it as $T = (x_T, y_T)$ . Sets $m'_1 \equiv x_T^{-1} c_1 \pmod{p}$ and $m'_2 \equiv y_T^{-1} c_2 \pmod{p}$ . Then $m'_1 = m_1$ and $m'_2 = m_2$ .	

Table 5.1: Menezes–Vanstone variant of ElGamal (Exercises 5.16, 5.17)

Factorial multiples of  $P$  on  $Y^2 = X^3 + 4X + 128$  modulo 26167.  
Computation of  $7! \cdot P$  gives  $26167 = 191 \cdot 137$ .

(c)

$n$	$n! \cdot P \bmod 1386493$
1	$P = (1, 1)$
2	$2! \cdot P = (7, 1386474)$
3	$3! \cdot P = (1059434, 60521)$
4	$4! \cdot P = (81470, 109540)$
5	$5! \cdot P = (870956, 933849)$
6	$6! \cdot P = (703345, 474777)$
7	$7! \cdot P = (335675, 1342927)$
8	$8! \cdot P = (1075584, 337295)$
9	$9! \cdot P = (149824, 1003869)$
10	$10! \cdot P = (92756, 1156933)$

Factorial multiples of  $P$  on  $Y^2 = X^3 + 3X - 3$  modulo 1386493  
 Computation of  $11! \cdot P$  gives  $1386493 = 1069 \cdot 1297$ .

(d)

$n$	$n! \cdot P \bmod 28102844557$
1	$P = (7, 4)$
2	$2! \cdot P = (1317321250, 11471660625)$
3	$3! \cdot P = (15776264786, 10303407105)$
4	$4! \cdot P = (27966589703, 26991329662)$
5	$5! \cdot P = (11450520276, 14900134804)$
$\vdots$	$\vdots$
24	$24! \cdot P = (25959867777, 9003083411)$
25	$25! \cdot P = (10400016599, 11715538594)$
26	$26! \cdot P = (22632202481, 6608272585)$
27	$27! \cdot P = (25446531195, 2223850203)$
28	$28! \cdot P = (12412875644, 7213676617)$

Factorial multiples of  $P$  on  $Y^2 = X^3 + 18X + 28102844104$  modulo  
 28102844557.

Computation of  $29! \cdot P$  gives  $28102844557 = 117763 \cdot 238639$ .

Section. Elliptic curves over  $\mathbb{F}_2$  and over  $\mathbb{F}_{2^k}$

**5.19.** Let  $E$  be an elliptic curve given by a generalized Weierstrass equation

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Let  $P_1 = (x_1, y_1)$  and  $P_2 = (x_2, y_2)$  be points on  $E$ . Prove that the following algorithm computes their sum  $P_3 = P_1 + P_2$ .

First, if  $x_1 = x_2$  and  $y_1 + y_2 + a_1x_2 + a_3 = 0$ , then  $P_1 + P_2 = \mathcal{O}$ .

Otherwise define quantities  $\lambda$  and  $\nu$  as follows:

$$\begin{aligned} \text{[If } x_1 \neq x_2] \quad \lambda &= \frac{y_2 - y_1}{x_2 - x_1}, & \nu &= \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, \\ \text{[If } x_1 = x_2] \quad \lambda &= \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \nu &= \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}. \end{aligned}$$

Then

$$P_3 = P_1 + P_2 = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3).$$

Solution to Exercise 5.19.

This is proven in any basic text on elliptic curves. See for example Group Law Algorithm 2.3 in [123, §2.2].

**5.20.** Let  $\mathbb{F}_8 = \mathbb{F}_2[T]/(T^3 + T + 1)$  be as in Example 5.28, and let  $E$  be the elliptic curve

$$E : Y^2 + XY + Y = X^3 + TX + (T + 1).$$

- (a) Calculate the discriminant of  $E$ .  
 (b) Verify that the points

$$P = (1 + T + T^2, 1 + T), \quad Q = (T^2, T), \quad R = (1 + T + T^2, 1 + T^2),$$

are in  $E(\mathbb{F}_8)$  and compute the values of  $P + Q$  and  $2R$ .

- (c) Find all of the points in  $E(\mathbb{F}_8)$ .  
 (d) Find a point  $P \in E(\mathbb{F}_8)$  such that every point in  $E(\mathbb{F}_8)$  is a multiple of  $P$ .

*Solution to Exercise 5.20.*

- (a)  $\Delta = 1 + T^2$ .  
 (b)  $P + Q = (1 + T + T^2, 1 + T^2)$  and  $2R = (T^2, T)$ .  
 (c, d) The point  $P = (1 + T + T^2, 1 + T^2)$  satisfies

$$\begin{aligned} P &= (1 + T + T^2, 1 + T^2) \\ 2P &= (T^2, T) \\ 3P &= (1, 0) \\ 4P &= (T^2, 1 + T + T^2) \\ 5P &= (1 + T + T^2, 1 + T) \\ 6P &= \mathcal{O}, \end{aligned}$$

and this is the complete set of points in  $E(\mathbb{F}_8)$ . (One can check this directly, or note that if there were more points, since the order of an element divides the order of a group, it would follow that  $\#E(\mathbb{F}_8)$  is at least 12, which contradicts the Hasse bound of  $8 + 1 + 2\sqrt{8} \approx 11.83$ .) The multiples of the point  $5P$  also give all of  $\#E(\mathbb{F}_8)$ .

**5.21.** Let  $\tau(\alpha) = \alpha^p$  be the Frobenius map on  $\mathbb{F}_{p^k}$ .

- (a) Prove that

$$\tau(\alpha + \beta) = \tau(\alpha) + \tau(\beta) \quad \text{and} \quad \tau(\alpha \cdot \beta) = \tau(\alpha) \cdot \tau(\beta) \quad \text{for all } \alpha, \beta \in \mathbb{F}_{p^k}.$$

(*Hint.* For the addition formula, use the binomial theorem (Theorem 4.10).)

- (b) Prove that  $\tau(\alpha) = \alpha$  for all  $\alpha \in \mathbb{F}_p$ .  
 (c) Let  $E$  be an elliptic curve over  $\mathbb{F}_p$  and let  $\tau(x, y) = (x^p, y^p)$  be the Frobenius map from  $E(\mathbb{F}_{p^k})$  to itself. Prove that

$$\tau(P + Q) = \tau(P) + \tau(Q) \quad \text{for all } P \in E(\mathbb{F}_{p^k}).$$

**5.22.** Let  $E_0$  be the Koblitz curve  $Y^2 + XY = X^3 + 1$  over the field  $\mathbb{F}_2$ , and for every  $k \geq 1$ , let

$$t_k = 2^k + 1 - \#E(\mathbb{F}_{2^k}).$$

- (a) Prove that  $t_1 = -1$  and  $t_2 = -3$ .

- (b) Prove that  $t_k$  satisfies the recursion

$$t_k = t_1 t_{k-1} - p t_{k-2} \quad \text{for all } t \geq 3.$$

(You may use the formula (5.12) that we stated, but did not prove, on page 313.)

- (c) Use the recursion in (b) to compute  $\#E(\mathbb{F}_{16})$ .  
 (d) Program a computer to calculate the recursion and use it to compute the values of  $\#E(\mathbb{F}_{2^{11}})$ ,  $\#E(\mathbb{F}_{2^{31}})$ , and  $\#E(\mathbb{F}_{2^{101}})$ .

Solution to Exercise 5.22.

- (a) A solution for this exercise is not currently available.  
 (b) A solution for this exercise is not currently available.  
 (c)  $\#E(\mathbb{F}_{16}) = 16$ .  
 (d)  $\#E(\mathbb{F}_{2^{11}}) = 2116$ .  
 $\#E(\mathbb{F}_{2^{31}}) = 2147574356$ .  
 $\#E(\mathbb{F}_{2^{101}}) = 2535301200456455833701195805484$ .

**5.23.** Let  $\tau$  satisfy  $\tau^2 = -2 - \tau$ . Prove that the following algorithm gives coefficients  $v_i \in \{-1, 0, 1\}$  such that the positive integer  $n$  is equal to

$$n = v_0 + v_1\tau + v_2\tau^2 + \cdots + v_\ell\tau^\ell. \quad (5.1)$$

Further prove that at most one-third of the  $v_i$  are nonzero and that  $\ell \leq \log(n)$ .

[1]	Set $n_0 = n$ and $n_1 = 0$ and $i = 0$
[2]	Loop while $n_0 \neq 0$ or $n_1 \neq 0$
[3]	If $n_0$ is odd
[4]	Set $v_i = 2 - ((n_0 - 2n_1) \bmod 4)$
[5]	Set $n_0 = n_0 - v_i$
[6]	Else
[7]	Set $v_i = 0$
[8]	End If
[9]	Set $i = i + 1$
[10]	Set $(n_0, n_1) = (n_1 - \frac{1}{2}n_0, -\frac{1}{2}n_0)$
[11]	End Loop

Solution to Exercise 5.23.

A solution for this exercise is not currently available.

**5.24.** Implement the algorithm in Exercise 5.23 and use it to compute the  $\tau$ -expansion (5.19) of the following integers. What is the highest power of  $\tau$  that appears and how many nonzero terms are there?

- (a)  $n = 931$       (b)  $n = 32755$       (c)  $n = 82793729188$

Solution to Exercise 5.24.

- (a)

$$931 = -1 + \tau^2 + \tau^{10} + \tau^{14} - \tau^{17} - \tau^{19} - \tau^{21}.$$

The highest power of  $\tau$  is  $\tau^{21}$  and the  $\tau$ -expansion has 7 nonzero terms.

(b)

$$32755 = -1 + \tau^2 + \tau^4 + \tau^6 + \tau^8 + \tau^{15} - \tau^{17} + \tau^{19} - \tau^{22} + \tau^{28} - \tau^{31}.$$

The highest power of  $\tau$  is  $\tau^{31}$  and the  $\tau$ -expansion has 11 nonzero terms.

(c)

$$\begin{aligned} 82793729188 = & \tau^2 + \tau^8 - \tau^{10} - \tau^{12} + \tau^{15} + \tau^{18} \\ & + \tau^{20} - \tau^{24} - \tau^{27} + \tau^{30} - \tau^{34} + \tau^{36} - \tau^{40} \\ & + \tau^{44} + \tau^{46} - \tau^{48} + \tau^{50} - \tau^{52} + \tau^{55} + \tau^{58} \\ & + \tau^{61} + \tau^{68} - \tau^{71} - \tau^{73}. \end{aligned}$$

The highest power of  $\tau$  is  $\tau^{73}$  and the  $\tau$ -expansion has 24 nonzero terms.

#### Section. Bilinear pairings on elliptic curves

**5.25.** Let  $R(x)$  and  $S(x)$  be rational functions. Prove that the divisor of a product is the sum of the divisors, i.e.,

$$\operatorname{div}(R(x)S(x)) = \operatorname{div}(R(x)) + \operatorname{div}(S(x)).$$

**5.26.** Prove that the Weil pairing satisfies

$$e_m(P, Q) = e_m(Q, P)^{-1} \quad \text{for all } P, Q \in E[m].$$

(Hint. Use the fact that  $e_m(P + Q, P + Q) = 1$  and expand using bilinearity.)

**5.27.** This exercise asks you to verify that the Weil pairing  $e_m$  is well-defined.

(a) Prove that the value of  $e_m(P, Q)$  is independent of the choice of rational functions  $f_P$  and  $f_Q$ .

(b) Prove that the value of  $e_m(P, Q)$  is independent of the auxiliary point  $S$ .

(Hint. Fix the points  $P$  and  $Q$  and consider the quantity

$$F(S) = \frac{f_P(Q + S)}{f_P(S)} \bigg/ \frac{f_Q(P - S)}{f_Q(-S)}$$

as a function of  $S$ . Compute the divisor of  $F$  and use the fact that every nonconstant function on  $E$  has at least one zero.)

You might also try to prove that the Weil pairing is bilinear, but do not be discouraged if you do not succeed, since the standard proofs use more tools than we have developed in the text.

**5.28.** Choose a basis  $\{P_1, P_2\}$  for  $E[m]$  and write each  $P \in E[m]$  as a linear combination  $P = a_P P_1 + b_P P_2$ . (See Remark 5.39.) Use the basic properties of the Weil pairing described in Theorem 5.38 to prove that

$$e_m(P, Q) = e_m(P_1, P_2)^{\det \begin{pmatrix} a_P & a_Q \\ b_P & b_Q \end{pmatrix}} = e_m(P_1, P_2)^{a_P b_Q - a_Q b_P}.$$



**5.29.** Complete the proof of Proposition 5.51 by proving that  $\phi(2P) = 2\phi(P)$ .

**5.30.** For each of the following elliptic curves  $E$ , finite fields  $\mathbb{F}_p$ , points  $P$  and  $Q$  of order  $m$ , and auxiliary points  $S$ , use Miller's algorithm to compute the Weil pairing  $e_m(P, Q)$ . (See Example 5.43.)

	$E$	$p$	$P$	$Q$	$m$	$S$
(a)	$y^2 = x^3 + 23$	1051	(109 203)	(240 203)	5	(1,554)
(b)	$y^2 = x^3 - 35x - 9$	883	(5, 66)	(103, 602)	7	(1,197)
(c)	$y^2 = x^3 + 37x$	1009	(8, 703)	(49, 20)	7	(0,0)
(d)	$y^2 = x^3 + 37x$	1009	(417, 952)	(561, 153)	7	(0,0)

Notice that (c) and (d) use the same elliptic curve. Letting  $P'$  and  $Q'$  denote the points in (d), verify that

$$P' = 2P, \quad Q' = 3Q, \quad \text{and} \quad e_7(P', Q') = e_7(P, Q)^6.$$

*Solution to Exercise 5.30.*

(a) We have  $\#E(\mathbb{F}_{1051}) = 1075 = 5^2 \cdot 43$ . The point  $S$  has order 215. Miller's algorithm gives

$$\frac{f_P(Q+S)}{f_P(S)} = \frac{109}{306} = 203 \quad \text{and} \quad \frac{f_Q(P-S)}{f_Q(-S)} = \frac{552}{406} = 312.$$

Taking the ratio of these two values yields

$$e_5(P, Q) = \frac{203}{312} = 671 \in \mathbb{F}_{1051}.$$

(b) We have  $\#E(\mathbb{F}_{883}) = 882 = 2 \cdot 3^2 \cdot 7^2$ . The point  $S$  has order 126. Miller's algorithm gives

$$\frac{f_P(Q+S)}{f_P(S)} = \frac{387}{413} = 730 \quad \text{and} \quad \frac{f_Q(P-S)}{f_Q(-S)} = \frac{454}{161} = 469.$$

Taking the ratio of these two values yields

$$e_7(P, Q) = \frac{730}{469} = 749 \in \mathbb{F}_{883}.$$

(c) We have  $\#E(\mathbb{F}_{1009}) = 980 = 2^2 \cdot 5 \cdot 7^2$ . The point  $S$  has order 2. Miller's algorithm gives

$$\frac{f_P(Q+S)}{f_P(S)} = \frac{92}{478} = 739 \quad \text{and} \quad \frac{f_Q(P-S)}{f_Q(-S)} = \frac{800}{810} = 574.$$

Taking the ratio of these two values yields

$$e_7(P, Q) = \frac{739}{574} = 105 \in \mathbb{F}_{1009}.$$

(d) Miller's algorithm gives

$$\frac{f_P(Q+S)}{f_P(S)} = \frac{86}{531} = 384 \quad \text{and} \quad \frac{f_Q(P-S)}{f_Q(-S)} = \frac{919}{759} = 969.$$

Taking the ratio of these two values yields

$$e_7(P, Q) = \frac{384}{969} = 394 \in \mathbb{F}_{1009}.$$

Finally, we check that

$$e_7(P, Q)^6 = 105^6 = 394 = e_7(P', Q'),$$

which is in accordance with  $P' = 2P$  and  $Q' = 3Q$ .

**5.31.** Let  $E$  over  $\mathbb{F}_q$  and  $\ell$  be as described in Theorem 5.44. Prove that the modified Tate pairing is symmetric, in the sense that

$$\hat{\tau}(P, Q) = \hat{\tau}(Q, P) \quad \text{for all } P, Q \in E(\mathbb{F}_q)[\ell].$$

*Solution to Exercise 5.31.*

By assumption we have  $E(\mathbb{F}_q)[\ell] = \mathbb{Z}/\ell\mathbb{Z}$ , a cyclic group. Let  $T$  be a generator. Then any  $P, Q \in E(\mathbb{F}_q)[\ell]$  can be written as  $P = uT$  and  $Q = vT$  for some  $u, v \in \mathbb{Z}/\ell\mathbb{Z}$ . But then the linearity of that Tate pairing gives

$$\begin{aligned} \hat{\tau}(P, Q) &= \hat{\tau}(uT, vT) = \hat{\tau}(T, T)^{uv}, \\ \hat{\tau}(Q, P) &= \hat{\tau}(vT, uT) = \hat{\tau}(T, T)^{vu}, \end{aligned}$$

which are clearly the same value.

**5.32.** Let  $E$  be an elliptic curve over  $\mathbb{F}_q$  and let  $P, Q \in E(\mathbb{F}_q)[\ell]$ . Prove that the Weil pairing and the Tate pairing are related by the formula

$$e_\ell(P, Q) = \frac{\tau(P, Q)}{\tau(Q, P)},$$

provided that the Tate pairings on the right-hand side are computed properly. Thus the Weil pairing requires approximately twice as much work to compute as does the Tate pairing.

**Section. The Weil pairing over fields of prime power order**

**5.33.** Prove Proposition 5.51(b) in the case  $P_1 = P_2$ .

**5.34.** Let  $E$  be an elliptic curve over  $\mathbb{F}_p$  and let  $\ell$  be a prime. Suppose that  $E(\mathbb{F}_p)$  contains a point of order  $\ell$  and that  $\ell > \sqrt{p} + 1$ . Prove that  $E(\mathbb{F}_p)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$ .

Solution to Exercise 5.34.

Hasse's theorem says that

$$\#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2.$$

The assumption on  $\ell$  then tells us that  $\#E(\mathbb{F}_p) < \ell^2$ . But if  $E(\mathbb{F}_p)[\ell]$  is larger than  $\mathbb{Z}/\ell\mathbb{Z}$ , then it is equal to  $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ , so we would have  $\ell^2$  elements, contradicting  $\#E(\mathbb{F}_p) < \ell^2$ .

**5.35.** Let  $E$  be an elliptic curve over a finite field  $\mathbb{F}_q$  and let  $\ell$  be a prime. Suppose that we are given four points  $P, aP, bP, cP \in E(\mathbb{F}_q)[\ell]$ . The (*elliptic*) *decision Diffie–Hellman problem* is to determine whether  $cP$  is equal to  $abP$ . Of course, if we could solve the Diffie–Hellman problem itself, then we could compute  $abP$  and compare it with  $cP$ , but the Diffie–Hellman problem is often difficult to solve.

Suppose that there exists a distortion map  $\phi$  for  $E[\ell]$ . Show how to use the modified Weil pairing to solve the elliptic decision Diffie–Hellman problem without actually having to compute  $abP$ .

Solution to Exercise 5.35.

Compute

$$\hat{e}_\ell(aP, bP) = \hat{e}_\ell(P, P)^{ab} \quad \text{and} \quad \hat{e}_\ell(P, cP) = \hat{e}_\ell(P, P)^c.$$

If they agree, then  $cP = abP$ , otherwise  $cP \neq abP$ .

**5.36.** Let  $E$  be the elliptic curve  $E : y^2 = x^3 + x$  and let  $\phi(x, y) = (-x, \alpha y)$  be the map described in Proposition 5.51. Prove that  $\phi(\phi(P)) = -P$  for all  $P \in E$ . (Intuitively,  $\phi$  behaves like multiplication by  $\sqrt{-1}$  when it is applied to points of  $E$ .)

Solution to Exercise 5.36.

Let  $P = (x, y)$ . We compute

$$\phi(\phi(P)) = \phi(-x, \alpha y) = (-(-x), \alpha \cdot \alpha y) = (x, \alpha^2 y) = (x, -y) = -P.$$

**5.37.** Let  $p \equiv 3 \pmod{4}$ , let  $E : y^2 = x^3 + x$ , let  $P \in E(\mathbb{F}_p)[\ell]$ , and let  $\phi(x, y) = (-x, \alpha y)$  be the  $\ell$ -distortion map for  $P$  described in Proposition 5.52. Suppose further that  $\ell \equiv 3 \pmod{4}$ . Prove that  $\phi$  is an  $\ell$ -distortion map for every point in  $E[\ell]$ . In other words, if  $Q \in E$  is any point of order  $\ell$ , prove that  $e_\ell(Q, \phi(Q))$  is a primitive  $\ell^{\text{th}}$  root of unity.

Solution to Exercise 5.37.

We can write  $Q = aP + b\phi(P)$ , since  $\{P, \phi(P)\}$  is a basis for  $E[\ell]$ . We have

$$\phi(Q) = \phi(aP + b\phi(P)) = a\phi(P) + b\phi(\phi(P)).$$

Note that

$$\phi(\phi(P)) = \phi(\phi(x, y)) = \phi(-x, \alpha y) = (x, \alpha^2 y) = (x, -y) = -P.$$

(This was a previous exercise.) So  $\phi(Q) = -bP + a\phi(P)$ . Hence

$$\begin{aligned} e_\ell(Q, \phi(Q)) &= e_\ell(aP + b\phi(P), -bP + a\phi(P)) \\ &= e_\ell(P, P)^{-ab} e_\ell(P, \phi(P))^{a^2} e_\ell(\phi(P), P)^{-b^2} e_\ell(\phi(P), \phi(P))^{ab} \\ &= e_\ell(P, \phi(P))^{a^2+b^2}. \end{aligned}$$

We know that  $e_\ell(P, \phi(P))$  is a primitive  $\ell^{\text{th}}$ -root of unity, so either  $e_\ell(Q, \phi(Q))$  is a primitive  $\ell^{\text{th}}$ -root of unity, or else  $a^2 + b^2$  is a multiple of  $\ell$ . (Note that we can assume that take  $0 \leq a, b < \ell$  and that  $a$  and  $b$  are not both 0.) But if  $\ell$  divides  $a^2 + b^2$ , then we get

$$1 = \left(\frac{a^2}{\ell}\right) = \left(\frac{-b^2}{\ell}\right) = \left(\frac{-1}{\ell}\right) \left(\frac{b^2}{\ell}\right) = \left(\frac{-1}{\ell}\right),$$

so  $-1$  is a square modulo  $\ell$ . From an easy piece of quadratic reciprocity, this implies that  $\ell \equiv 1 \pmod{4}$ , contradicting our assumption that  $\ell \equiv 3 \pmod{4}$ .

**5.38.** Let  $E$  be the elliptic curve

$$E : y^2 = x^3 + 1$$

over a field  $K$ , and suppose that  $K$  contains an element  $\beta \neq 1$  satisfying  $\beta^3 = 1$ . (We say that  $\beta$  is a *primitive cube root of unity*.) Define a map  $\phi$  by

$$\phi(x, y) = (\beta x, y) \quad \text{and} \quad \phi(\mathcal{O}) = \mathcal{O}.$$

- (a) Let  $P \in E(K)$ . Prove that  $\phi(P) \in E(K)$ .
- (b) Prove that  $\phi$  respects the addition law on  $E$ , i.e.,  $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$  for all  $P_1, P_2 \in E(K)$ .

**5.39.** Let  $E : y^2 = x^3 + 1$  be the elliptic curve in Exercise 5.38.

- (a) Let  $p \geq 3$  be a prime with  $p \equiv 2 \pmod{3}$ . Prove that  $\mathbb{F}_p$  does not contain a primitive cube root of unity, but that  $\mathbb{F}_{p^2}$  does contain a primitive cube root of unity.
- (b) Let  $\beta \in \mathbb{F}_{p^2}$  be a primitive cube root of unity and define a map  $\phi(x, y) = (\beta x, y)$  as in Exercise 5.38. Suppose that  $E(\mathbb{F}_p)$  contains a point  $P$  of prime order  $\ell \geq 5$ . Prove that  $\phi$  is an  $\ell$ -distortion map for  $P$ .

Solution to Exercise 5.39.

(b) This is the same as the proof of Proposition 5.52. The multiples of  $P$  are in  $E(\mathbb{F}_p)$ , but  $\phi(P)$  is not unless its  $x$ -coordinate is 0. Then one checks that points on  $E$  of the form  $(0, y)$  are points of order 3. Hence  $\phi(P)$  is not a multiple of  $P$ , and then Proposition 5.49 tells us that  $e_\ell(P, \phi(P))$  is a primitive  $\ell^{\text{th}}$ -root of unity.

**5.40.** Let  $E$  be the elliptic curve  $E : y^2 = x^3 + x$  over the field  $\mathbb{F}_{691}$ . The point  $P = (301, 14) \in \#E(\mathbb{F}_{691})$  has order 173. Use the distortion map on  $E$  from Exercises 5.38 and 5.39 to compute  $\hat{e}_{173}(P, P)$  (cf. Example 5.54). Verify that the value is a primitive 173<sup>rd</sup> root of unity.

*Solution to Exercise 5.40.*

We have  $\phi(P) = (-301, 14i) = (390, 14i)$ . We randomly choose a point

$$S = (499 + 325i, 41 + 140i) \in E(\mathbb{F}_{691^2})$$

and use Miller's algorithm to compute

$$\begin{aligned} \frac{f_P(\phi(P) + S)}{f_P(S)} &= \frac{452 + 325i}{236 + 219i} = 432 + 271i, \\ \frac{f_{\phi(P)}(P - S)}{f_{\phi(P)}(-S)} &= \frac{48 + 608i}{115 + 533i} = 259 + 271i. \end{aligned}$$

Then

$$\hat{e}(P, P) = e_{173}(P, \phi(P)) = \frac{432 + 271i}{259 + 271i} = 242 + 92i \in \mathbb{F}_{691^2}.$$

We check that  $(242 + 92i)^{173} = 1$ .

**5.41.** Continuing with the curve  $E$ , prime  $p = 691$ , and point  $P = (301, 14)$  from Exercise 5.40, let

$$Q = (143, 27) \in E(\mathbb{F}_{691}).$$

Use the MOV method to solve the ECDLP for  $P$  and  $Q$ , i.e., compute  $\hat{e}_{173}(P, Q)$  and express it as the  $n^{\text{th}}$  power of  $\hat{e}_{173}(P, P)$ . Check your answer by verifying that  $nP$  is equal to  $Q$ .

*Solution to Exercise 5.41.*

The distortion map gives  $\phi(Q) = (548, 278i)$ , and we use the randomly chosen point  $S = (379 + 605i, 205 + 534i) \in E(\mathbb{F}_{691^2})$  to compute

$$\hat{e}_{173}(P, Q) = e_{173}(P, \phi(Q)) = \frac{\frac{139+432i}{506+550i}}{\frac{239+375i}{142+299i}} = 500 + 603i \in \mathbb{F}_{691^2}.$$

From the previous exercise we have  $\hat{e}_{173}(P, P) = 242 + 92i$ , so we need to solve the DLP

$$(242 + 92i)^n = 500 + 603i \quad \text{in } \mathbb{F}_{691^2}.$$

The solution to this DLP is  $n = 122$ , and we can check that  $Q = P$ , so  $n = 122$  is also a solution to the ECDLP.

**Section. Applications of the Weil pairing**

**5.42.** Alice, Bob, and Carl use tripartite Diffie–Hellman with the curve

$$E : y^2 = x^3 + x \quad \text{over the field } \mathbb{F}_{1723}.$$

They use the point

$$P = (668, 995) \quad \text{of order 431.}$$

- (a) Alice chooses the secret value  $n_A = 278$ . What is Alice’s public point  $Q_A$ ?
- (b) Bob’s public point is  $Q_B = (1275, 1550)$  and Carl’s public point is  $Q_C = (897, 1323)$ . What is the value of  $\hat{e}_{431}(Q_B, Q_C)$ ?
- (c) What is their shared value?
- (d) Bob’s secret value is  $n_B = 224$ . Verify that  $\hat{e}_{431}(Q_A, Q_C)^{n_B}$  is the same as the value that you got in (c).
- (e) Figure out Carl’s secret value  $n_C$ . (Since  $P$  has order 431, you can do this on a computer by trying all possible values.)

Solution to Exercise 5.42.

- (a) Alice’s public point is  $Q_A = n_A P = (726, 1127)$ .
- (b)  $\hat{e}_{431}(Q_B, Q_C) = 1444 + 1288i$ .
- (c) The shared value is  $\hat{e}_{431}(Q_B, Q_C)^{278} = (1444 + 1288i)^{278} = 68 + 428i$ .
- (d)  $\hat{e}_{431}(Q_A, Q_C)^{224} = (1264 + 1083i)^{224} = 68 + 428i$ .
- (e) Carl’s secret value is  $n_C = 145$ . We check that he gets the same shared value,  $\hat{e}_{431}(Q_A, Q_B)^{145} = (977 + 1163i)^{145} = 68 + 428i$ .

**5.43.** Show that Eve can break tripartite Diffie–Hellman key exchange as described in Table 5.10.1 if she knows how to solve the Diffie–Hellman problem (page 67) for the field  $\mathbb{F}_q$ .

Solution to Exercise 5.43.

Eve can compute

$$\hat{e}_\ell(P, P) \quad \text{and} \quad \hat{e}_\ell(Q_A, P) = \hat{e}_\ell(n_A P, P) = \hat{e}_\ell(P, P)^{n_A}.$$

But she can also compute

$$\hat{e}_\ell(Q_B, Q_C) = \hat{e}_\ell(P, P)^{n_B n_C}.$$

Thus Eve knows the quantities

$$g^{n_A} \quad \text{and} \quad g^{n_B n_C}$$

for a certain primitive  $\ell^{\text{th}}$  root of unity  $g$  in  $\mathbb{F}_q^*$ . If she can solve the Diffie–Hellman problem in  $\mathbb{F}_q^*$ , then she can use these known values to compute Alice, Bob, and Carl’s shared value  $g^{n_A n_B n_C}$ .



## Chapter 6

# Lattices and Cryptography

### Exercises for Chapter 6

Section. A congruential public key cryptosystem

**6.1.** Alice uses the congruential cryptosystem with  $q = 918293817$  and private key  $(f, g) = (19928, 18643)$ .

- (a) What is Alice's public key  $h$ ?
- (b) Alice receives the ciphertext  $e = 619168806$  from Bob. What is the plaintext?
- (c) Bob sends Alice a second message by encrypting the plaintext  $m = 10220$  using the ephemeral key  $r = 19564$ . What is the ciphertext that Bob sends to Alice?

Solution to Exercise 6.1.

- (a)  $h = 767748560$ .
- (b) First compute

$$a \equiv fe \equiv 600240756 \pmod{q}$$

Then

$$m = f^{-1}a = 9764 \cdot 600240756 \equiv 11818 \pmod{g}.$$

(The ephemeral key was 19564.)

- (c)

$$e \equiv rh + m \equiv 619167208 \pmod{q}.$$

Section. Subset-sum problems and knapsack cryptosystems

**6.2.** Use the algorithm described in Proposition 6.5 to solve each of the following subset-sum problems. If the “solution” that you get is not correct, explain what went wrong.

- (a)  $\mathbf{M} = (3, 7, 19, 43, 89, 195)$ ,  $S = 260$ .



- (b)  $\mathbf{M} = (5, 11, 25, 61, 125, 261)$ ,  $S = 408$ .  
 (c)  $\mathbf{M} = (2, 5, 12, 28, 60, 131, 257)$ ,  $S = 334$ .  
 (d)  $\mathbf{M} = (4, 12, 15, 36, 75, 162)$ ,  $S = 214$ .

Solution to Exercise 6.2.

- (a) Output from algorithm is  $\mathbf{x} = (1, 0, 1, 1, 0, 1)$ . Sum is correct.  
 (b) Output from algorithm is  $\mathbf{x} = (1, 1, 0, 0, 1, 1)$ . Sum is 402 instead of 408. Incorrect. Superincreasing, but this  $S$  has no solution.  
 (c) Output from algorithm is  $\mathbf{x} = (0, 1, 1, 0, 1, 0, 1)$ . Sum is correct.  
 (d) Output from algorithm is  $\mathbf{x} = (0, 0, 1, 1, 0, 1)$ . Sum is 213 instead of 214. Incorrect.  $\mathbf{M}$  is not superincreasing, this problem has a solution  $(1, 1, 0, 1, 0, 1)$ , but it is not found by the algorithm.

**6.3.** Alice's public key for a knapsack cryptosystem is

$$\mathbf{M} = (5186, 2779, 5955, 2307, 6599, 6771, 6296, 7306, 4115, 7039).$$

Eve intercepts the encrypted message  $S = 26560$ . She also breaks into Alice's computer and steals Alice's secret multiplier  $A = 4392$  and secret modulus  $B = 8387$ . Use this information to find Alice's superincreasing private sequence  $\mathbf{r}$  and then decrypt the message.

Solution to Exercise 6.3.

*A solution for this exercise is not currently available.*

**6.4.** Proposition 6.3 gives an algorithm that solves an  $n$ -dimensional knapsack problem in  $\mathcal{O}(2^{n/2})$  steps, but it requires  $\mathcal{O}(2^{n/2})$  storage. Devise an algorithm, similar to Pollard's  $\rho$  algorithm (Section 4.5), that takes  $\mathcal{O}(2^{n/2})$  steps, but requires only  $\mathcal{O}(1)$  storage.

Solution to Exercise 6.4.

*A solution for this exercise is not currently available.*

Section. A brief review of vector spaces

**6.5.** (a) Let

$$\mathcal{B} = \{(1, 3, 2), (2, -1, 3), (1, 0, 2)\}, \quad \mathcal{B}' = \{(-1, 0, 2), (3, 1, -1), (1, 0, 1)\}.$$

Each of the sets  $\mathcal{B}$  and  $\mathcal{B}'$  is a basis for  $\mathbb{R}^3$ . Find the change of basis matrix that transforms  $\mathcal{B}'$  into  $\mathcal{B}$ .

- (b) Let  $\mathbf{v} = (2, 3, 1)$  and  $\mathbf{w} = (-1, 4, -2)$ . Compute the lengths  $\|\mathbf{v}\|$  and  $\|\mathbf{w}\|$  and the dot product  $\mathbf{v} \cdot \mathbf{w}$ . Compute the angle between  $\mathbf{v}$  and  $\mathbf{w}$ .

Solution to Exercise 6.5.

(a) Let

$$B = \begin{pmatrix} 1 & 3 & 2 \\ 2 & -1 & 3 \\ 1 & 0 & 2 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} -1 & 0 & 2 \\ 3 & 1 & -1 \\ 1 & 0 & 1 \end{pmatrix}$$

Then

$$C^{-1} = \begin{pmatrix} \frac{-1}{3} & 0 & \frac{2}{3} \\ \frac{4}{3} & 1 & \frac{-5}{3} \\ \frac{1}{3} & 0 & \frac{1}{3} \end{pmatrix} \quad \text{and} \quad A = BC^{-1} = \begin{pmatrix} \frac{13}{3} & 3 & \frac{-11}{3} \\ -1 & -1 & 4 \\ \frac{1}{3} & 0 & \frac{4}{3} \end{pmatrix}$$

$$(b) \quad \|\mathbf{v}\| = \sqrt{14} \approx 3.7417. \quad \|\mathbf{w}\| = \sqrt{21} \approx 4.5826. \quad \mathbf{v} \cdot \mathbf{w} = 8.$$

$$\cos(\theta) = 8/\sqrt{14} \cdot \sqrt{21} \approx 0.4666, \text{ so}$$

$$\theta \approx \cos^{-1}(0.4666) \approx 1.0854 \text{ radians} \approx 62.188 \text{ degrees.}$$

**6.6.** Use the Gram–Schmidt algorithm (Theorem 6.13) to find an orthogonal basis from the given basis.

$$(a) \quad \mathbf{v}_1 = (1, 3, 2), \quad \mathbf{v}_2 = (4, 1, -2), \quad \mathbf{v}_3 = (-2, 1, 3).$$

$$(b) \quad \mathbf{v}_1 = (4, 1, 3, -1), \quad \mathbf{v}_2 = (2, 1, -3, 4), \quad \mathbf{v}_3 = (1, 0, -2, 7).$$

Solution to Exercise 6.6.

(a)

$$\mathbf{v}_1^* = (1, 3, 2), \quad \mathbf{v}_2^* = (53/14, 5/14, -17/7), \quad \mathbf{v}_3^* = (56/285, -14/57, 77/285).$$

(b)

$$\mathbf{v}_1^* = (4, 1, 3, -1), \quad \mathbf{v}_2^* = (70/27, 31/27, -23/9, 104/27),$$

$$\mathbf{v}_3^* = (-287/397, -405/397, 799/397, 844/397).$$

Section. Lattices: Basic definitions and properties

**6.7.** Let  $L$  be the lattice generated by  $\{(1, 3, -2), (2, 1, 0), (-1, 2, 5)\}$ . Draw a picture of a fundamental domain for  $L$  and find its volume.

Solution to Exercise 6.7.

The volume is

$$\left| \det \begin{pmatrix} 1 & 3 & -2 \\ 2 & 1 & 0 \\ -1 & 2 & 5 \end{pmatrix} \right| = 35.$$

**6.8.** Let  $L \subset \mathbb{R}^m$  be an additive subgroup with the property that there is a positive constant  $\epsilon > 0$  such that

$$L \cap \{\mathbf{w} \in \mathbb{R}^m : \|\mathbf{w}\| < \epsilon\} = \{\mathbf{0}\}.$$

Prove that  $L$  is discrete, and hence is a lattice. (In other words, show that in the definition of discrete subgroup, it suffices to check that (6.8) is true for the single vector  $\mathbf{v} = \mathbf{0}$ .)

Solution to Exercise 6.8.

*A solution for this exercise is not currently available.*

**6.9.** Prove that a subset of  $\mathbb{R}^m$  is a lattice if and only if it is a discrete additive subgroup.

Solution to Exercise 6.9.

*A solution for this exercise is not currently available.*

**6.10.** This exercise describes a result that you may have seen in your linear algebra course.

Let  $A$  be an  $n$ -by- $n$  matrix with entries  $a_{ij}$ , and for each pair of indices  $i$  and  $j$ , let  $A_{ij}$  denote the  $(n-1)$ -by- $(n-1)$  matrix obtained by deleting the  $i^{\text{th}}$  row of  $A$  and the  $j^{\text{th}}$  column of  $A$ . Define a new matrix  $B$  whose  $ij^{\text{th}}$  entry  $b_{ij}$  is given by the formula

$$b_{ij} = (-1)^{i+j} \det(A_{ji}).$$

(Note that  $b_{ij}$  is the determinant of the submatrix  $A_{ji}$ , i.e., the indices are reversed.) The matrix  $B$  is called the *adjoint* of  $A$ .

(a) Prove that

$$AB = BA = \det(A)I_n,$$

where  $I_n$  is the  $n$ -by- $n$  identity matrix.

(b) Deduce that if  $\det(A) \neq 0$ , then

$$A^{-1} = \frac{1}{\det(A)} B.$$

(c) Suppose that  $A$  has integer entries. Prove that  $A^{-1}$  exists and has integer entries if and only if  $\det(A) = \pm 1$ .

(d) For those who know ring theory from Section 2.10 or from some other source, suppose that  $A$  has entries in a ring  $R$ . Prove that  $A^{-1}$  exists and has entries in  $R$  if and only if  $\det(A)$  is a unit in  $R$ .

Solution to Exercise 6.10.

*A solution for this exercise is not currently available.*

**6.11.** Recall from Remark 6.16 that the general linear group  $\text{GL}_n(\mathbb{Z})$  is the group of  $n$ -by- $n$  matrices with integer coefficients and determinant  $\pm 1$ . Let  $A$  and  $B$  be matrices in  $\text{GL}_n(\mathbb{Z})$ .

(a) Prove that  $AB \in \text{GL}_n(\mathbb{Z})$ .

(b) Prove that  $A^{-1} \in \text{GL}_n(\mathbb{Z})$ .

(c) Prove that the  $n$ -by- $n$  identity matrix is in  $\text{GL}_n(\mathbb{Z})$ .

(d) Prove that  $\text{GL}_n(\mathbb{Z})$  is a group. (*Hint.* You have already done most of the work in proving (a), (b), and (c). For the associative law, either prove it directly or use the fact that you know that it is true for matrices with real coefficients.)

(e) Is  $\text{GL}_n(\mathbb{Z})$  a commutative group?

*Solution to Exercise 6.11.*

(a) By assumption,  $A^{-1}$  and  $B^{-1}$  have integer entries. Hence  $(AB)^{-1} = B^{-1}A^{-1}$  also has integer entries, so  $AB \in \text{GL}_n(\mathbb{Z})$ .

(b)  $(A^{-1})^{-1}$  is equal to  $A$ , so it has integer entries. Hence  $A^{-1} \in \text{GL}_n(\mathbb{Z})$ .

(c) Let  $I$  be the identity matrix. Then  $I$  has integer entries, and  $I^{-1} = I$  also has integer entries, so  $I \in \text{GL}_n(\mathbb{Z})$ .

(d) As the hint says, (a), (b) and (c) show that the product and inverse of matrices in  $\text{GL}_n(\mathbb{Z})$  are again in  $\text{GL}_n(\mathbb{Z})$  and the identity matrix is in  $\text{GL}_n(\mathbb{Z})$ , so really just need to check the associative law  $(AB)C = A(BC)$ . But you proved the associative law for matrix multiplication in linear algebra when the entries are real numbers (or maybe even more generally), so it is certainly true when the entries are integers.

(e) No,  $\text{GL}_n(\mathbb{Z})$  is not commutative for  $n \geq 2$ . For example,  $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$  and  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  do not commute, and similar examples exist for any  $n \geq 2$ . Of course, for  $n = 1$ ,  $\text{GL}_1(\mathbb{Z}) = \{\pm 1\}$  is commutative.

**6.12.** Which of the following matrices are in  $\text{GL}_n(\mathbb{Z})$ ? Find the inverses of those matrices that are in  $\text{GL}_n(\mathbb{Z})$ .

$$(a) \quad A_1 = \begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix}$$

$$(b) \quad A_2 = \begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}$$

$$(c) \quad A_3 = \begin{pmatrix} 3 & 2 & 2 \\ 2 & 1 & 2 \\ -1 & 3 & 1 \end{pmatrix}$$

$$(d) \quad A_4 = \begin{pmatrix} -3 & -1 & 2 \\ 1 & -3 & -1 \\ 3 & 0 & -2 \end{pmatrix}$$

*Solution to Exercise 6.12.*

(a) No, since  $\det = 4$ .

(b) Yes, since  $\det = 1$ .  $A_2^{-1} = \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}$ .

(c) No, since  $\det = -9$ .

(d) Yes, since  $\det = 1$ .  $A_4^{-2} = \begin{pmatrix} 6 & -2 & 7 \\ -1 & 0 & -1 \\ 9 & -3 & 10 \end{pmatrix}$ .

**6.13.** Let  $L$  be the lattice given by the basis

$$\mathcal{B} = \{(3, 1, -2), (1, -3, 5), (4, 2, 1)\}.$$

Which of the following sets of vectors are also bases for  $L$ ? For those that are, express the new basis in terms of the basis  $\mathcal{B}$ , i.e., find the change of basis matrix.

(a)  $\mathcal{B}_1 = \{(5, 13, -13), (0, -4, 2), (-7, -13, 18)\}$ .

(b)  $\mathcal{B}_2 = \{(4, -2, 3), (6, 6, -6), (-2, -4, 7)\}$ .

Solution to Exercise 6.13.

(a) Yes. The change of basis matrix is

$$\begin{pmatrix} 5 & 13 & -13 \\ 0 & -4 & 2 \\ -7 & -13 & 18 \end{pmatrix} = \begin{pmatrix} 0 & -3 & 2 \\ 1 & 1 & -1 \\ -2 & 3 & -1 \end{pmatrix} \begin{pmatrix} 3 & 1 & -2 \\ 1 & -3 & 5 \\ 4 & 2 & 1 \end{pmatrix}$$

The inverse matrix is

$$\begin{pmatrix} 0 & -3 & 2 \\ 1 & 1 & -1 \\ -2 & 3 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 4 & 2 \\ 5 & 6 & 3 \end{pmatrix}$$

which shows that  $\mathcal{B}$  and  $\mathcal{B}_1$  generate the same lattice.

(b) No, since  $\det(\mathcal{B}) = -48$  and  $\det(\mathcal{B}_2) = 96$ .

**6.14.** Let  $L \subset \mathbb{R}^m$  be a lattice of dimension  $n$  and let  $\mathbf{v}_1, \dots, \mathbf{v}_n$  be a basis for  $L$ . (Note that we are allowing  $n$  to be smaller than  $m$ .) The *Gram matrix* of  $\mathbf{v}_1, \dots, \mathbf{v}_n$  is the matrix

$$\text{Gram}(\mathbf{v}_1, \dots, \mathbf{v}_n) = (\mathbf{v}_i \cdot \mathbf{v}_j)_{1 \leq i, j \leq n}.$$

(a) Let  $F(\mathbf{v}_1, \dots, \mathbf{v}_n)$  be the matrix (6.11) described in Proposition (6.20), except that now  $F(\mathbf{v}_1, \dots, \mathbf{v}_n)$  is an  $n$ -by- $m$  matrix, so it need not be square. Prove that

$$\text{Gram}(\mathbf{v}_1, \dots, \mathbf{v}_n) = F(\mathbf{v}_1, \dots, \mathbf{v}_n)F(\mathbf{v}_1, \dots, \mathbf{v}_n)^t,$$

where  $F(\mathbf{v}_1, \dots, \mathbf{v}_n)^t$  is the transpose matrix, i.e., the matrix with rows and columns interchanged.

(b) If  $m = n$ , prove that

$$\det(\text{Gram}(\mathbf{v}_1, \dots, \mathbf{v}_n)) = \det(L)^2. \quad (6.1)$$

(c) In general, prove that  $\det \text{Gram}(\mathbf{v}_1, \dots, \mathbf{v}_n)$  is the square of the volume of a fundamental domain for  $L$ , so we can use (6.61) to compute  $\det(L)$ .

(d) Let  $L \subset \mathbb{R}^4$  be the 3-dimensional lattice with basis

$$\mathbf{v}_1 = (1, 0, 1, -1), \quad \mathbf{v}_2 = (1, 2, 0, 4), \quad \mathbf{v}_3 = (1, -1, 2, 1).$$

Compute the Gram matrix of this basis and use it to compute  $\det(L)$ .

(e) Let  $\mathbf{v}_1^*, \dots, \mathbf{v}_n^*$  be the Gram-Schmidt orthogonalized vectors (Theorem 6.13) associated to  $\mathbf{v}_1, \dots, \mathbf{v}_n$ . Prove that

$$\text{Gram}(\mathbf{v}_1, \dots, \mathbf{v}_n) = \|\mathbf{v}_1^*\|^2 \|\mathbf{v}_2^*\|^2 \cdots \|\mathbf{v}_n^*\|^2.$$

Solution to Exercise 6.14.

(a-c) A solution for this exercise is not currently available.

(d)

$$\text{Gram}(\mathbf{v}_1, \dots, \mathbf{v}_n) = \begin{pmatrix} 1 & 0 & 1 & -1 \\ 1 & 2 & 0 & 4 \\ 1 & -1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & -1 \\ 1 & 0 & 2 \\ -1 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 3 & -3 & 2 \\ -3 & 21 & 3 \\ 2 & 3 & 7 \end{pmatrix}$$

Then

$$\det(L) = \sqrt{\det \text{Gram}(\mathbf{v}_1, \dots, \mathbf{v}_n)} = \sqrt{231}.$$

### Section. The shortest and closest vector problems

**6.15.** Let  $L$  be a lattice and let  $\mathcal{F}$  be a fundamental domain for  $L$ . This exercise sketches a proof that

$$\lim_{R \rightarrow \infty} \frac{\#(\mathbb{B}_R(\mathbf{0}) \cap L)}{\text{Vol}(\mathbb{B}_R(\mathbf{0}))} = \frac{1}{\text{Vol}(\mathcal{F})}. \quad (6.2)$$

- (a) Consider the translations of  $\mathcal{F}$  that are entirely contained within  $\mathbb{B}_R(\mathbf{0})$ , and also those that have nontrivial intersection with  $\mathbb{B}_R(\mathbf{0})$ . Prove the inclusion of sets

$$\bigcup_{\substack{\mathbf{v} \in L \\ \mathcal{F} + \mathbf{v} \subset \mathbb{B}_R(\mathbf{0})}} (\mathcal{F} + \mathbf{v}) \subset \mathbb{B}_R(\mathbf{0}) \subset \bigcup_{\substack{\mathbf{v} \in L \\ (\mathcal{F} + \mathbf{v}) \cap \mathbb{B}_R(\mathbf{0}) \neq \emptyset}} (\mathcal{F} + \mathbf{v}).$$

- (b) Take volumes in (a) and prove that

$$\begin{aligned} & \# \{ \mathbf{v} \in L : \mathcal{F} + \mathbf{v} \subset \mathbb{B}_R(\mathbf{0}) \} \cdot \text{Vol}(\mathcal{F}) \\ & \leq \text{Vol}(\mathbb{B}_R(\mathbf{0})) \leq \# \{ \mathbf{v} \in L : (\mathcal{F} + \mathbf{v}) \cap \mathbb{B}_R(\mathbf{0}) \neq \emptyset \} \cdot \text{Vol}(\mathcal{F}). \end{aligned}$$

(Hint. Proposition 6.18 says that the different translates of  $\mathcal{F}$  are disjoint.)

- (c) Prove that the number of translates  $\mathcal{F} + \mathbf{v}$  that intersect  $\mathbb{B}_R(\mathbf{0})$  without being entirely contained within  $\mathbb{B}_R(\mathbf{0})$  is comparatively small compared to the number of translates  $\mathcal{F}_{\mathbf{v}}$  that are entirely contained within  $\mathbb{B}_R(\mathbf{0})$ . (This is the hardest part of the proof.)

- (d) Use (b) and (c) to prove that

$$\text{Vol}(\mathbb{B}_R(\mathbf{0})) = \#(\mathbb{B}_R(\mathbf{0}) \cap L) \cdot \text{Vol}(\mathcal{F}) + (\text{smaller term}).$$

Divide by  $\text{Vol}(\mathbb{B}_R(\mathbf{0}))$  and let  $R \rightarrow \infty$  to complete the proof of (6.2).

Solution to Exercise 6.15.

A solution for this exercise is not currently available.

**6.16.** A lattice  $L$  of dimension  $n = 251$  has determinant  $\det(L) \approx 2^{2251.58}$ . With no further information, approximately how large would you expect the shortest nonzero vector to be?

*Solution to Exercise 6.16.*

The Gaussian heuristic (6.21) predicts that the shortest nonzero vector in  $L$  has length approximately

$$\sigma(L) = \sqrt{\frac{n}{2\pi e}} (\det L)^{1/n} \approx 1922.96.$$

Section. Babai's algorithm and solving CVP with a "good" basis

**6.17.** Let  $L \subset \mathbb{R}^2$  be the lattice given by the basis  $\mathbf{v}_1 = (213, -437)$  and  $\mathbf{v}_2 = (312, 105)$ , and let  $\mathbf{w} = (43127, 11349)$ .

- Use Babai's algorithm to find a vector  $\mathbf{v} \in L$  that is close to  $\mathbf{w}$ . Compute the distance  $\|\mathbf{v} - \mathbf{w}\|$ .
- What is the value of the Hadamard ratio  $\det(L)/\|\mathbf{v}_1\|\|\mathbf{v}_2\|$ ? Is the basis  $\{\mathbf{v}_1, \mathbf{v}_2\}$  a "good" basis?
- Show that the vectors  $\mathbf{v}'_1 = (2937, -1555)$  and  $\mathbf{v}'_2 = (11223, -5888)$  are also a basis for  $L$  by expressing them as linear combinations of  $\mathbf{v}_1$  and  $\mathbf{v}_2$  and checking that the change-of-basis matrix has integer coefficients and determinant  $\pm 1$ .
- Use Babai's algorithm with the basis  $\{\mathbf{v}'_1, \mathbf{v}'_2\}$  to find a vector  $\mathbf{v}' \in L$ . Compute the distance  $\|\mathbf{v}' - \mathbf{w}\|$  and compare it to your answer from (a).
- Compute the Hadamard ratio using  $\mathbf{v}'_1$  and  $\mathbf{v}'_2$ . Is  $\{\mathbf{v}'_1, \mathbf{v}'_2\}$  a good basis?

*Solution to Exercise 6.17.*

(a)  $(t_1, t_2) = (6.22, 133.98)$ , so  $\mathbf{v} = 6\mathbf{v}_1 + 134\mathbf{v}_2 = (43086, 11448)$ . Then  $\|\mathbf{v} - \mathbf{w}\| = 107.15$ .

(b)  $\det(L)/\|\mathbf{v}_1\|\|\mathbf{v}_2\| = 158709/(486.15)(329.19) = 0.9917$ . The ratio is close to 1, so  $\{\mathbf{v}_1, \mathbf{v}_2\}$  a good basis.

(c)  $\mathbf{v}'_1 = 5\mathbf{v}_1 + 6\mathbf{v}_2$  and  $\mathbf{v}'_2 = 19\mathbf{v}_1 + 23\mathbf{v}_2$ . We have  $\det \begin{pmatrix} 5 & 6 \\ 19 & 23 \end{pmatrix} = 1$ .

(d)  $(t_1, t_2) = (-2402.52, 632.57)$ , so  $\mathbf{v}' = -2403\mathbf{v}'_1 + 633\mathbf{v}'_2 = (46548, 9561)$ . Then  $\|\mathbf{v}' - \mathbf{w}\| = 3860.08$ .

(e)  $\det(L)/\|\mathbf{v}'_1\|\|\mathbf{v}'_2\| = 158709/(3323.25)(12673.76) = 0.00377$ . The ratio is very small, so  $\{\mathbf{v}'_1, \mathbf{v}'_2\}$  a bad basis.

Section. The GGH public key cryptosystem

**6.18.** Alice uses the GGH cryptosystem with private basis

$$\mathbf{v}_1 = (4, 13), \quad \mathbf{v}_2 = (-57, -45),$$

and public basis

$$\mathbf{w}_1 = (25453, 9091), \quad \mathbf{w}_2 = (-16096, -5749).$$

- (a) Compute the determinant of Alice's lattice and the Hadamard ratio of the private and public bases.
- (b) Bob sends Alice the encrypted message  $\mathbf{e} = (155340, 55483)$ . Use Alice's private basis to decrypt the message and recover the plaintext. Also determine Bob's random perturbation  $\mathbf{r}$ .
- (c) Try to decrypt Bob's message using Babai's algorithm with the public basis  $\{\mathbf{w}_1, \mathbf{w}_2\}$ . Is the output equal to the plaintext?

Solution to Exercise 6.18.

(a)  $\det(L) = 561$ , The Hadamard ratio of the private key is 0.75362. and the Hadamard ratio of the public key is 0.0011.

(b)

$$\begin{aligned}\mathbf{e} &\approx -6823.12\mathbf{v}_1 - 3204.08\mathbf{v}_2. \\ \mathbf{v} &= -6823\mathbf{v}_1 - 3204\mathbf{v}_2 \\ &= (155336, 55481) \\ &= 8\mathbf{w}_1 + 3\mathbf{w}_2.\end{aligned}$$

So the plaintext is  $\mathbf{m} = (8, 3)$ . Also  $\mathbf{r} = \mathbf{w} - \mathbf{v} = (4, 2)$ .

(c)

$$\mathbf{e} \approx -8.39\mathbf{w}_1 - 22.92\mathbf{w}_2.$$

This yields the incorrect plaintext  $(-8, -23)$ .

**6.19.** Alice uses the GGH cryptosystem with private basis

$$\mathbf{v}_1 = (58, 53, -68), \quad \mathbf{v}_2 = (-110, -112, 35), \quad \mathbf{v}_3 = (-10, -119, 123)$$

and public basis

$$\begin{aligned}\mathbf{w}_1 &= (324850, -1625176, 2734951), \\ \mathbf{w}_2 &= (165782, -829409, 1395775), \\ \mathbf{w}_3 &= (485054, -2426708, 4083804).\end{aligned}$$

- (a) Compute the determinant of Alice's lattice and the Hadamard ratio of the private and public bases.
- (b) Bob sends Alice the encrypted message  $\mathbf{e} = (8930810, -44681748, 75192665)$ . Use Alice's private basis to decrypt the message and recover the plaintext. Also determine Bob's random perturbation  $\mathbf{r}$ .
- (c) Try to decrypt Bob's message using Babai's algorithm with the public basis  $\{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3\}$ . Is the output equal to the plaintext?

Solution to Exercise 6.19.

(a)  $\det(L) = -672858$ , The Hadamard ratio of the private key is 0.61697 and the Hadamard ratio of the public key is 0.00003.

(b)



$$\begin{aligned}
\mathbf{e} &\approx -334865.23\mathbf{v}_1 - 304373.02\mathbf{v}_2 + 512803.95\mathbf{v}_3. \\
\mathbf{v} &= -334865\mathbf{v}_1 - 304373\mathbf{v}_2 + 512804\mathbf{v}_3 \\
&= (8930820, -44681745, 75192657) \\
&= -50\mathbf{w}_1 - 91\mathbf{w}_2 + 83\mathbf{w}_3.
\end{aligned}$$

So the plaintext is  $\mathbf{m} = (-50, -91, 83)$ . Also  $\mathbf{r} = \mathbf{w} - \mathbf{v} = (-10, -3, 8)$ .

(c)

$$\mathbf{e} \approx 51.59\mathbf{w}_1 + 416.67\mathbf{w}_2 - 158.55\mathbf{w}_3.$$

This yields the incorrect plaintext  $(52, 417, -159)$ .

**6.20.** Bob uses the GGH cryptosystem to send some messages to Alice.

- (a) Suppose that Bob sends the same message  $\mathbf{m}$  twice, using different random perturbations  $\mathbf{r}$  and  $\mathbf{r}'$ . Explain what sort of information Eve can deduce from the ciphertexts  $\mathbf{e} = \mathbf{m}W + \mathbf{r}$  and  $\mathbf{e}' = \mathbf{m}W + \mathbf{r}'$ .
- (b) For example, suppose that  $n = 5$  and that random permutations are chosen with coordinates in the set  $\{-2, -1, 0, 1, 2\}$ . This means that there are  $5^5 = 3125$  possibilities for  $\mathbf{r}$ . Suppose further that Eve intercepts two ciphertexts

$$\mathbf{e} = (-9, -29, -48, 18, 48) \quad \text{and} \quad \mathbf{e}' = (-6, -26, -51, 20, 47)$$

having the same plaintext. With this information, how many possibilities are there for  $\mathbf{r}$ ?

- (c) Suppose that Bob is lazy and uses the same perturbation to send two different messages. Explain what sort of information Eve can deduce from the ciphertexts  $\mathbf{e} = \mathbf{m}W + \mathbf{r}$  and  $\mathbf{e}' = \mathbf{m}'W + \mathbf{r}$ .

Solution to Exercise 6.20.

(a) Eve can compute  $\mathbf{e}' - \mathbf{e} = \mathbf{r}' - \mathbf{r}$  and use this information to narrow down the possibilities for  $\mathbf{r}$  and  $\mathbf{r}'$ .

(b) Eve computes

$$\mathbf{e} - \mathbf{e}' = \mathbf{r} - \mathbf{r}' = (-3, -3, 3, -2, 1).$$

Thus

$$r_1 = r'_1 - 3, \quad r_2 = r'_2 - 3, \quad r_3 = r'_3 + 3, \quad r_4 = r'_4 - 2, \quad r_5 = r'_5 + 1.$$

Further, Eve knows that all of the  $r_i$  and all of the  $r'_i$  are between  $-2$  and  $2$ . Thus each equation puts some restrictions on the coordinates of  $\mathbf{r}$ . For example

$$r_1 = r'_1 - 3 \leq 2 - 3 = -1, \quad \text{so} \quad r_1 \in \{-2, -1\},$$

and similarly

$$\begin{aligned}
r_2 &= r'_2 - 3 \leq -2 + 3 = 1, & \text{so } r_2 &\in \{-2, -1\}, \\
r_3 &= r'_3 + 3 \geq -2 + 3 = 1, & \text{so } r_3 &\in \{1, 2\}, \\
r_4 &= r'_4 - 2 \leq 2 - 2 = 0, & \text{so } r_4 &\in \{-2, -1, 0\}, \\
r_5 &= r'_5 + 1 \geq -2 + 1 = -1, & \text{so } r_1 &\in \{-1, 0, 1, 2\}.
\end{aligned}$$

Hence the number of possibilities for  $\mathbf{r}$  has been reduced to  $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 72$ , which is far less than 3125.

(c) This time Eve can compute  $(\mathbf{e} - \mathbf{e}')W^{-1} = \mathbf{m} - \mathbf{m}'$ , and then the fact that  $\mathbf{m}$  and  $\mathbf{m}'$  are small again allows Eve to narrow down the possibilities.

#### Section. Convolution polynomial rings

**6.21.** Compute (by hand!) the polynomial convolution product  $\mathbf{c} = \mathbf{a} \star \mathbf{b}$  using the given value of  $N$ .

- (a)  $N = 3$ ,  $\mathbf{a}(x) = -1 + 4x + 5x^2$ ,  $\mathbf{b}(x) = -1 - 3x - 2x^2$ ;
- (b)  $N = 5$ ,  $\mathbf{a}(x) = 2 - x + 3x^3 - 3x^4$ ,  $\mathbf{b}(x) = 1 - 3x^2 - 3x^3 - x^4$ ;
- (c)  $N = 6$ ,  $\mathbf{a}(x) = x + x^2 + x^3$ ,  $\mathbf{b}(x) = 1 + x + x^5$ ;
- (d)  $N = 10$ ,  $\mathbf{a}(x) = x + x^2 + x^3 + x^4 + x^6 + x^7 + x^9$ ,  
 $\mathbf{b}(x) = x^2 + x^3 + x^6 + x^8$ .

*Solution to Exercise 6.21.*

- (a)  $\mathbf{c} = \mathbf{a} \star \mathbf{b} = -22 - 11x - 15x^2$ .
- (b)  $\mathbf{c} = \mathbf{a} \star \mathbf{b} = -6 - x + 3x^3 - 2x^4$ .
- (c)  $\mathbf{c} = \mathbf{a} \star \mathbf{b} = 1 + 2x + 3x^2 + 2x^3 + x^4$ .
- (d)  $\mathbf{c} = \mathbf{a} \star \mathbf{b} = 3 + 2x + 3x^2 + 2x^3 + 3x^4 + 4x^5 + 2x^6 + 3x^7 + 2x^8 + 4x^9$ .

**6.22.** Compute the polynomial convolution product  $\mathbf{c} = \mathbf{a} \star \mathbf{b}$  modulo  $q$  using the given values of  $q$  and  $N$ .

- (a)  $N = 3$ ,  $q = 7$ ,  $\mathbf{a}(x) = 1 + x$ ,  $\mathbf{b}(x) = -5 + 4x + 2x^2$ ;
- (b)  $N = 5$ ,  $q = 4$ ,  $\mathbf{a}(x) = 2 + 2x - 2x^2 + x^3 - 2x^4$ ,  
 $\mathbf{b}(x) = -1 + 3x - 3x^2 - 3x^3 - 3x^4$ ;
- (c)  $N = 7$ ,  $q = 3$ ,  $\mathbf{a}(x) = x + x^3$ ,  $\mathbf{b}(x) = x + x^2 + x^4 + x^6$ ;
- (d)  $N = 10$ ,  $q = 2$ ,  $\mathbf{a}(x) = x^2 + x^5 + x^7 + x^8 + x^9$ ,  
 $\mathbf{b}(x) = 1 + x + x^3 + x^4 + x^5 + x^7 + x^8 + x^9$ .

*Solution to Exercise 6.22.*

- (a)  $\mathbf{c} \equiv \mathbf{a} \star \mathbf{b} \equiv 4 + 6x + 6x^2 \pmod{7}$ .
- (b)  $\mathbf{c} \equiv \mathbf{a} \star \mathbf{b} \equiv 1 + x + x^2 + 3x^3 + 3x^4 \pmod{4}$ .
- (c)  $\mathbf{c} \equiv \mathbf{a} \star \mathbf{b} \equiv 2 + 2x^2 + x^3 + x^4 + 2x^5 \pmod{3}$ .
- (d)  $\mathbf{c} \equiv \mathbf{a} \star \mathbf{b} \equiv x + x^2 + x^4 + x^6 \pmod{2}$ .

**6.23.** Let  $\mathbf{a}(x) \in (\mathbb{Z}/q\mathbb{Z})[x]$ , where  $q$  is a prime.

(a) Prove that

$$\mathbf{a}(1) \equiv 0 \pmod{q} \quad \text{if and only if} \quad (x-1) \mid \mathbf{a}(x) \quad \text{in } (\mathbb{Z}/q\mathbb{Z})[x].$$

(b) Suppose that  $\mathbf{a}(1) \equiv 0 \pmod{q}$ . Prove that  $\mathbf{a}(x)$  is not invertible in  $R_q$ .

Solution to Exercise 6.23.

(a) Working in  $(\mathbb{Z}/q\mathbb{Z})[x]$ , we use division with remainder to divide  $\mathbf{a}(x)$  by  $x-1$ . The result is

$$\mathbf{a}(x) = (x-1)\mathbf{b}(x) + \mathbf{r}(x) \quad \text{with } \deg \mathbf{r} < \deg(x-1) = 1.$$

Thus either  $\mathbf{r}(x) = 0$  or  $\deg \mathbf{r}(x) = 0$ , so in any case,  $\mathbf{r}(x)$  is a constant. Thus

$$\mathbf{a}(x) = (x-1)\mathbf{b}(x) + c \quad \text{for some } c \in \mathbb{Z}/q\mathbb{Z}.$$

We can determine  $c$  by substituting  $x = 1$ , which gives  $c = \mathbf{a}(1)$ . Thus

$$\mathbf{a}(x) = (x-1)\mathbf{b}(x) + \mathbf{a}(1).$$

Now (a) is obvious, since this equation shows that  $\mathbf{a}(x)$  is a multiple of  $x-1$  if and only if  $\mathbf{a}(1) = 0$ .

(b) Suppose that  $\mathbf{a}(x)$  is invertible in  $R_q$ , say  $\mathbf{a}(x)\mathbf{b}(x) = 1$  in  $R_q$ . We have a well-defined map  $R_q \rightarrow \mathbb{Z}/q\mathbb{Z}$  defined by evaluating a polynomial at  $x = 1$ . This map is well-defined because the extra relation  $x^N = 1$  is true when we set  $x = 1$ . Further, the map respects addition and multiplication. Hence the relation  $\mathbf{a}(x)\mathbf{b}(x) = 1$  in  $R_q$  leads to the relation  $\mathbf{a}(1)\mathbf{b}(1) = 1$  in  $\mathbb{Z}/q\mathbb{Z}$ . In particular, we certainly can't have  $\mathbf{a}(1) = 0$ . This proves

$$\mathbf{a}(x) \text{ invertible} \implies \mathbf{a}(1) \neq 0,$$

which is equivalent to the statement

$$\mathbf{a}(1) = 0 \implies \mathbf{a}(x) \text{ is not invertible.}$$

**6.24.** Let  $N = 5$  and  $q = 3$  and consider the two polynomials

$$\mathbf{a}(x) = 1 + x^2 + x^3 \in R_3 \quad \text{and} \quad \mathbf{b}(x) = 1 + x^2 - x^3 \in R_3.$$

One of these polynomials has an inverse in  $R_3$  and the other does not. Compute the inverse that exists, and explain why the other doesn't exist.

Solution to Exercise 6.24.

$\mathbf{a}(x)$  does not have an inverse, because  $\mathbf{a}(1) \equiv 0 \pmod{3}$ . The previous exercise then implies that  $\mathbf{a}(x)$  does not have an inverse. Alternatively, using the Euclidean algorithm, one finds that

$$\gcd(\mathbf{a}(x), x^5 - 1) = 1 - x \quad \text{in } (\mathbb{Z}/3\mathbb{Z})[x],$$

so  $\mathbf{a}(x)$  does not have an inverse from Proposition 6.45.

Similarly,  $\gcd(\mathbf{b}(x), x^5 - 1) = 1$  in  $(\mathbb{Z}/3\mathbb{Z})[x]$ , and using the extended Euclidean algorithm, we find that

$$\mathbf{b}(x)^{-1} = 1 - x - x^2 - x^3 \quad \text{in } (\mathbb{Z}/3\mathbb{Z})[x].$$

**6.25.** For each of the following values of  $N$ ,  $q$ , and  $\mathbf{a}(x)$ , either find  $\mathbf{a}(x)^{-1}$  in  $R_q$  or show that the inverse does not exist.

- (a)  $N = 5$ ,  $q = 11$ , and  $\mathbf{a}(x) = x^4 + 8x + 3$ ;
- (b)  $N = 5$ ,  $q = 13$ , and  $\mathbf{a}(x) = x^3 + 2x - 3$ .
- (c)  $N = 7$ ,  $q = 23$ , and  $\mathbf{a}(x) = 20x^6 + 8x^5 + 4x^4 + 15x^3 + 19x^2 + x + 8$ .

*Solution to Exercise 6.25.*

- (a)  $\mathbf{a}(x)^{-1} = 7x^4 + 8x^3 + 3x^2 + 2x + 3$  in  $\mathbb{F}_{11}[x]$ .
- (b)  $\gcd(\mathbf{a}(x), x^5 - 1) = x + 12$  in  $\mathbb{F}_{13}[x]$ , so no inverse.
- (c)  $\mathbf{a}(x)^{-1} = 17x^6 + 4x^5 + 12x^4 + 18x^2 + 12x + 10$  in  $\mathbb{F}_{23}[x]$ .

**6.26.** This exercise illustrates how to find inverses in

$$R_m = \frac{(\mathbb{Z}/m\mathbb{Z})[x]}{(x^N - 1)}$$

when  $m$  is a prime power  $p^e$ .

- (a) Let  $f(x) \in \mathbb{Z}[x]/(X^N - 1)$  be a polynomial, and suppose that we have already found a polynomial  $F(x)$  such that

$$f(x) \star F(x) \equiv 1 \pmod{p^i}$$

for some  $i \geq 1$ . Prove that the polynomial

$$G(x) = F(x) \star (2 - f(x) \star F(x))$$

satisfies

$$f(x) \star G(x) \equiv 1 \pmod{p^{2i}}.$$

- (b) Suppose that we know an inverse of  $f(x)$  modulo  $p$ . Using (a) repeatedly, how many convolution multiplications does it take to compute the inverse of  $f(x)$  modulo  $p^e$ ?
- (c) Use the method in (a) to compute the following inverses modulo  $m = p^e$ , where to ease your task, we have given you the inverse modulo  $p$ .

- (i)  $N = 5, \quad m = 2^4, \quad f(x) = 7 + 3x + x^2,$   
 $f(x)^{-1} \equiv 1 + x^2 + x^3 \pmod{2}.$
- (ii)  $N = 5, \quad m = 2^7, \quad f(x) = 22 + 11x + 5x^2 + 7x^3,$   
 $f(x)^{-1} \equiv 1 + x^2 + x^3 \pmod{2}.$
- (iii)  $N = 7, \quad m = 5^5, \quad f(x) = 112 + 34x + 239x^2 + 234x^3 + 105x^4$   
 $+ 180x^5 + 137x^6,$   
 $f(x)^{-1} \equiv 1 + 3x^2 + 2x^4 \pmod{5}.$

Solution to Exercise 6.26.

(a) We have

$$\begin{aligned} fG - 1 &= f(F(2 - fF)) - 1 \\ &= 2fF - (fF)^2 - 1 \\ &= -(fF - 1)^2. \end{aligned}$$

We are assuming that  $fF \equiv 1 \pmod{p^i}$ , say  $fF = 1 + p^i H$ . Then

$$fG - 1 = -(fF - 1)^2 = p^{2i} H,$$

so  $fG \equiv 1 \pmod{p^{2i}}$ .

(b) Each iteration of (a) takes two convolution multiplications, and each doubles the exponent of  $p$ . So after  $k$  iterations, we've done  $2k$  convolution multiplications and we have an inverse of  $f$  modulo  $p^{2^k}$ . So we need  $2^k \geq e$ , which means that  $k = \lceil \log_2 e \rceil$  (or one less, if  $e$  is a power of 2). Then the number of convolution multiplications is  $2\lceil \log_2 e \rceil$ .

- (c) (i)  $f(x)^{-1} \pmod{2^4} = 13 + 5X^2 + 7X^3 + 10X^4.$   
(ii)  $f(x)^{-1} \pmod{2^7} = 101 + 12X + X^2 + 17X^3 + 34X^4.$   
(iii)  $f(x)^{-1} \pmod{5^5} = 840 + 711X + 710X^2 + 268X^3 + 1710X^4 + 1142X^5 + 2430X^6.$

Section. The NTRU public key cryptosystem

**6.27.** Alice and Bob agree to communicate using the NTRU cryptosystem with

$$(N, p, q) = (7, 2, 37).$$

Alice's private key is

$$\mathbf{f}(x) = x + x^3 + x^6 \quad \text{and} \quad \mathbf{F}_2(x) = 1 + x + x^4 + x^5 + x^6.$$

(You can check that  $\mathbf{f} \star \mathbf{F}_2 \equiv 1 \pmod{2}$ .) Alice receives the ciphertext

$$\mathbf{e}(x) = 1 + 3x + 3x^2 + 4x^3 + 4x^4 + x^5 + 35x^6$$

from Bob. Decipher the message and find the plaintext.

Solution to Exercise 6.27.

Alice first computes

$$\mathbf{a} \equiv \mathbf{f} \star \mathbf{e} \equiv 5 + 5x + 5x^2 + 8x^3 + 8x^4 + 5x^5 + 6x^6 \pmod{37}.$$

Then she computes

$$\begin{aligned} \mathbf{F}_2 \star \mathbf{a} &= 29 + 31x + 31x^2 + 32x^3 + 32x^4 + 29x^5 + 26x^6 \\ &\equiv 1 + x + x^2 + x^5 \pmod{2}. \end{aligned}$$

The plaintext is  $\mathbf{m} = 1 + x + x^2 + x^4 + x^6$ .

**6.28.** Alice and Bob decide to communicate using the NTRU cryptosystem with parameters  $(N, p, q) = (7, 2, 29)$ . Alice's public key is

$$\mathbf{h}(x) = 23 + 23x + 23x^2 + 24x^3 + 23x^4 + 24x^5 + 23x^6.$$

Bob sends Alice the plaintext message  $\mathbf{m}(x) = 1 + x^5$  using the ephemeral key  $\mathbf{r}(x) = 1 + x + x^3 + x^6$ .

- (a) What ciphertext does Bob send to Alice?
- (b) Alice's secret key is  $\mathbf{f}(x) = 1 + x + x^2 + x^4 + x^5$  and  $\mathbf{F}_2(x) = 1 + x^5 + x^6$ . Check your answer in (a) by using  $\mathbf{f}$  and  $\mathbf{F}_2$  to decrypt the message.

Solution to Exercise 6.28.

- (a)  $\mathbf{c} \equiv 2\mathbf{r} \star \mathbf{h} + \mathbf{m} \equiv 11 + 12x + 12x^2 + 12x^3 + 14x^4 + 13x^5 + 14x^6 \pmod{29}$ .
- (b) First compute

$$\mathbf{b} \equiv \mathbf{f} \star \mathbf{c} \equiv 4 + 5x + 4x^2 + 5x^3 + 5x^4 + 4x^5 + 7x^6 \pmod{37}.$$

Then compute

$$\begin{aligned} \mathbf{F}_2 \star \mathbf{b} &= 13 + 14x + 14x^2 + 14x^3 + 16x^4 + 15x^5 + 16x^6 \\ &\equiv 1 + x^5 \pmod{2}. \end{aligned}$$

This agrees with the plaintext.

**6.29.** What is the message expansion of NTRU in terms of  $N$ ,  $p$ , and  $q$ ?

Solution to Exercise 6.29.

The plaintext is  $N$  numbers modulo  $p$ , so consists of  $N \log_2(p)$  bits. The ciphertext is  $N$  numbers modulo  $q$ , so consists of  $N \log_2(q)$  bits. Hence the message expansion of NTRU is  $\log_2(q)/\log_2(p)$ .

**6.30.** The guidelines for choosing NTRU public parameters  $(N, p, q, d)$  require that  $\gcd(p, q) = 1$ . Prove that if  $p \mid q$ , then it is very easy for Eve to decrypt the message without knowing the private key. (*Hint.* First do the case that  $p = q$ .)

Solution to Exercise 6.30.

We always have

$$\mathbf{e}(x) \equiv p\mathbf{r}(x)\mathbf{h}(x) + \mathbf{m}(x) \equiv \mathbf{m}(x) \pmod{q}.$$

If  $p = q$ , then this reduces to  $\mathbf{e}(x) = \mathbf{m}(x)$ , so the ciphertext is equal to the plaintext. In general, if  $p \mid q$ , then reducing  $\mathbf{e}(x)$  modulo  $p$  gives the plaintext  $\mathbf{m}(x)$ .

**6.31.** Alice uses the NTRU cryptosystem with  $p = 3$  to send messages to Bob.

- (a) Suppose that Alice uses the same ephemeral key  $\mathbf{r}(x)$  to encrypt two different plaintexts  $\mathbf{m}_1(x)$  and  $\mathbf{m}_2(x)$ . Explain how Eve can use the two ciphertexts  $\mathbf{e}_1(x)$  and  $\mathbf{e}_2(x)$  to determine approximately  $\frac{2}{9}$  of the coefficients of  $\mathbf{m}_1(x)$ . (See Exercise 6.34 for a way to exploit this information.)
- (b) For example, suppose that  $N = 8$ , so there are  $3^8$  possibilities for  $\mathbf{m}_1(x)$ . Suppose that Eve intercepts two ciphertexts

$$\begin{aligned}\mathbf{e}_1(x) &= 32 + 21x - 9x^2 - 20x^3 - 29x^4 - 29x^5 - 19x^6 + 38x^7, \\ \mathbf{e}_2(x) &= 33 + 21x - 7x^2 - 19x^3 - 31x^4 - 27x^5 - 19x^6 + 38x^7,\end{aligned}$$

that were encrypted using the same ephemeral key  $\mathbf{r}(x)$ . How many coefficients of  $\mathbf{m}_1(x)$  can she determine exactly? How many possibilities are there for  $\mathbf{m}_1(x)$ ?

- (c) Formulate a similar attack if Alice uses two different ephemeral keys  $\mathbf{r}_1(x)$  and  $\mathbf{r}_2(x)$  to encrypt the same plaintext  $\mathbf{m}(x)$ . (*Hint.* Do it first assuming that  $\mathbf{h}(x)$  has an inverse in  $R_q$ . The problem is harder without this assumption.)

Solution to Exercise 6.31.

- (a) Eve computes

$$\begin{aligned}\mathbf{e}_1(x) - \mathbf{e}_2(x) &\equiv (\mathbf{r}(x) \star \mathbf{h}(x) + \mathbf{m}_1(x)) - (\mathbf{r}(x) \star \mathbf{h}(x) + \mathbf{m}_2(x)) \pmod{q} \\ &\equiv \mathbf{m}_1(x) - \mathbf{m}_2(x) \pmod{q}.\end{aligned}$$

The coefficients of  $\mathbf{m}_1(x) - \mathbf{m}_2(x)$  are in the set  $\{-2, -1, 0, 1, 2\}$ , so since  $q > 5$ , Eve recovers  $\mathbf{m}_1(x) - \mathbf{m}_2(x)$  exactly. Any coefficient that is nonzero limits the possibilities for that coefficient of  $\mathbf{m}_1(x)$ . (This is the same as the analogous GGH exercise.)

More precisely, Eve can recover the  $i^{\text{th}}$  coefficient of  $\mathbf{m}_1(x)$  if the  $i^{\text{th}}$  coefficient of both  $\mathbf{m}_1(x)$  and  $\mathbf{m}_2(x)$  are both  $+1$  or both  $-1$ . Assuming that the coefficients are random, the probability of this happening is  $2 \cdot \frac{1}{3} \cdot \frac{1}{3} = \frac{2}{9}$ . So Eve recovers approximately  $\frac{2}{9}$  of the coefficients of  $\mathbf{m}_1(x)$ .

- (b) Eve finds that

$$\mathbf{m}_1(x) - \mathbf{m}_2(x) = \mathbf{e}_1(x) - \mathbf{e}_2(x) = -1 - 2x^2 - x^3 + 2x^4 - 2x^5$$

The coefficients of  $x^2$ ,  $x^4$  and  $x^5$  for  $\mathbf{m}_1$  are determined, they are  $-x^2 + x^4 - x^5$ . So Eve knows three of the coefficients of  $\mathbf{m}_1$ .

More generally,  $\mathbf{m}_1(x)$  looks like

$$A + Bx - x^2 + Cx^3 + x^4 - x^5 + Dx^6 + Ex^7.$$

Further, Eve knows that  $A \in \{0, 1\}$  and  $C \in \{0, 1\}$ . So there are  $2 \cdot 3 \cdot 2 \cdot 3 \cdot 3 = 108$  possibilities for  $\mathbf{m}_1(x)$ , which is much smaller than  $3^8 = 6561$ .

(c) If  $\mathbf{h}(x)$  is invertible in  $R_q$ , then Eve can compute

$$\begin{aligned} \mathbf{h}(x)^{-1}(\mathbf{e}_1(x) - \mathbf{e}_2(x)) &= \mathbf{h}(x)^{-1}(p\mathbf{r}_1(x)\mathbf{h}(x) - p\mathbf{r}_2(x)\mathbf{h}(x)) \pmod{q} \\ &= \mathbf{r}_1(x) - \mathbf{r}_2(x) \pmod{q}. \end{aligned}$$

Then the analysis is the same as in (a), since  $\mathbf{r}_1$  and  $\mathbf{r}_2$  have ternary coefficients.

In general, however,  $\mathbf{h}(x)$  is not invertible, since  $\mathbf{g}(x)$  is not invertible, since  $\mathbf{g}(1) = 0$ . One way around this problem is to develop a theory of “almost inverses” based on the fact that the ring  $\mathbb{Z}[x]/(x^N - 1)$  is isomorphic to  $\mathbb{Z} \times \mathbb{Z}[x]/(\Phi(x))$ , where  $\Phi(x) = x^{N-1} + x^{N-2} + \dots + x + 1$ . The image of  $g(x)$  in the product ring is  $(0, \overline{g(x)})$ , so one inverts the second factor.

Section. NTRU as a lattice cryptosystem

**6.32.** This exercise explains how to formulate NTRU message recovery as a closest vector problem. Let  $\mathbf{h}(x)$  be an NTRU public key and let

$$\mathbf{e}(x) \equiv p\mathbf{r}(x) \star \mathbf{h}(x) + \mathbf{m}(x) \pmod{q}$$

be a message encrypted using  $\mathbf{h}(x)$ .

- Prove that the vector  $(p\mathbf{r}, \mathbf{e} - \mathbf{m})$  is in  $L_{\mathbf{h}}^{\text{NTRU}}$ .
- Prove that the lattice vector in (a) is almost certainly the closest lattice vector to the known vector  $(0, \mathbf{e})$ . Hence solving CVP reveals the plaintext  $\mathbf{m}$ . (For simplicity, you may assume that  $d \approx N/3$  and  $q \approx 2N$ , as we did in Proposition 6.61.)
- Show how one can reduce the lattice-to-target distance, without affecting the determinant, by using instead a modified NTRU lattice of the form

$$\begin{pmatrix} 1 & p\mathbf{h} \\ 0 & q \end{pmatrix}.$$

*Solution to Exercise 6.32.*

- By the definition of  $\mathbf{e}$ , we can find a polynomial  $\mathbf{v}(x)$  satisfying

$$\mathbf{e} = p\mathbf{r} \star \mathbf{h} + \mathbf{m} + q\mathbf{v}(x).$$

Thus



$$\begin{aligned}
(p\mathbf{r}, \mathbf{v})M_{\mathbf{h}}^{\text{NTRU}} &= (p\mathbf{r}, \mathbf{v}) \begin{pmatrix} 1 & \mathbf{h} \\ 0 & q \end{pmatrix} \\
&= (p\mathbf{r}, p\mathbf{r} \star \mathbf{h} + q\mathbf{v}) \\
&= (p\mathbf{r}, \mathbf{e} - \mathbf{m}).
\end{aligned}$$

This shows that  $(p\mathbf{r}, \mathbf{e} - \mathbf{m})$  is in the NTRU lattice  $L_{\mathbf{h}}^{\text{NTRU}}$  spanned by the rows of  $M_{\mathbf{h}}^{\text{NTRU}}$ . Also notice that

$$(p\mathbf{r}, \mathbf{e} - \mathbf{m}) = \overbrace{(0, \mathbf{e})}^{\text{Eve knows this vector}} + \overbrace{(p\mathbf{r}, -\mathbf{m})}^{\text{a short vector}}.$$

(b) We have

$$\begin{aligned}
\|(p\mathbf{r}, \mathbf{e} - \mathbf{m}) - (0, \mathbf{e})\| &= \|(p\mathbf{r}, -\mathbf{m})\| \\
&= \sqrt{p^2 \cdot 2d + 2d} \\
&\approx \sqrt{(p^2 + 1)2N/3}.
\end{aligned}$$

Since  $p$  is small, typically 2 or 3, this is between  $1.83\sqrt{N}$  and  $2.58\sqrt{N}$ . But as in the Proposition, the Gaussian heuristic predicts that a random CVP has a solution of size approximately  $\sigma(L_{\mathbf{h}}^{\text{NTRU}}) \approx 0.484N$ .

(c) Let

$$A_{\mathbf{h}}^{\text{NTRU}} = \begin{pmatrix} 1 & p\mathbf{h} \\ 0 & q \end{pmatrix}.$$

Then with notation as in (a), we have

$$\begin{aligned}
(\mathbf{r}, \mathbf{v})A_{\mathbf{h}}^{\text{NTRU}} &= (\mathbf{r}, \mathbf{v}) \begin{pmatrix} 1 & p\mathbf{h} \\ 0 & q \end{pmatrix} \\
&= (p\mathbf{r}, p\mathbf{r} \star \mathbf{h} + q\mathbf{v}) \\
&= (p\mathbf{r}, \mathbf{e} - \mathbf{m}).
\end{aligned}$$

This shows that  $(\mathbf{r}, \mathbf{e} - \mathbf{m})$  is in the lattice spanned by the rows of  $A_{\mathbf{h}}^{\text{NTRU}}$ . And  $\det(A_{\mathbf{h}}^{\text{NTRU}}) = q^N$ , which is the same as  $\det(M_{\mathbf{h}}^{\text{NTRU}})$ .

Now reworking (b), we see that

$$\begin{aligned}
\|(\mathbf{r}, \mathbf{e} - \mathbf{m}) - (0, \mathbf{e})\| &= \|(\mathbf{r}, -\mathbf{m})\| \\
&= \sqrt{4d} \approx \sqrt{4N/3} \approx 1.15\sqrt{N}.
\end{aligned}$$

So the distance to the closest vector using this new lattice is less than when using the old lattice.

**6.33.** The guidelines for choosing NTRU public parameters  $(N, p, q, d)$  include the assumption that  $N$  is prime. To see why, suppose (say) that  $N$  is even. Explain how Eve can recover the private key by solving a lattice problem in dimension  $N$ , rather than in dimension  $2N$ . *Hint.* Use the natural map

$$\mathbb{Z}[x]/(x^N - 1) \rightarrow \mathbb{Z}[x]/(x^{N/2} - 1).$$

Solution to Exercise 6.33.

This method of breaking NTRU when  $N$  is composite is due to Craig Gentry, Key recovery and message attacks on NTRU-composite, *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, Lecture Notes in Comput. Sci. **2045**, 182–194, Springer, Berlin, 2001.

**6.34.** Suppose that Bob and Alice are using NTRU to exchange messages and that Eve intercepts a ciphertext  $\mathbf{e}(x)$  for which she already knows part of the plaintext  $\mathbf{m}(x)$ . (This is not a ludicrous assumption; see Exercise 6.31, for example.) More precisely, suppose that Eve knows  $t$  of the coefficients of  $\mathbf{m}(x)$ . Explain how to set up a CVP to find  $\mathbf{m}(x)$  using a lattice of dimension  $2N - 2t$ .

Solution to Exercise 6.34.

*A solution for this exercise is not currently available.*

Section. Lattice reduction algorithms

**6.35.** Let  $\mathbf{b}_1$  and  $\mathbf{b}_2$  be vectors, and set

$$t = \mathbf{b}_1 \cdot \mathbf{b}_2 / \|\mathbf{b}_1\|^2 \quad \text{and} \quad \mathbf{b}_2^* = \mathbf{b}_2 - t\mathbf{b}_1.$$

Prove that  $\mathbf{b}_2^* \cdot \mathbf{b}_1 = 0$  and that  $\mathbf{b}_2^*$  is the projection of  $\mathbf{b}_2$  onto the orthogonal complement of  $\mathbf{b}_1$ .

Solution to Exercise 6.35.

*A solution for this exercise is not currently available.*

**6.36.** Let  $\mathbf{a}$  and  $\mathbf{b}$  be nonzero vectors in  $\mathbb{R}^n$ .

- What value of  $t \in \mathbb{R}$  minimizes the distance  $\|\mathbf{a} - t\mathbf{b}\|$ ? (*Hint.* It's easier to minimize the value of  $\|\mathbf{a} - t\mathbf{b}\|^2$ .)
- What is the minimum distance in (a)?
- If  $t$  is chosen as in (a), show that  $\mathbf{a} - t\mathbf{b}$  is the projection of  $\mathbf{a}$  onto the orthogonal complement of  $\mathbf{b}$ .
- If the angle between  $\mathbf{a}$  and  $\mathbf{b}$  is  $\theta$ , use your answer in (b) to show that the minimum distance is  $\|\mathbf{a}\| \sin \theta$ . Draw a picture illustrating this result.

Solution to Exercise 6.36.

(a) We have

$$\begin{aligned} F(t) &= \|\mathbf{a} - t\mathbf{b}\|^2 \\ &= (\mathbf{a} - t\mathbf{b}) \cdot (\mathbf{a} - t\mathbf{b}) \\ &= \|\mathbf{a}\|^2 - 2t\mathbf{a} \cdot \mathbf{b} + t^2\|\mathbf{b}\|^2. \end{aligned}$$

One can then use calculus (i.e., set  $F'(t) = 0$ ) or complete the square to minimize the value of the quadratic polynomial. The minimizing value of  $t$  is  $t = \frac{\mathbf{a} \cdot \mathbf{b}}{\|\mathbf{b}\|^2}$ .

- Substituting this value of  $t$  and simplifying gives the minimum distance

$$\sqrt{\frac{\|\mathbf{a}\|^2\|\mathbf{b}\|^2 - (\mathbf{a} \cdot \mathbf{b})^2}{\|\mathbf{b}\|^2}}.$$

- (c) A solution for this exercise is not currently available.  
 (d) Substitute  $\mathbf{a} \cdot \mathbf{b} = \|\mathbf{a}\|\|\mathbf{b}\|\cos\theta$  into (b) and use

$$\begin{aligned}\|\mathbf{a}\|^2\|\mathbf{b}\|^2 - (\mathbf{a} \cdot \mathbf{b})^2 &= \|\mathbf{a}\|^2\|\mathbf{b}\|^2 - (\|\mathbf{a}\|\|\mathbf{b}\|\cos\theta)^2 \\ &= \|\mathbf{a}\|^2\|\mathbf{b}\|^2(1 - \cos^2\theta) \\ &= \|\mathbf{a}\|^2\|\mathbf{b}\|^2\sin^2\theta.\end{aligned}$$

**6.37.** Apply Gauss's lattice reduction algorithm (Proposition 6.63) to solve SVP for the following two dimensional lattices having the indicated basis vectors. How many steps does the algorithm take?

- (a)  $\mathbf{v}_1 = (120670, 110521)$  and  $\mathbf{v}_2 = (323572, 296358)$ .  
 (b)  $\mathbf{v}_1 = (174748650, 45604569)$  and  $\mathbf{v}_2 = (35462559, 9254748)$ .  
 (c)  $\mathbf{v}_1 = (725734520, 613807887)$  and  $\mathbf{v}_2 = (3433061338, 2903596381)$ .

Solution to Exercise 6.37.

(a)

Step	$\mathbf{v}_1$	$\mathbf{v}_2$	$m$
1	(120670, 110521)	(323572, 296358)	3
2	(-38438, -35205)	(120670, 110521)	-3
3	(5356, 4906)	(-38438, -35205)	-7
4	(-946, -863)	(5356, 4906)	-6
5	(-320, -272)	(-946, -863)	3
6	(14, -47)	(-320, -272)	3
7	(14, -47)	(-362, -131)	0

The solution to SVP is  $\mathbf{v} = (14, -47)$ .

(b)

Step	$\mathbf{v}_1$	$\mathbf{v}_2$	$m$
1	(35462559, 9254748)	(174748650, 45604569)	5
2	(-2564145, -669171)	(35462559, 9254748)	-14
3	(-435471, -113646)	(-2564145, -669171)	6
4	(48681, 12705)	(-435471, -113646)	-9
5	(2658, 699)	(48681, 12705)	18
6	(837, 123)	(2658, 699)	3
7	(147, 330)	(837, 123)	1
8	(147, 330)	(690, -207)	0

The solution to SVP is  $\mathbf{v} = (147, 330)$ .

(c)

Step	$\mathbf{v}_1$	$\mathbf{v}_2$	$m$
1	(725734520, 613807887)	(3433061338, 2903596381)	5
2	(-195611262, -165443054)	(725734520, 613807887)	-4
3	(-56710528, -47964329)	(-195611262, -165443054)	3
4	(-25479678, -21550067)	(-56710528, -47964329)	2
5	(-5751172, -4864195)	(-25479678, -21550067)	4
6	(-2474990, -2093287)	(-5751172, -4864195)	2
7	(-801192, -677621)	(-2474990, -2093287)	3
8	(-71414, -60424)	(-801192, -677621)	11
9	(-15638, -12957)	(-71414, -60424)	5
10	(6776, 4361)	(-15638, -12957)	-3
11	(4690, 126)	(6776, 4361)	1
12	(4690, 126)	(2086, 4235)	0

The solution to SVP is  $\mathbf{v} = (4690, 126)$ .

**6.38.** Let  $V$  be a vector space, let  $W \subset V$  be a vector subspace of  $V$ , and let  $W^\perp$  be the orthogonal complement of  $W$  in  $V$ .

- Prove that  $W^\perp$  is also a vector subspace of  $V$ .
- Prove that every vector  $\mathbf{v} \in V$  can be written as a sum  $\mathbf{v} = \mathbf{w} + \mathbf{w}'$  for unique vectors  $\mathbf{w} \in W$  and  $\mathbf{w}' \in W^\perp$ . (One says that  $V$  is the *direct sum* of the subspaces  $W$  and  $W^\perp$ .)
- Let  $\mathbf{w} \in W$  and  $\mathbf{w}' \in W^\perp$  and let  $\mathbf{v} = a\mathbf{w} + b\mathbf{w}'$ . Prove that

$$\|\mathbf{v}\|^2 = a^2\|\mathbf{w}\|^2 + b^2\|\mathbf{w}'\|^2.$$

Solution to Exercise 6.38.

*A solution for this exercise is not currently available.*

**6.39.** Let  $L$  be a lattice with basis vectors  $\mathbf{v}_1 = (161, 120)$  and  $\mathbf{v}_2 = (104, 77)$ .

- Is  $(0, 1)$  in the lattice?
- Find an LLL reduced basis.
- Use the reduced basis to find the closest lattice vector to  $(-\frac{9}{2}, 11)$ .

Solution to Exercise 6.39.

*A solution for this exercise is not currently available.*

**6.40.** Use the LLL algorithm to reduce the lattice with basis

$$\mathbf{v}_1 = (20, 16, 3), \quad \mathbf{v}_2 = (15, 0, 10), \quad \mathbf{v}_3 = (0, 18, 9).$$

You should do this exercise by hand, writing out each step.

Solution to Exercise 6.40.

Compute

$$\mu_{2,1} = \frac{300 + 30}{400 + (14)^2 + 64} = \frac{330}{665} < \frac{1}{2}.$$

Checking the Lovász condition for  $\mathbf{v}_2$  amounts to checking that  $\|\mathbf{v}_2\|^2 \geq \frac{3}{4}\|\mathbf{v}_1\|^2$  and  $\|\mathbf{v}_2\|^2 = 225 + 100 = 325$ ,  $\|\mathbf{v}_1\|^2 = 665$ , so swap. Now  $\mathbf{v}_1 = (15, 0, 10)$  and  $\mathbf{v}_2 = (20, 16, 3)$ . Recompute  $\mu_{2,1} = \frac{356}{325}$  and subtract one multiple of  $\mathbf{v}_1$  from  $\mathbf{v}_2$ . New  $\mathbf{v}_2 = (5, 16, -7)$ . Note that the (new)  $\mu_{2,1}$  is now  $(75 - 70)/325 = -5/325$ .

Move on to  $\mathbf{v}_3$  computing

$$\mu_{3,1} = \frac{-75 + 160}{325} = \frac{85}{325} < \frac{1}{2},$$

$$\mu_{3,2} = \frac{225}{330} > \frac{1}{2}.$$

Subtract one multiple of  $\mathbf{v}_2$  from  $\mathbf{v}_3$  obtaining the new  $\mathbf{v}_3 = (-5, 2, 16)$ .

On to the Lovász condition, computing

$$\|\mathbf{v}_3^* + \mu_{3,2}\mathbf{v}_2^*\|^2 = \|\mathbf{v}_3 - \mu_{3,1}\mathbf{v}_1\|^2 = \|(-5, 2, 16) - \frac{85}{325}(15, 0, 10)\|^2 = \|\frac{1}{13}(-14, 26, 174)\|^2.$$

Next compute

$$\|\mathbf{v}_2^*\|^2 = \|\frac{1}{13}(62, 208, 3)\|^2$$

and we find the condition (2) is not satisfied, so we swap. At this point,

$$\mathbf{v}_1 = (15, 0, 10), \quad \mathbf{v}_2 = (-5, 2, 16), \quad \mathbf{v}_3 = (5, 16, -7).$$

Checking condition (2) for (the new)  $\mathbf{v}_2$ :  $\|\mathbf{v}_2\|^2 = 285$ , which is larger than  $3/4$  times  $\|\mathbf{v}_1\|^2 = 325$ . (If, instead of  $3/4$ , we had chosen a constant closer to 1, like .99, then we would perform the swap step again. This makes sense since the length of  $\mathbf{v}_2$  is smaller than the length of  $\mathbf{v}_1$ .) Now check the value of

$$\mu_{3,2} = \frac{-105}{285}$$

and the Lovász condition for  $\mathbf{v}_3$ , which is satisfied. So we now have an LLL reduced basis.

**6.41.** Let  $L$  be the lattice generated by the rows of the matrix

$$M = \begin{pmatrix} 20 & 51 & 35 & 59 & 73 & 73 \\ 14 & 48 & 33 & 61 & 47 & 83 \\ 95 & 41 & 48 & 84 & 30 & 45 \\ 0 & 42 & 74 & 79 & 20 & 21 \\ 6 & 41 & 49 & 11 & 70 & 67 \\ 23 & 36 & 6 & 1 & 46 & 4 \end{pmatrix}.$$

Implement the LLL algorithm (Figure 6.7) on a computer and use your program to answer the following questions.

- (a) Compute  $\det(L)$  and  $\mathcal{H}(M)$ . What is the shortest basis vector?

- (b) Apply LLL to  $M$ . How many swaps (Step [11]) are required? What is the value of  $\mathcal{H}(M^{LLL})$ ? What is the shortest basis vector in the LLL reduced basis? How does it compare with the Gaussian expected shortest length?
- (c) Reverse the order of the rows of  $M$  and apply LLL to the new matrix. How many swaps are required? What is the value of  $\mathcal{H}(M^{LLL})$  and what is the shortest basis vector?
- (d) Apply LLL to the original matrix  $M$ , but in the Lovász condition (Step [8]), use 0.99 instead of  $\frac{3}{4}$ . How many swaps are required? What is the value of  $\mathcal{H}(M^{LLL})$  and what is the shortest basis vector?

Solution to Exercise 6.41.

(a)  $\det(L) = 21242880806$ ,  $\mathcal{H}(M) = 0.45726$ , smallest basis vector is  $\|\mathbf{v}_6\| = 63.198$ ,

(b) The output is

$$\begin{pmatrix} -6 & -3 & -2 & 2 & -26 & 10 \\ 11 & 30 & 2 & 5 & -6 & 24 \\ -14 & -10 & 14 & -48 & -3 & -6 \\ -3 & 24 & 43 & 23 & -33 & -38 \\ 64 & -44 & -16 & -46 & -13 & 4 \\ -28 & -25 & 41 & 5 & 30 & 39 \end{pmatrix}$$

There are 11 swap steps. We have  $\mathcal{H}(M^{LLL}) = 0.91981$  and the shortest vector is  $\|\mathbf{v}_1\| = 28.792$ . Gaussian expected shortest is  $\sigma(L) = 40.0239$ . This suggests that  $\mathbf{v}_1$  is probably the shortest vector in  $L$ .

(c) With the rows in reverse order, the LLL output is

$$\begin{pmatrix} 6 & 3 & 2 & -2 & 26 & -10 \\ 11 & 30 & 2 & 5 & -6 & 24 \\ 14 & 10 & -14 & 48 & 3 & 6 \\ -28 & -25 & 41 & 5 & 30 & 39 \\ -3 & 24 & 43 & 23 & -33 & -38 \\ 47 & -35 & 54 & 30 & -13 & 11 \end{pmatrix}$$

There are 8 swap steps. We have  $\mathcal{H}(M^{LLL}) = 0.94427$  and the shortest vector is  $\|\mathbf{v}_1\| = 28.792$ .

(d) With Lovász condition 0.99,

$$\begin{pmatrix} -6 & -3 & -2 & 2 & -26 & 10 \\ 11 & 30 & 2 & 5 & -6 & 24 \\ -14 & -10 & 14 & -48 & -3 & -6 \\ -3 & 24 & 43 & 23 & -33 & -38 \\ -28 & -25 & 41 & 5 & 30 & 39 \\ 47 & -35 & 54 & 30 & -13 & 11 \end{pmatrix}$$

There are 12 swap steps. We have  $\mathcal{H}(M^{LLL}) = 0.944270$  and the shortest vector is  $\|\mathbf{v}_1\| = 28.792$ . This is the same basis as in (c), in a different order.

**6.42.** A more efficient way to implement the LLL algorithm is described in Figure 6.8, with Reduce and Swap subroutines given in Figure 6.9. (This implementation of LLL follows [26, Algorithm 2.6.3]. We thank Henri Cohen for his permission to include it here.)

- (a) Prove that the algorithm described in Figures 6.8 and 6.9 returns an LLL reduced basis.
- (b) For any given  $N$  and  $q$ , let  $L_{N,q}$  be the  $N$ -dimensional lattice with basis  $\mathbf{v}_1, \dots, \mathbf{v}_N$  described by the formulas

$$\mathbf{v}_i = (r_{i1}, r_{i2}, \dots, r_{iN}), \quad r_{ij} \equiv (i + N)^j \pmod{q}, \quad 0 \leq r_{ij} < q.$$

Implement the LLL algorithm and use it to LLL reduce  $L_{N,q}$  for each of the following values of  $N$  and  $q$ :

- (i)  $(N, q) = (10, 541)$                       (ii)  $(N, q) = (20, 863)$   
 (iii)  $(N, q) = (30, 1223)$                       (iv)  $(N, q) = (40, 3571)$

In each case, compare the Hadamard ratio of the original basis to the Hadamard ratio of the LLL reduced basis, and compare the length of the shortest vector found by LLL to the Gaussian expected shortest length.

*Solution to Exercise 6.42.*

(b) We write  $L$  for the original basis and  $L'$  for the LLL reduced basis, and we write  $\mathbf{v}$  for the shortest vector in the original basis and  $\mathbf{v}'$  for the shortest vector in the LLL reduced basis. Here are the shortest vectors in the LLL reduced basis (N.B. the shortest vector was not always the first vector):

- (i)  $\mathbf{v}' = (-98, 166, -131, -18, 100, 28, 81, 50, -39, -39).$   
 (ii)  $\mathbf{v}' = (-122, -33, -59, 166, 9, -394, -46, 227, -148, -86, -46, 108, -214, 173, -107, 171, 34, -86, -153, -117).$   
 (iii)  $\mathbf{v}' = (98, -148, -263, -370, 76, 53, 258, -128, 221, -435, -119, -59, 142, -336, 311, 290, 89, -538, 16, 437, 108, 361, 322, -374, 56, -117, -208, -131, 645, 42).$   
 (iv)  $\mathbf{v}' = (192, -1426, 552, -292, 52, 482, 1046, -1344, -414, -226, -1413, -1466, -447, 653, -484, -553, -284, 232, 1975, 1944, 27, 1203, -1363, 707, 91, -549, -831, 974, 768, 1074, 57, -966, 1997, 2099, 828, -1295, -972, -842, 185, -2271).$

The lengths, Hadamard ratios, and Gaussian expected shortest lengths are given in the following table:

	$\ \mathbf{v}\ $	$\ \mathbf{v}'\ $	$\mathcal{H}(L)$	$\mathcal{H}(L')$	$\sigma(L)$
(i)	632.369	278.446	0.309773	0.853005	241.775
(ii)	1846.49	679.056	0.253273	0.694868	659.505
(iii)	3133.91	1505.95	0.304603	0.579003	1613.89
(iv)	10711.4	6706.75	0.281214	0.470440	5775.49

```

[1]  Input a basis  $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$  for a lattice  $L$ 
[2]  Set  $k = 2$ ,  $k_{\max} = 1$ ,  $\mathbf{v}_1^* = \mathbf{v}_1$ , and  $B_1 = \|\mathbf{v}_1\|^2$ 
[3]  If  $k \leq k_{\max}$  go to Step [9]
[4]  Set  $k_{\max} = k$  and  $\mathbf{v}_k^* = \mathbf{v}_k$ 
[5]  Loop  $j = 1, 2, \dots, k-1$ 
[6]      Set  $\mu_{k,j} = \mathbf{v}_k \cdot \mathbf{v}_j^* / B_j$  and  $\mathbf{v}_k^* = \mathbf{v}_k^* - \mu_{k,j} \mathbf{v}_j^*$ 
[7]  End  $j$  Loop
[8]  Set  $B_k = \|\mathbf{v}_k^*\|^2$ 
[9]  Execute Subroutine RED( $k, k-1$ )
[10] If  $B_k < \left(\frac{3}{4} - \mu_{k,k-1}^2\right) B_{k-1}$ 
[11]     Execute Subroutine SWAP( $k$ )
[12]     Set  $k = \max(2, k-1)$  and go to Step [9]
[13] Else
[14]     Loop  $\ell = k-2, k-3, \dots, 2, 1$ 
[15]         Execute Subroutine RED( $k, \ell$ )
[16]     End  $\ell$  Loop
[17]     Set  $k = k+1$ 
[18] End If
[19] If  $k \leq n$  go to Step [3]
[20] Return LLL reduced basis  $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ 

```

Figure 6.1: The LLL algorithm—Main routine

**6.43.** Let  $\frac{1}{4} < \alpha < 1$  and suppose that we replace the Lovász condition with the condition

$$\|\mathbf{v}_i^*\|^2 \geq (\alpha - \mu_{i,i-1}^2) \|\mathbf{v}_{i-1}^*\|^2 \quad \text{for all } 1 < i \leq n.$$

- (a) Prove a more version of Theorem 6.66. What quantity, depending on  $\alpha$ , replaces the 2 that appears in the estimates (6.53), (6.54), and (6.55)?
- (b) Prove a version of Theorem 6.68. In particular, how does the upper bound for the number of swap steps depend on  $\alpha$ ? What happens as  $\alpha \rightarrow 1$ ?

Solution to Exercise 6.43.

*A solution for this exercise is not currently available.*

**6.44.** Let  $\mathbf{v}_1, \dots, \mathbf{v}_n$  be an LLL reduced basis for a lattice  $L$ .

- (a) Prove that there are constants  $C_1 > 1 > C_2 > 0$  such that for all  $y_1, \dots, y_n \in \mathbb{R}$  we have

$$C_1^n \sum_{i=1}^n y_i^2 \|\mathbf{v}_i\|^2 \geq \left\| \sum_{i=1}^n y_i \mathbf{v}_i \right\|^2 \geq C_2^n \sum_{i=1}^n y_i^2 \|\mathbf{v}_i\|^2. \quad (6.3)$$

(This is a hard exercise.) We observe that the inequality (6.63) is another way of saying that the basis  $\mathbf{v}_1, \dots, \mathbf{v}_n$  is quasi-orthogonal, since if it



```

      — Subroutine RED( $k, \ell$ ) —
[1] If  $|\mu_{k,\ell}| \leq \frac{1}{2}$ , return to Main Routine
[2] Set  $m = \lfloor \mu_{k,\ell} \rfloor$ 
[3] Set  $\mathbf{v}_k = \mathbf{v}_k - m\mathbf{v}_\ell$  and  $\mu_{k,\ell} = \mu_{k,\ell} - m$ 
[4] Loop  $i = 1, 2, \dots, \ell - 1$ 
[5]     Set  $\mu_{k,i} = \mu_{k,i} - m\mu_{\ell,i}$ 
[6] End  $i$  Loop
[7] Return to Main Routine

      — Subroutine SWAP( $k$ ) —
[1] Exchange  $\mathbf{v}_{k-1}$  and  $\mathbf{v}_k$ 
[2] Loop  $j = 1, 2, \dots, k - 2$ 
[3]     Exchange  $\mu_{k-1,j}$  and  $\mu_{k,j}$ 
[4] End  $j$  Loop
[5] Set  $\mu = \mu_{k,k-1}$  and  $B = B_k - \mu^2 B_{k-1}$ 
[6] Set  $\mu_{k,k-1} = \mu B_{k-1}/B$  and  $B_k = B_{k-1} B_k/B$  and  $B_{k-1} = B$ 
[7] Loop  $i = k + 1, k + 2, \dots, k_{\max}$ 
[8]     Set  $m = \mu_{i,k}$  and  $\mu_{i,k} = \mu_{i,k-1} - \mu m$  and  $\mu_{i,k-1} = m + \mu_{k,k-1} \mu_{i,k}$ 
[9] End  $i$  Loop
[10] Return to Main Routine

```

Figure 6.2: The LLL algorithm—RED and SWAP subroutines

were truly orthogonal, then we would have an equality  $\|\sum y_i \mathbf{v}_i\|^2 = \sum y_i^2 \|\mathbf{v}_i\|^2$ .

- (b) Prove that there is a constant  $C$  such that for any target vector  $\mathbf{w} \in \mathbb{R}^n$ , Babai's algorithm (Theorem 6.34) finds a lattice vector  $\mathbf{v} \in L$  satisfying

$$\|\mathbf{w} - \mathbf{v}\| \leq C^n \min_{\mathbf{u} \in L} \|\mathbf{w} - \mathbf{u}\|.$$

Thus Babai's algorithm applied with an LLL reduced basis solves **ap-prCVP** to within a factor of  $C^n$ . This is Theorem 6.73.

- (c) Find explicit values for the constants  $C_1$ ,  $C_2$ , and  $C$  in (a) and (b).

*Solution to Exercise 6.44.*

- (a) This is a hard exercise. We follow the proof given in [?, §5.7].

Fix a basis  $\mathbf{v}_1, \dots, \mathbf{v}_n$ , let  $\mathbf{v}_1^*, \dots, \mathbf{v}_n^*$  be the associated Gram–Schmidt orthogonalized basis, and let

$$\mathbf{e}_i = \mathbf{v}_i^* / \|\mathbf{v}_i^*\|, \quad 1 \leq i \leq n,$$

be the associated orthonormal basis. Let  $\mu_{i,j}$  be as usual (setting  $\mu_{i,i} = 1$  and  $\mu_{i,j} = 0$  for  $i > j$ ), so the change of basis matrix  $M = (\mu_{i,j})$  satisfies

$$V = V^* M.$$

(The rows of  $V$  are  $\mathbf{v}_1, \dots, \mathbf{v}_n$  and the rows of  $V^*$  are  $\mathbf{v}_1^*, \dots, \mathbf{v}_n^*$ .)

In general, for any linear transformation  $A$ , we write  $A = (a_{i,j})$  as a matrix relative to the orthonormal basis  $\mathbf{e}_1^*, \dots, \mathbf{e}_n^*$  and define

$$\|A\| = \sup_{\mathbf{0} \neq \mathbf{v} \in \mathbb{R}^n} \frac{\|\mathbf{v}A\|}{\|\mathbf{v}\|} \quad \text{and} \quad \|A\|_{\mathbf{e}} = \sup_{i,j} |a_{i,j}|.$$

We observe that if  $\mathbf{v} = \sum x_i \mathbf{e}_i^*$ , then  $\|\mathbf{v}\|^2 = \sum x_i^2$  and we have

$$\begin{aligned} \|\mathbf{v}A\|^2 &= \left\| \sum_{i=1}^n x_i \sum_{j=1}^n a_{i,j} \mathbf{e}_j \right\|^2 \\ &= \sum_{j=1}^n \left( \sum_{i=1}^n x_i a_{i,j} \right)^2 \\ &\leq \sum_{j=1}^n \|\mathbf{v}\|^2 \|\mathbf{a}_{\cdot,j}\|^2 \quad (\text{Cauchy-Schwartz}), \\ &\leq \sum_{j=1}^n \|\mathbf{v}\|^2 n \|A\|_{\mathbf{e}}^2 \\ &= n^2 \|A\|_{\mathbf{e}}^2 \|\mathbf{v}\|^2. \end{aligned}$$

Taking square roots, dividing by  $\|\mathbf{v}\|$ , and taking the sup over nonzero  $\mathbf{v}$  yields

$$\|A\| \leq n \|A\|_{\mathbf{e}}.$$

To ease notation, we let

$$c_i = \|\mathbf{v}_i^*\|, \quad \text{so} \quad \mathbf{v}_i^* = c_i \mathbf{e}_i.$$

Now we compute

$$\begin{aligned} \mathbf{e}_i M &= c_i^{-1} \mathbf{v}_i^* M = c_i^{-1} \mathbf{v}_i = c_i^{-1} \left( \mathbf{v}_i^* + \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{v}_j^* \right) = c_i^{-1} \left( c_i \mathbf{e}_i + \sum_{j=1}^{i-1} \mu_{i,j} c_j \mathbf{e}_j \right) \\ &= \mathbf{e}_i + \sum_{j=1}^{i-1} \mu_{i,j} c_i^{-1} c_j \mathbf{e}_j. \end{aligned}$$

So relative to the  $\mathbf{e}$  basis, the linear transformation  $M$  has a matrix that is lower triangular with 1's on the diagonal and with  $ij^{\text{th}}$  entry satisfying

$$|\mu_{i,j} c_i^{-1} c_j| \leq \frac{1}{2} \cdot \frac{\|\mathbf{v}_j^*\|}{\|\mathbf{v}_i^*\|} \leq 2^{(i-j)/2-1}, \quad (6.4)$$

where for the last inequality we use (6.57) (N.B. This is where we use the fact that the basis is reduced, since the size condition gives  $|\mu_{i,j}| \leq \frac{1}{2}$  and the Lovász condition implies the estimate (6.57).) Therefore,

$$\|M\|_{\mathbf{e}} \leq \max_{1 \leq j \leq i \leq n} 2^{(i-j)/2-1} = 2^{(n-3)/2}.$$

(If  $n \leq 2$ , we need to replace this upper bound by 1.)

This allows us to get an upper bound

$$\begin{aligned} \left\| \sum_{i=1}^n y_i \mathbf{v}_i \right\|^2 &= \|\mathbf{y}V\|^2 = \|\mathbf{y}V^*M\| \leq \|\mathbf{y}V^*\| \|M\| \leq \|\mathbf{y}V^*\| \cdot n \|M\|_{\mathbf{e}} \\ &\leq \|\mathbf{y}V^*\| n 2^{(n-3)/2} = n 2^{(n-3)/2} \sum_{i=1}^n y_i^2 \|\mathbf{v}_i^*\|^2. \end{aligned} \quad (6.5)$$

To obtain a lower bound, we observe that

$$\begin{aligned} \sum_{i=1}^n y_i^2 \|\mathbf{v}_i^*\|^2 &= \|\mathbf{y}V^*\|^2 = \|\mathbf{y}VM^{-1}\|^2 \\ &\leq \|\mathbf{y}V\| \|M^{-1}\|^2 = \|M^{-1}\|^2 \left\| \sum_{i=1}^n y_i \mathbf{v}_i \right\|^2. \end{aligned} \quad (6.6)$$

So we need an upper bound for  $\|M^{-1}\|$ .

Note that

$$M = I - N,$$

where  $N$  is lower triangular with 0's on the diagonal, so  $N$  is nilpotent, and indeed it satisfies  $N^n = 0$ . Hence

$$M^{-1} = I + N + N^2 + \cdots + N^{n-1}.$$

The following lemma provides the necessary estimate. We refer the reader to [?, Lemma 7.10] for the proof.

**Lemma 6.1.** *Let  $B = (b_{i,j})$  be the matrix of a linear transformation relative to an orthonormal basis  $\{\mathbf{e}_i\}$ . Suppose that there are positive constants  $\beta$  and  $\gamma$  so that*

$$b_{i,j} = 0 \text{ for } i \leq j \quad \text{and} \quad |b_{i,j}| \leq \gamma \delta^{j-i} \text{ for } i > j.$$

Then

$$\|B + B^2 + B^3 + \cdots + B^{n-1}\|_{\mathbf{e}} \leq \gamma(\gamma + 1)^{n-2} \delta^{n-1}.$$

Note that (??) tells us that the coefficients of  $N$  satisfy

$$|\text{coef. of } N| \leq 2^{(i-j)/2-1} = \frac{1}{2} \cdot \left( \frac{1}{\sqrt{2}} \right)^{j-i}.$$

So we can apply the lemma to  $N$  with  $\gamma = 1/2$  and  $\delta = 1/\sqrt{2}$ , which gives

$$\|N + N^2 + \cdots + N^{n-1}\|_{\mathbf{e}} \leq \frac{1}{2} \cdot \left( \frac{3}{2} \right)^{n-2} \cdot \left( \frac{1}{\sqrt{2}} \right)^{n-1} = \frac{1}{3} \left( \frac{9}{8} \right)^{(n-1)/2}.$$

Hence

$$\begin{aligned}\|M^{-1}\| &\leq n \|M^{-1}\|_{\mathbf{e}} \leq n (1 + \|N + N^2 + \dots + N^{n-1}\|_{\mathbf{e}}) \\ &\leq n + \frac{n}{3} \left(\frac{9}{8}\right)^{(n-1)/2} \leq n \left(\frac{9}{8}\right)^{(n-1)/2}.\end{aligned}$$

(The last inequality is valid for  $n \geq 8$ . For smaller  $n$ , one can put in a small correction factor.)

Substituting into (??) gives

$$\sum_{i=1}^n y_i^2 \|\mathbf{v}_i^*\|^2 \leq n^2 \left(\frac{9}{8}\right)^{n-1} \left\| \sum_{i=1}^n y_i \mathbf{v}_i \right\|^2. \quad (6.7)$$

We now apply (6.54) from Theorem 6.66, which says that  $\|\mathbf{v}_i^*\|^2 \geq 2^{-(i-1)} \|\mathbf{v}_i\|^2$ . This yields

$$\left\| \sum_{i=1}^n y_i \mathbf{v}_i \right\|^2 \geq n^{-2} \left(\frac{8}{9}\right)^{n-1} \sum_{i=1}^n y_i^2 \cdot 2^{-(i-1)} \|\mathbf{v}_i\|^2 \geq n^{-2} \left(\frac{4}{9}\right)^{n-1} \sum_{i=1}^n y_i^2 \|\mathbf{v}_i\|^2.$$

(b) Let  $\mathbf{a} = \sum a_i \mathbf{v}_i \in L$  be any lattice vector, for example, it could be the lattice vector that is closest to  $\mathbf{w}$ . Write

$$\mathbf{w} = \sum \beta_i \mathbf{v}_i \quad \text{with } \beta_i \in \mathbb{R},$$

and let

$$\mathbf{b} = \sum b_i \mathbf{v}_i \quad \text{with } b_i = \lfloor \beta_i \rfloor$$

be the vector returned by Babai's algorithm. Also write

$$\beta_i = b_i + \delta_i \quad \text{with } |\delta_i| \leq \frac{1}{2}.$$

Then

$$\begin{aligned}\|\mathbf{w} - \mathbf{a}\|^2 &= \left\| \sum (\beta_i - a_i) \mathbf{v}_i \right\|^2 \\ &\geq C_2^n \sum (\beta_i - a_i)^2 \|\mathbf{v}_i\|^2 && \text{from (6.63),} \\ &= C_2^n \sum (b_i - a_i + \delta_i)^2 \|\mathbf{v}_i\|^2.\end{aligned}$$

If  $a_i \neq b_i$ , then  $|b_i - a_i| \geq 1$ , so

$$(b_i - a_i + \delta_i)^2 \geq \frac{1}{4} (b_i - a_i)^2,$$

and clearly this is also valid if  $a_i = b_i$ . Hence using the other inequality in (6.63),

```

Input a basis  $\mathbf{v}_1, \dots, \mathbf{v}_n$  of a lattice  $L$ .
Input a target vector  $\mathbf{t}$ .
Compute Gram–Schmidt orthogonalized vectors  $\mathbf{v}_1^*, \dots, \mathbf{v}_n^*$  (Theorem 6.13).
Set  $\mathbf{w} = \mathbf{t}$ .
Loop  $i = n, n-1, \dots, 2, 1$ 
    Set  $\mathbf{w} = \mathbf{w} - \lfloor \mathbf{w} \cdot \mathbf{v}_i^* / \|\mathbf{v}_i^*\|^2 \rfloor \mathbf{v}_i$ .
End  $i$  Loop
Return the lattice vector  $\mathbf{t} - \mathbf{w}$ .

```

Figure 6.3: Babai’s closest plane algorithm

$$\begin{aligned}
\|\mathbf{w} - \mathbf{a}\|^2 &\geq C_2^n \sum \frac{1}{4} (b_i - a_i)^2 \|\mathbf{v}_i\|^2 \\
&\geq \frac{1}{4} C_2^n C_1^{-n} \left\| \sum (b_i - a_i) \mathbf{v}_i \right\|^2 \\
&= \frac{1}{4} C_2^n C_1^{-n} \|\mathbf{b} - \mathbf{a}\|^2.
\end{aligned}$$

Using the triangle inequality, we find that

$$\|\mathbf{w} - \mathbf{a}\| \geq \frac{1}{2} (C_2/C_1)^{n/2} \|\mathbf{b} - \mathbf{a}\| \geq \frac{1}{2} (C_2/C_1)^{n/2} (\|\mathbf{b} - \mathbf{w}\| - \|\mathbf{w} - \mathbf{a}\|),$$

and now a little bit of algebra yields

$$\|\mathbf{w} - \mathbf{b}\| \leq \left( 2 \left( \frac{C_1}{C_2} \right)^{n/2} + 1 \right) \|\mathbf{w} - \mathbf{a}\|.$$

This shows that the Babai vector  $\mathbf{b}$  is the closest vector to  $\mathbf{w}$  up to a factor of  $2(C_1/C_2)^{n/2} + 1$ .

**6.45.** Babai’s *Closest Plane Algorithm*, which is described in Figure 6.10, is an alternative rounding method that uses a given basis to solve **apprCVP**. As usual, the more orthogonal the basis, the better the solution, so generally people first use LLL to create a quasi-orthogonal basis and then apply one of Babai’s methods. In both theory and practice, Babai’s closest plane algorithm seems to yield better results than Babai’s closest vertex algorithm.

Implement both of Babai’s algorithms (Theorem 6.34 and Figure 6.10) and use them to solve **apprCVP** for each of the following lattices and target vectors. Which one gives the better result?

- (a)  $L$  is the lattice generated by the rows of the matrix

$$M_L = \begin{pmatrix} -5 & 16 & 25 & 25 & 13 & 8 \\ 26 & -3 & -11 & 14 & 5 & -26 \\ 15 & -28 & 16 & -7 & -21 & -4 \\ 32 & -3 & 7 & -30 & -6 & 26 \\ 15 & -32 & -17 & 32 & -3 & 11 \\ 5 & 24 & 0 & -13 & -46 & 15 \end{pmatrix}$$

and the target vector is  $\mathbf{t} = (-178, 117, -407, 419, -4, 252)$ . (Notice that the matrix  $M_L$  is LLL reduced.)

- (b)  $L$  is the lattice generated by the rows of the matrix

$$M_L = \begin{pmatrix} -33 & -15 & 22 & -34 & -32 & 41 \\ 10 & 9 & 45 & 10 & -6 & -3 \\ -32 & -17 & 43 & 37 & 29 & -30 \\ 26 & 13 & -35 & -41 & 42 & -15 \\ -50 & 32 & 18 & 35 & 48 & 45 \\ 2 & -5 & -2 & -38 & 38 & 41 \end{pmatrix}$$

and the target vector is  $\mathbf{t} = (-126, -377, -196, 455, -200, -234)$ . (Notice that the matrix  $M_L$  is not LLL reduced.)

- (c) Apply LLL reduction to the basis in (b), and then use both of Babai's methods to solve **apprCVP**. Do you get better solutions?

Solution to Exercise 6.45.

- (a) The Closest Plane Algorithm gives the vector

$$\mathbf{w} = (-185, 105, -414, 419, -8, 277) = (-1, -4, -13, -3, 12, 5)M_L \in L.$$

It satisfies  $\|\mathbf{t} - \mathbf{w}\| = 29.7153$ . The Closest Vertex Algorithm gives the vector

$$\mathbf{w} = (-159, 102, -425, 433, -3, 251) = (-1, -3, -13, -3, 12, 5)M_L \in L.$$

It satisfies  $\|\mathbf{t} - \mathbf{w}\| = 33.2866$ . So the Closest Plane Algorithm gives a slightly better result than the Closest Vertex Algorithm.

- (b) The Closest Plane Algorithm gives the vector

$$\mathbf{w} = (-166, -394, -203, 460, -196, -204) = (-6, -13, 4, -12, -4, 3)M_L \in L.$$

It satisfies  $\|\mathbf{t} - \mathbf{w}\| = 53.6563$ . The Closest Vertex Algorithm gives the vector

$$\mathbf{w} = (-156, -385, -158, 470, -202, -207) = (-6, -12, 4, -12, -4, 3)M_L \in L.$$

It satisfies  $\|\mathbf{t} - \mathbf{w}\| = 58.0172$ . So the Closest Plane Algorithm gives a slightly better result than the Closest Vertex Algorithm.

- (c) The LLL reduced basis is

$$\begin{pmatrix} 10 & 9 & 45 & 10 & -6 & -3 \\ 9 & -3 & 11 & 37 & 28 & 15 \\ -24 & -18 & 33 & 3 & -4 & 56 \\ 2 & -5 & -2 & -38 & 38 & 41 \\ -41 & -14 & 32 & 0 & 1 & -45 \\ -35 & 53 & -26 & -5 & 24 & -26 \end{pmatrix}$$

The Closest Plane Algorithm gives the vector

$$\mathbf{w} = (-132, -367, -191, 467, -198, -263) = (-12, 6, 1, -9, 4, -4)M_L \in L.$$

It satisfies  $\|\mathbf{t} - \mathbf{w}\| = 33.9116$ . The Closest Vertex Algorithm gives the exact same result. So starting with an LLL reduced basis yields a significantly better solution to  $\text{apprCVP}$ .

Section. Applications of LLL to cryptanalysis

**6.46.** You have been spying on George for some time and overhear him receiving a ciphertext  $e = 83493429501$  that has been encrypted using the congruential cryptosystem described in Section 6.1. You also know that George's public key is  $h = 24201896593$  and the public modulus is  $q = 148059109201$ . Use Gaussian lattice reduction to recover George's private key  $(f, g)$  and the message  $m$ .

*Solution to Exercise 6.46.*

Gaussian lattice reduction on the lattice generated by

$$(1, 24201896593) \quad \text{and} \quad (0, 148059109201)$$

gives the short basis

$$(233444, 255333) \quad \text{and} \quad (330721, -272507),$$

so the private key is

$$f = 233444 \quad \text{and} \quad g = 255333.$$

We check that

$$f^{-1}g \equiv 133037176740 \cdot 255333 \equiv 24201896593 \equiv h \pmod{q}.$$

In order to decrypt the message, we first compute

$$a \equiv fe \equiv 94843884201 \pmod{q}.$$

Then we do a computation modulo  $g$  to recover the plaintext  $m$ ,

$$m = f^{-1}a = 94649 \cdot 94843884201 \equiv 186000 \pmod{g}.$$

**6.47.** Let

$$\mathbf{M} = (81946, 80956, 58407, 51650, 38136, 17032, 39658, 67468, 49203, 9546)$$

and let  $S = 168296$ . Use the LLL algorithm to solve the subset-sum problem for  $\mathbf{M}$  and  $S$ , i.e., find a subset of the elements of  $\mathbf{M}$  whose sum is  $S$ .

*Solution to Exercise 6.47.*

We apply LLL to the matrix

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 81946 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 80956 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 58407 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 51650 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 38136 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 17032 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 39658 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 67468 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 49203 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 9546 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 168296 \end{pmatrix}.$$

It takes LLL 102 swaps to find the reduced matrix

$$\begin{pmatrix} 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 0 \\ 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 3 & 1 & 1 & 3 & 1 & 1 & 1 & -3 & 1 & -1 & 0 \\ 3 & 1 & 1 & -1 & 3 & 1 & -3 & 1 & 1 & 1 & 2 \\ -2 & 0 & 2 & -2 & 4 & 0 & 2 & 2 & 2 & 0 & 2 \\ -2 & -2 & 4 & -4 & -2 & 0 & 2 & 0 & 0 & -2 & -2 \\ -1 & -3 & -1 & 1 & 1 & -3 & -3 & -1 & 1 & 1 & 3 \\ -2 & 2 & 0 & 4 & -2 & -4 & -2 & 0 & 0 & 2 & -2 \\ -2 & 4 & 4 & 0 & -2 & 2 & 0 & -2 & 2 & 0 & 1 \\ -4 & -2 & 0 & 2 & 4 & 0 & 0 & 2 & -4 & -2 & 0 \\ 2 & 4 & 2 & 0 & -2 & -2 & -2 & 2 & -4 & -4 & -1 \end{pmatrix}.$$

The top row gives the solution

$$(0, -1, 0, 0, -1, 0, -1, 0, 0, -1, 1),$$

i.e., we have

$$80956 + 38136 + 39658 + 9546 = 168296.$$

This problem was created using the superincreasing sequence

$$\mathbf{r} = (73, 160, 323, 657, 1325, 2660, 5348, 10698, 21396, 42807)$$

and the multiplier and modulus  $A = 79809$  and  $B = 85733$ .

**6.48.** Alice and Bob communicate using the GGH cryptosystem. Alice's public key is the lattice generated by the rows of the matrix

$$\begin{pmatrix} 10305608 & -597165 & 45361210 & 39600006 & 12036060 \\ -71672908 & 4156981 & -315467761 & -275401230 & -83709146 \\ -46304904 & 2685749 & -203811282 & -177925680 & -54081387 \\ -68449642 & 3969419 & -301282167 & -263017213 & -79944525 \\ -46169690 & 2677840 & -203215644 & -177405867 & -53923216 \end{pmatrix}.$$



Bob sends her the encrypted message

$$\mathbf{e} = (388120266, -22516188, 1708295783, 1491331246, 453299858).$$

Use LLL to find a reduced basis for Alice's lattice, and then use Babai's algorithm to decrypt Bob's message.

*Solution to Exercise 6.48.*

LLL takes 52 swaps to produce the following matrix whose Hadamard ratio is  $\mathcal{H} = 0.963$ , so it is quite orthogonal:

$$\begin{pmatrix} 72 & -116 & 172 & -290 & -51 \\ 180 & -218 & -53 & 298 & 161 \\ -158 & -301 & -230 & -185 & -25 \\ 114 & 172 & -148 & -311 & 297 \\ 462 & 164 & -258 & 91 & -491 \end{pmatrix}.$$

Babai's closest vertex method gives the lattice vector

$$(388120256, -22516180, 1708295793, 1491331242, 453299848)$$

that is close to the target vector  $\mathbf{e}$ . If we let  $\mathbf{v}_1, \dots, \mathbf{v}_5$  be the LLL-reduced basis vectors and  $\mathbf{w}_1, \dots, \mathbf{w}_5$  be the original basis vectors, then

$$\begin{aligned} (388120256, -22516180, 1708295793, 1491331242, 453299848) \\ = 1622959\mathbf{v}_1 + 2403687\mathbf{v}_2 - 4093270\mathbf{v}_3 - 1942134\mathbf{v}_4 - 1269978\mathbf{v}_5 \\ = -3\mathbf{w}_1 - 9\mathbf{w}_2 + 0\mathbf{w}_3 + 6\mathbf{w}_4 - 4\mathbf{w}_5. \end{aligned}$$

So Bob's plaintext is the vector  $(-3, -9, 0, 6, -4)$ .

**6.49.** Alice and Bob communicate using the NTRU cryptosystem with public parameters  $(N, p, q, d) = (11, 3, 97, 3)$ . Alice's public key is

$$\mathbf{h} = 39 + 9x + 33x^2 + 52x^3 + 58x^4 + 11x^5 + 38x^6 + 6x^7 + x^8 + 48x^9 + 41x^{10}.$$

Apply the LLL algorithm to the associated NTRU lattice to find an NTRU private key  $(\mathbf{f}, \mathbf{g})$  for  $\mathbf{h}$ . Check your answer by verifying that  $\mathbf{g} \equiv \mathbf{f} \star \mathbf{h} \pmod{q}$ . Use the private key to decrypt the ciphertext

$$\mathbf{e} = 52 + 50x + 50x^2 + 61x^3 + 61x^4 + 7x^5 + 53x^6 + 46x^7 + 24x^8 + 17x^9 + 50x^{10}.$$

*Solution to Exercise 6.49.*

We apply LLL to the 22 dimensional NTRU lattice  $L_{\mathbf{h}}^{\text{NTRU}}$  associated to  $\mathbf{h}$ . It requires 322 swaps and returns the LLL reduced the matrix

$$\begin{bmatrix} -1 & -1 & -1 & 0 & 0 & -1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & -1 & 0 & 0 & -1 & -1 & 0 & 1 & 0 & -1 \\ 1 & -1 & -1 & -1 & 0 & 0 & -1 & 0 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & 0 & 0 & -1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & 0 & -2 & 0 & -1 & 0 & 0 & -1 & 1 & 1 & 0 & -1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & -2 & 1 & -1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & -1 \\ 0 & 1 & 1 & -1 & -1 & -1 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & -1 & 1 & 1 & -1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 2 & 1 & 0 & -1 & 0 & 0 & 1 & 1 & -1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 & -1 & 0 & -1 & 1 & 0 & 2 & 0 & 1 & 0 & 0 & 1 & -1 & -1 & 0 & 1 & -1 & 0 & 0 \\ 1 & -1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & -2 & 0 & -1 & 1 & -1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 2 & 1 & 0 & 1 & -1 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & -1 & 0 & -2 & 0 & -2 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & -1 & 0 \\ 1 & 1 & 1 & -1 & 1 & 1 & 0 & 0 & -2 & 0 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 1 & 0 & -1 & 1 & 0 \\ -4 & 8 & 0 & 2 & -7 & 0 & 1 & -8 & 13 & -4 & -2 & 4 & -9 & -1 & 0 & 7 & -7 & -6 & 1 & 2 & 18 & -10 \\ 9 & 2 & 3 & -7 & -1 & 0 & -9 & 12 & -4 & -4 & -3 & -10 & 0 & 0 & 7 & -6 & -5 & 1 & 1 & 17 & -11 & 4 \\ -6 & -2 & -5 & 3 & 13 & 2 & 0 & 1 & 5 & -11 & -1 & 16 & -3 & 9 & 5 & 3 & 2 & -8 & -5 & -14 & -4 & -2 \\ -3 & 7 & 2 & 0 & 8 & -12 & 3 & 3 & 4 & -8 & -1 & 0 & -7 & 7 & 6 & -1 & -2 & -17 & 12 & -5 & 9 & 1 \\ -9 & 7 & 7 & -8 & -14 & 2 & -10 & -8 & -2 & 1 & -1 & 4 & -3 & 1 & -6 & 2 & 0 & 3 & -1 & 21 & 12 & -1 \\ 7 & 1 & 0 & 9 & -12 & 4 & 4 & 3 & -9 & -2 & -3 & -7 & 6 & 5 & -1 & -1 & -17 & 11 & -4 & 10 & 0 & 0 \\ -2 & -3 & 9 & 2 & 3 & -6 & -1 & 0 & -8 & 13 & -4 & -11 & 4 & -8 & 0 & 0 & 8 & -6 & -5 & 1 & 2 & 18 \\ 13 & 3 & -4 & 1 & 3 & 4 & -12 & -2 & 9 & -14 & -2 & 14 & -2 & -7 & 2 & -10 & -12 & 3 & 3 & 8 & 4 & -4 \\ -1 & -5 & 11 & 1 & 6 & 2 & 5 & -3 & -13 & -2 & 0 & 5 & 14 & 4 & 2 & -16 & 3 & -9 & -5 & -3 & -2 & 8 \\ -6 & 11 & 0 & 6 & 2 & 5 & -3 & -11 & -3 & 1 & -2 & 15 & 4 & 1 & -16 & 2 & -9 & -5 & -3 & -2 & 9 & 4 \\ -3 & -3 & -3 & 9 & 2 & 1 & -8 & -1 & 0 & -7 & 13 & 18 & -10 & 5 & -9 & 0 & 0 & 7 & -7 & -5 & 1 & 0 \end{bmatrix}.$$

The top row is

$$(-1, -1, -1, 0, 0, -1, 0, 1, 0, 1, 1, 1, 1, -1, 0, 0, -1, -1, 0, 1, 0, -1),$$

which gives the private key polynomials

$$\begin{aligned} \mathbf{f}(x) &= -1 - x - x^2 - x^5 + x^7 + x^9 + x^{10} \\ \mathbf{g}(x) &= 1 + x - x^2 - x^5 - x^6 + x^8 - x^{10}. \end{aligned}$$

To decipher the message, we compute

$$\mathbf{a} \equiv \mathbf{f} \star \mathbf{e} \equiv -11 - 13x - 1x^2 + 3x^3 - 4x^4 + 2x^5 + 16x^6 + 4x^7 + 4x^9 - 2x^{10} \pmod{q}.$$

Then we use

$$\mathbf{f}^{-1} \equiv -1 + x - x^3 + x^4 - x^6 + x^7 - x^8 - x^9 + x^{10} \pmod{3}$$

to compute the plaintext

$$\mathbf{m} \equiv \mathbf{a} \star \mathbf{f}^{-1} \equiv 1 - x - x^2 - x^3 - x^4 + x^7 + x^{10} \pmod{3}.$$

In vector form,  $\mathbf{m} = (1, -1, -1, -1, -1, 0, 0, 1, 0, 0, 1)$ .

- 6.50.** (a) Suppose that  $k$  is a 10 digit integer, and suppose that when  $\sqrt{k}$  is computed, the first 15 digits *after* the decimal place are 418400286617716. Find the number  $k$ . (*Hint.* Reformulate it as a lattice problem.)  
 (b) More generally, suppose that you know the first  $d$ -digits after the decimal place of  $\sqrt{K}$ . Explain how to set up a lattice problem to find  $K$ .  
 See Exercise 1.47 for a cryptosystem associated to this problem.

*Solution to Exercise 6.50.*

We do (b) first, then illustrate the general idea by doing (a). Let  $\alpha$  be the  $d$ -digit number consisting of the first  $d$  digits after the decimal place of  $\sqrt{K}$ . If we let  $\beta = \alpha/10^d$ , then we can write

$$\sqrt{K} \approx J + \beta \quad \text{for some } J \in \mathbb{Z}.$$

There are two unknowns here,  $K$  and  $J$ , and all that we know is that they are both integers. Squaring both sides gives

$$K \approx J^2 + 2J\beta + \beta^2.$$

Thus there are integers  $A$  and  $B$  satisfying

$$\beta^2 + A\beta + B \approx 0,$$

namely  $A = 2J$  and  $B = J^2 - K$ . Of course, we don't know  $A$  or  $B$ , so we now describe a lattice reduction problem that finds a (quadratic) polynomial with small integer coefficients that has a given decimal number as an (approximate) root. Once we find  $A$  and  $B$ , it is easy to recover  $K$  as  $K = \frac{1}{4}A^2 - B$ .

Let  $L$  be the lattice generated by the rows of the matrix

$$M = \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & c\beta \\ 0 & 0 & t & c\beta^2 \end{pmatrix},$$

where we will choose  $t$  and  $c$  later. Notice that

$$(B \ A \ 1) \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & c\beta \\ 0 & 0 & t & c\beta^2 \end{pmatrix} = (B \ A \ t \ c(B + A\beta + \beta^2)).$$

So if  $B + A\beta + \beta^2$  is small, then we have found a small vector in the lattice. In other words, if we find a small vector in the lattice having the form  $(B, A, *)$ , then we have probably found the values of  $A$  and  $B$  that we want. (We choose  $t$  reasonably large to force the relation to look like  $(B, A, 1)$ , instead of  $(B, A, C)$  for some larger  $C$ .)

(b) *A solution for this exercise is not currently available.*

## Chapter 7

# Digital Signatures

### Exercises for Chapter 7

Section. RSA digital signatures

**7.1.** Samantha uses the RSA signature scheme with primes  $p = 541$  and  $q = 1223$  and public verification exponent  $v = 159853$ .

- (a) What is Samantha's public modulus? What is her private signing key?
- (b) Samantha signs the digital document  $D = 630579$ . What is the signature?

*Solution to Exercise 7.1.*

(a) Samantha's public modulus is  $N = p \cdot q = 541 \cdot 1223 = 661643$ . Samantha knows that  $(p - 1)(q - 1) = 540 \cdot 1222 = 659880$ , so she can solve

$$vs \equiv 1 \pmod{(p-1)(q-1)}, \quad 159853 \cdot s \equiv 1 \pmod{659880},$$

for the private signing key  $s = 561517$ .

- (b) Samantha takes the document  $D = 630579$  and computes

$$S = D^s \pmod{N}, \quad 630579^{561517} \equiv 206484 \pmod{661643}.$$

So the signature is  $S = 206484$ .

She can check that this is correct by computing

$$C \equiv S^v \pmod{N}, \quad C \equiv 206484^{159853} \equiv 630579 \pmod{661643}$$

and noting that this value agrees with  $D = 630579$ .

**7.2.** Samantha uses the RSA signature scheme with public modulus  $N = 1562501$  and public verification exponent  $v = 87953$ . Adam claims that Samantha has signed each of the documents

$$D = 119812, \quad D' = 161153, \quad D'' = 586036,$$

and that the associated signatures are

$$S = 876453, \quad S' = 870099, \quad S'' = 602754.$$

Which of these are valid signatures?

*Solution to Exercise 7.2.*

Victor uses Samantha's public key  $(N, v) = (1562501, 87953)$  to compute:

$$\begin{aligned} C &\equiv S^v \pmod{N}, & C &\equiv 876453^{87953} \equiv 772481 \pmod{1562501}, \\ C' &\equiv S'^v \pmod{N}, & C' &\equiv 870099^{87953} \equiv 161153 \pmod{1562501}, \\ C'' &\equiv S''^v \pmod{N}, & C'' &\equiv 602754^{87953} \equiv 586036 \pmod{1562501}. \end{aligned}$$

Comparing the values of  $C, C', C''$  with the document values  $D, D', D''$ , we see that  $S'$  and  $S''$  are valid signatures, but  $S$  is not. We remark that Samantha's private factorization is

$$N = p \cdot q = 1301 \cdot 1201 = 1562501$$

and her signing key is  $s = 261617$ .

**7.3.** Samantha uses the RSA signature scheme with public modulus and public verification exponent

$$N = 27212325191 \quad \text{and} \quad v = 22824469379.$$

Use whatever method you want to factor  $N$ , and then forge Samantha's signature on the document  $D = 12910258780$ .

*Solution to Exercise 7.3.*

The factorization of Samantha's public modulus is

$$N = p \cdot q = 128311 \cdot 212081 = 27212325191.$$

Then  $(p-1)(q-1) = 128310 \cdot 212080 = 27211984800$ , so we can solve

$$vs \equiv 1 \pmod{(p-1)(q-1)}, \quad 22824469379 \cdot s \equiv 1 \pmod{27211984800}$$

for Samantha's private signing exponent  $s = 18408628619$ . We can then sign the document  $D = 12910258780$  by computing

$$\begin{aligned} S &\equiv D^s \pmod{N}, \\ 12910258780^{18408628619} &\equiv 22054770669 \pmod{27212325191}. \end{aligned}$$

To check that this signature is correct, we compute

$$\begin{aligned} C &\equiv S^v \pmod{N}, \\ C &\equiv 22054770669^{22824469379} \equiv 12910258780 \pmod{27212325191} \end{aligned}$$

and note that it agrees with  $D = 12910258780$ .

## Section. Discrete logarithm digital signatures

**7.4.** Samantha uses the ElGamal signature scheme with prime  $p = 6961$  and primitive root  $g = 437$ .

- (a) Samantha's private signing key is  $s = 6104$ . What is her public verification key?
- (b) Samantha signs the digital document  $D = 5584$  using the ephemeral key  $e = 4451$ . What is the signature?

Solution to Exercise 7.4.

(a)

$$v \equiv 437^{6104} \equiv 2065 \pmod{6961}.$$

(b)

$$\begin{aligned} S_1 &\equiv 437^{4451} \equiv 3534 \pmod{6961}, \\ S_2 &\equiv (5584 - 6104 \cdot 3534)4451^{-1} \equiv 5888 \pmod{6960}. \end{aligned}$$

So the signature on  $D$  is  $(3534, 5888)$ .

**7.5.** Samantha uses the ElGamal signature scheme with prime  $p = 6961$  and primitive root  $g = 437$ . Her public verification key is  $v = 4250$ . Adam claims that Samantha has signed each of the documents

$$D = 1521, \quad D' = 1837, \quad D'' = 1614,$$

and that the associated signatures are

$$(S_1, S_2) = (4129, 5575), \quad (S'_1, S'_2) = (3145, 1871), \quad (S''_1, S''_2) = (2709, 2994).$$

Which of these are valid signatures?

Solution to Exercise 7.5.

(a)

$$\begin{aligned} v^{S_1} \cdot S_1^{S_2} &\equiv (4250^{4129}) \cdot 4129^{5575} \equiv 231 \pmod{6961}, \\ g^D &\equiv 437^{1521} \equiv 231 \pmod{6961}. \end{aligned}$$

So the signature is valid. (The ephemeral key was  $e = 5627$ .)

(b)

$$\begin{aligned} v^{S'_1} \cdot S'_1^{S'_2} &\equiv (4250^{3145}) \cdot 3145^{1871} \equiv 6208 \pmod{6961}, \\ g^{D'} &\equiv 437^{1837} \equiv 2081 \pmod{6961}. \end{aligned}$$

So the signature is *not* valid.

(c)

$$\begin{aligned} v^{S''_1} \cdot S''_1^{S''_2} &\equiv (4250^{2709}) \cdot 2709^{2994} \equiv 2243 \pmod{6961}, \\ g^{D''} &\equiv 437^{1614} \equiv 2243 \pmod{6961}. \end{aligned}$$

So the signature is valid. (The ephemeral key was  $e = 3997$ .)

(Samantha's private signing key is  $s = 4804$ .)

**7.6.** Let  $p$  be a prime and let  $i$  and  $j$  be integers with  $\gcd(j, p-1) = 1$ . Set  $S_1 \equiv g^i v^j \pmod{p}$ ,  $S_2 \equiv -S_1 j^{-1} \pmod{p-1}$ ,  $D \equiv -S_1 i j^{-1} \pmod{p-1}$ .

Prove that  $(S_1, S_2)$  is a valid ElGamal signature on the document  $D$  for the verification key  $v$ . Thus Eve can produce signatures on random documents.

*Solution to Exercise 7.6.*

We compute

$$\begin{aligned} v^{S_1} S_1^{S_2} &\equiv v^{S_1} (g^i v^j)^{-S_1 j^{-1}} \pmod{p} \\ &\equiv v^{S_1} g^{-i j^{-1} S_1} v^{-S_1} \pmod{p} \\ &\equiv g^D \pmod{p}. \end{aligned}$$

**7.7.** Suppose that Samantha is using the ElGamal signature scheme and that she is careless and uses the same ephemeral key  $e$  to sign two documents  $D$  and  $D'$ .

- Explain how Eve can tell at a glance whether Samantha has made this mistake.
- If the signature on  $D$  is  $(S_1, S_2)$  and the signature on  $D'$  is  $(S'_1, S'_2)$ , explain how Eve can recover  $s$ , Samantha's private signing key.
- Apply your method from (b) to the following example and recover Samantha's signing key  $s$ , where Samantha is using the prime  $p = 348149$ , base  $g = 113459$ , and verification key  $v = 185149$ .

$$\begin{array}{lll} D = 153405, & S_1 = 208913, & S_2 = 209176, \\ D' = 127561, & S'_1 = 208913, & S'_2 = 217800. \end{array}$$

*Solution to Exercise 7.7.*

(a) Since  $S_1 \equiv g^e$  and  $S'_1 \equiv g^{e'}$ , Eve can check if the two signatures used the same ephemeral key by checking if  $S_1 = S'_1$ .

(b) Using discrete logarithms to the base  $g$ , the verification conditions are

$$\begin{aligned} S_1 \log(v) + S_2 \log(S_1) &\equiv D \pmod{p-1}, \\ S'_1 \log(v) + S'_2 \log(S'_1) &\equiv D' \pmod{p-1}. \end{aligned}$$

Since  $S_1 = S'_1$  from (a), this becomes

$$\begin{aligned} S_1 s + S_2 \log(S_1) &\equiv D \pmod{p-1}, \\ S_1 s + S'_2 \log(S_1) &\equiv D' \pmod{p-1}, \end{aligned}$$

where  $s = \log(v)$  is Samantha's secret signing key. Taking  $S'_2$  times the first congruence and subtracting  $S_2$  times the second congruence, we obtain

$$S_1(S'_2 - S_2)s \equiv S'_2 D - S_2 D' \pmod{p-1}.$$

For notational convenience we write this congruence as

$$As \equiv B \pmod{p-1},$$

where we know the values of  $A$  and  $B$ . If  $\gcd(A, p-1) = 1$ , we can solve uniquely for  $s$ . In general, if  $\gcd(A, p-1) > 1$  (it's unlikely to be too large), then there are  $\gcd(A, p-1)$  solutions for  $s$ , and after computing them, we can decide which one is correct by checking which one yields  $g^s \equiv v \pmod{p}$ .

(c) From (b) we begin by computing

$$\begin{aligned} A &\equiv S_1(S'_2 - S_2) \equiv 347960 \pmod{p-1}, \\ B &\equiv S'_2 D - S_2 D' \equiv 252868 \pmod{p-1}. \end{aligned}$$

We need to solve  $As \equiv B \pmod{p-1}$ , so we need to solve

$$347960s \equiv 252868 \pmod{348148}.$$

This congruence has several solutions. More precisely, since  $\gcd(347960, 348148) = 4$  and  $4 \mid 252868$ , we divide through by 4 to get

$$86990s \equiv 63217 \pmod{87037}.$$

Then  $\gcd(86990, 87037) = 1$ , so we can solve this congruence. The solution is

$$s \equiv 72729 \pmod{87037}.$$

Adding on multiples of  $(p-1)/4 = 87037$  yields the four solutions

$$s \equiv 72729, 159766, 246803, 333840 \pmod{348148}$$

to the original congruence. We can pick out which solution is correct from the relation  $g^s \equiv v \pmod{p}$ , i.e., the correct value of  $s$  should satisfy

$$113459^s \equiv 185149 \pmod{348149}.$$

We compute

$$\begin{aligned} 113459^{72729} &\equiv 185149 \pmod{348149}, \\ 113459^{159766} &\equiv 137653 \pmod{348149}, \\ 113459^{246803} &\equiv 163000 \pmod{348149}, \\ 113459^{333840} &\equiv 210496 \pmod{348149}. \end{aligned}$$

Hence Samantha's secret signing key is

$$s = 72729.$$



**7.8.** Samantha uses DSA with public parameters  $(p, q, g) = (22531, 751, 4488)$ . She chooses the secret signing key  $s = 674$ .

- (a) What is Samantha's public verification key?
- (b) Samantha signs the document  $D = 244$  using the ephemeral key  $e = 574$ . What is the signature?

Solution to Exercise 7.8.

- (a) Samantha's public verification key is

$$v \equiv 4488^{674} \equiv 4940 \pmod{22531}.$$

- (b) The signature is

$$\begin{aligned} S_1 &= (4488^{574} \pmod{22531}) \pmod{751} = 444, \\ S_2 &\equiv (244 + 674 \cdot 444) 574^{-1} \equiv 56 \pmod{751}. \end{aligned}$$

**7.9.** Samantha uses DSA with public parameters  $(p, q, g) = (22531, 751, 4488)$ . Her public verification key is  $v = 22476$ .

- (a) Is  $(S_1, S_2) = (183, 260)$  a valid signature on the document  $D = 329$ ?
- (b) Is  $(S_1, S_2) = (211, 97)$  a valid signature on the document  $D = 432$ ?

Solution to Exercise 7.9.

- (a) Victor computes

$$V_1 \equiv 329 \cdot 260^{-1} \equiv 293 \pmod{751} \quad \text{and} \quad V_2 \equiv 183 \cdot 260^{-1} \equiv 252 \pmod{751}.$$

He then computes

$$g^{V_1} v^{V_2} \equiv 4488^{293} \cdot 22476^{252} \equiv 6191 \pmod{22531}$$

and verifies that  $6191 \pmod{751} = 183$  is equal to  $S_1$ . So the signature is valid. (Samantha's secret signing key happens to be  $s = 38$ .)

- (b) Victor computes

$$V_1 \equiv 432 \cdot 97^{-1} \equiv 709 \pmod{751} \quad \text{and} \quad V_2 \equiv 211 \cdot 97^{-1} \equiv 428 \pmod{751}.$$

He then computes

$$g^{V_1} v^{V_2} \equiv 4488^{709} \cdot 22476^{428} \equiv 3979 \pmod{22531}.$$

Then he observes that

$$(g^{V_1} v^{V_2} \pmod{p}) \pmod{q} = 3979 \pmod{751} = 224$$

is not equal to  $S_1 = 211$ . So the signature is not valid.

**7.10.** Samantha's DSA public parameters are  $(p, q, g) = (103687, 1571, 21947)$ , and her public verification key is  $v = 31377$ . Use whatever method you prefer (brute-force, collision, index calculus, ...) to solve the DLP and find Samantha's private signing key. Use her key to sign the document  $D = 510$  using the ephemeral key  $e = 1105$ .

Solution to Exercise 7.10.

Solving  $31377 \equiv 21947^s \pmod{103687}$  gives  $s = 602$ . Then the signature on  $D = 510$  using the ephemeral key  $e = 1105$  is

$$\begin{aligned} S_1 &= (21947^{1105} \bmod 103687) \bmod 1571 = 439 \\ S_2 &\equiv (510 + 602 \cdot 439)1105^{-1} \equiv 1259 \pmod{1571}. \end{aligned}$$

**7.11.** The *Elliptic Curve Digital Signature Algorithm* (ECDSA) is described in Table 7.7. Prove that ECDSA works, i.e., prove that the verification step succeeds in verifying a valid signature.

Solution to Exercise 7.11.

We compute

$$\begin{aligned} v_1G + v_2V &= ds_2^{-1}G + s_1s_2^{-1}(sG) \\ &= (d + ss_1)s_2^{-1}G \\ &= (es_2)s_2^{-1}G \\ &= eG \in E(\mathbb{F}_p). \end{aligned}$$

Hence

$$x(v_1G + v_2V) \bmod q = x(eG) \bmod q = s_1.$$

**7.12.** This exercise asks you to compute some numerical instances of the elliptic curve digital signature algorithm described in Table 7.7 for the public parameters

$$E : y^2 = x^3 + 231x + 473, \quad p = 17389, \quad q = 1321, \quad G = (11259, 11278) \in E(\mathbb{F}_p).$$

You should begin by verifying that  $G$  is a point of order  $q$  in  $E(\mathbb{F}_p)$ .

- Samantha's private signing key is  $s = 542$ . What is her public verification key? What is her digital signature on the document  $d = 644$  using the ephemeral key  $e = 847$ ?
- Tabitha's public verification key is  $V = (11017, 14637)$ . Is  $(s_1, s_2) = (907, 296)$  a valid signature on the document  $d = 993$ ?
- Umberto's public verification key is  $V = (14594, 308)$ . Use any method that you want to find Umberto's private signing key, and then use the private key to forge his signature on the document  $d = 516$  using the ephemeral key  $e = 365$ .

Public Parameter Creation	
A trusted party chooses a finite field $\mathbb{F}_p$ , an elliptic curve $E/\mathbb{F}_p$ , and a point $G \in E(\mathbb{F}_p)$ of large prime order $q$ .	
Samantha	Victor
Key Creation	
Choose secret signing key $1 < s < q - 1$ . Compute $V = sG \in E(\mathbb{F}_p)$ . Publish the verification key $V$ .	
Signing	
Choose document $d \bmod q$ . Choose ephemeral key $e \bmod q$ . Compute $eG \in E(\mathbb{F}_p)$ and then, $s_1 = x(eG) \bmod q$ and $s_2 \equiv (d + ss_1)e^{-1} \pmod{q}$ . Publish the signature $(s_1, s_2)$ .	
Verification	
	Compute $v_1 \equiv ds_2^{-1} \pmod{q}$ and $v_2 \equiv s_1s_2^{-1} \pmod{q}$ . Compute $v_1G + v_2V \in E(\mathbb{F}_p)$ and verify that $x(v_1G + v_2V) \bmod q = s_1$ .

Table 7.1: The elliptic curve digital signature algorithm (ECDSA)

Solution to Exercise 7.12.

(a) Samantha's public verification key is

$$V = 542(11259, 11278) = (8689, 1726) \in E(\mathbb{F}_p).$$

Her signature on  $d = 644$  using  $e = 847$  is obtained by first computing  $eG = (8417, 8276) \in E(\mathbb{F}_p)$  and then

$$s_1 = x(eG) \bmod q = 491 \quad \text{and} \quad s_2 \equiv (d + ss_1)e^{-1} \equiv 290 \pmod{q}.$$

(b) Victor computes

$$v_1 \equiv ds_2^{-1} \equiv 106 \pmod{q} \quad \text{and} \quad v_2 \equiv s_1s_2^{-1} \equiv 311 \pmod{q}.$$

Then  $v_1G + v_2V = (8833, 4526) \in E(\mathbb{F}_p)$ , and

$$x(v_1G + v_2V) \bmod q = 8833 \bmod 1321 = 907$$

is equal to  $s_1$ , so the signature is valid.

(c) After some work, one finds that Umberto's private signing key is  $s = 1294$ , since

$$1294G = 1294(11259, 11278) = (14594, 308) \in E(\mathbb{F}_p).$$

We can then forge a signature on the document  $d = 516$  using the ephemeral key  $e = 365$  by first computing  $eG = (3923, 12121) \in E(\mathbb{F}_p)$  and then

$$s_1 = x(eG) \bmod q = 1281 \quad \text{and} \quad s_2 \equiv (d + ss_1)e^{-1} \equiv 236 \pmod{q}.$$

To check that the signature is valid, we compute  $v_1G + v_2V = (3923, 12121) \in E(\mathbb{F}_p)$ , and

$$x(v_1G + v_2V) \bmod q = 3923 \bmod 1321 = 1281,$$

which is equal to  $s_1$ .

**Section. Lattice-based digital signatures**

**7.13.** Samantha uses the GGH digital signature scheme with private and public bases

$$\begin{aligned} \mathbf{v}_1 &= (-20, -8, 1), & \mathbf{w}_1 &= (-248100, 220074, 332172), \\ \mathbf{v}_2 &= (14, 11, 23), & \mathbf{w}_2 &= (-112192, 99518, 150209), \\ \mathbf{v}_3 &= (-18, 1, -12), & \mathbf{w}_3 &= (-216150, 191737, 289401). \end{aligned}$$

What is her signature on the document

$$\mathbf{d} = (834928, 123894, 7812738)?$$

*Solution to Exercise 7.13.*

Samantha uses Babai's algorithm with the good basis to find the vector

$$\mathbf{s} = 283411\mathbf{v}_1 + 233700\mathbf{v}_2 - 179519\mathbf{v}_3 = (834922, 123893, 7812739)$$

that is close to  $\mathbf{d}$ ,

$$\|\mathbf{s} - \mathbf{d}\| \approx 6.16.$$

She then expresses the signature in terms of bad basis,

$$\mathbf{s} = 785152901\mathbf{w}_1 - 1383699316\mathbf{w}_2 - 183004589\mathbf{w}_3$$

and publishes the signature  $(785152901, -1383699316, -183004589)$ .

**7.14.** Samantha uses the GGH digital signature scheme with public basis

$$\begin{aligned} \mathbf{w}_1 &= (3712318934, -14591032252, 11433651072), \\ \mathbf{w}_2 &= (-1586446650, 6235427140, -4886131219), \\ \mathbf{w}_3 &= (305711854, -1201580900, 941568527). \end{aligned}$$

She publishes the signature

$$(6987814629, 14496863295, -9625064603)$$

on the document

$$\mathbf{d} = (5269775, 7294466, 1875937).$$

If the maximum allowed distance from the signature to the document is 60, verify that Samantha's signature is valid.

Solution to Exercise 7.14.

We first compute

$$\begin{aligned}\mathbf{s} &= 6987814629\mathbf{w}_1 + 14496863295\mathbf{w}_2 - 9625064603\mathbf{w}_3 \\ &= (5269774, 7294492, 1875902) \in L.\end{aligned}$$

Then we compute the distance

$$\|\mathbf{s} - \mathbf{d}\| \approx 43.61$$

and verify that it is smaller than the cutoff value of 60, so the signature is valid.

**7.15.** Samantha uses the GGH digital signature scheme with public basis

$$\begin{aligned}\mathbf{w}_1 &= (-1612927239, 1853012542, 1451467045), \\ \mathbf{w}_2 &= (-2137446623, 2455606985, 1923480029), \\ \mathbf{w}_3 &= (2762180674, -3173333120, -2485675809).\end{aligned}$$

Use LLL or some other lattice reduction algorithm to find a good basis for Samantha's lattice, and then use the good basis to help Eve forge a signature on the document

$$\mathbf{d} = (87398273893, 763829184, 118237397273).$$

What is the distance from your forged signature lattice vector to the target vector? (You should be able to get a distance smaller than 100.)

Solution to Exercise 7.15.

Eve's implementation of LLL gives the basis

$$\mathbf{v}_1 = (-9, -147, -136), \quad \mathbf{v}_2 = (73, 169, -41), \quad \mathbf{v}_3 = (109, -132, -110).$$

Using this LLL reduced basis, she computes

$$\begin{aligned}\mathbf{s} &= -1542740188\mathbf{v}_1 - 532211991\mathbf{v}_2 + 1030872363\mathbf{v}_3 \\ &= (87398273916, 763829241, 118237397269) \in L.\end{aligned}$$

It satisfies

$$\|\mathbf{s} - \mathbf{d}\| \approx 61.60,$$

so is quite a good solution. To find the signature, Eve expresses  $\mathbf{s}$  in terms of the original bad basis,

$$\mathbf{s} = 203927306009123\mathbf{w}_1 + 225365519245447\mathbf{w}_2 + 293473443761381\mathbf{w}_3.$$

The signature is

$$(203927306009123, 225365519245447, 293473443761381).$$

## Section. NTRU digital signatures

**7.16.** Samantha uses an NTRU digital signature with  $(N, q, d) = (11, 23, 3)$ .

(a) Samantha's private key is

$$\begin{aligned}\mathbf{f} &= (1, -1, 1, 0, 1, 0, -1, 1, 0, -1, 0), \\ \mathbf{g} &= (0, -1, 0, 1, 1, 0, 0, 1, -1, 1, -1), \\ \mathbf{F} &= (0, -1, -1, 1, -3, -1, 0, -3, -3, -2, 2), \\ \mathbf{G} &= (-3, -1, 2, 4, 3, -4, -1, 3, 5, 5, -1).\end{aligned}$$

She uses her private key to sign the digital document  $\mathbf{D} = (\mathbf{D}_1, \mathbf{D}_2)$  given by

$$\begin{aligned}\mathbf{D}_1 &= (0, 8, -6, -6, -5, -1, 9, -2, -6, -4, -6), \\ \mathbf{D}_2 &= (9, 9, -10, 2, -3, 2, 6, 6, 5, 0, 8).\end{aligned}$$

Compute the signature  $\mathbf{s}$ .

(b) Samantha's public verification key is

$$\mathbf{h} = (5, 8, -5, -11, 8, 8, 8, 5, 3, -10, 5).$$

Compute the other part of the signature  $\mathbf{t} \equiv \mathbf{h} \star \mathbf{s} \pmod{q}$  and find the distance between the lattice vector  $(\mathbf{s}, \mathbf{t})$  and the target vector  $\mathbf{D}$ .

(c) Suppose that Eve attempts to sign  $\mathbf{D}$  using Samantha's public vectors  $(\mathbf{1}, \mathbf{h})$  and  $(\mathbf{0}, \mathbf{q})$ . What signature  $(\mathbf{s}', \mathbf{t}')$  does she get and how far is it from the target vector  $\mathbf{D}$ ?

*Solution to Exercise 7.16.*

(a) Samantha first computes

$$\begin{aligned}\mathbf{v}_1 &= \left\lfloor \left( \frac{-164}{23}, \frac{-64}{23}, \frac{32}{23}, \frac{143}{23}, \frac{146}{23}, \frac{1}{23}, \frac{-178}{23}, \frac{-1,120}{23}, \frac{108}{23}, \frac{25}{23} \right) \right\rfloor \\ &= (-7, -3, 1, 6, 6, 0, -8, -1, 5, 5, 1), \\ \mathbf{v}_2 &= \left\lfloor \left( \frac{27}{23}, \frac{13}{23}, \frac{0,35}{23}, \frac{-27}{23}, \frac{4}{23}, \frac{2}{23}, \frac{16}{23}, \frac{11}{23}, \frac{-24}{23}, \frac{-4}{23} \right) \right\rfloor \\ &= (1, 1, 0, 2, -1, 0, 0, 1, 0, -1, 0),\end{aligned}$$

and then

$$\mathbf{s} = (-2, 8, -4, -7, -5, -2, 9, -4, -9, -4, -8).$$

(b)

$$\mathbf{t} \equiv \mathbf{h} \star \mathbf{s} \equiv (11, 9, -9, 2, -4, 5, 4, 8, 4, 0, 11) \pmod{23}.$$

Then

$$\|(\mathbf{s}, \mathbf{t}) - \mathbf{D}\| = 7.74597.$$

(c) The signature using the  $\mathbf{h}$ -basis is

$$\begin{aligned}\mathbf{s}' &= (0, 8, -6, -6, -5, -1, 9, -2, -6, -4, -6), \\ \mathbf{t}' &= (5, 17, -3, 9, 3, 2, 14, 13, 2, 10, 1).\end{aligned}$$

It satisfies

$$\|(\mathbf{s}', \mathbf{t}') - \mathbf{D}\| = 22.0227.$$

**7.17.** Samantha uses an NTRU digital signature with  $(N, q, d) = (11, 23, 3)$ .

(a) She creates a private key using the ternary vectors

$$\begin{aligned}\mathbf{f} &= (1, 1, 1, 1, 0, -1, -1, 0, 0, 0, -1), \\ \mathbf{g} &= (-1, 0, 1, 1, -1, 0, 0, 1, -1, 0, 1).\end{aligned}$$

Use the algorithm described in Table 7.6 to find short vectors  $\mathbf{F}$  and  $\mathbf{G}$  satisfying  $\mathbf{f} \star \mathbf{G} - \mathbf{g} \star \mathbf{F} = q$ .

(b) Samantha uses the private signing key  $(\mathbf{f}, \mathbf{g}, \mathbf{F}, \mathbf{G})$  to sign the digital document  $\mathbf{D} = (\mathbf{D}_1, \mathbf{D}_2)$  given by

$$\begin{aligned}\mathbf{D}_1 &= (5, 5, -5, -10, 3, -7, -3, 2, 0, -5, -11), \\ \mathbf{D}_2 &= (8, 9, -10, -7, 6, -3, 1, 4, 4, 4, -7).\end{aligned}$$

What the signature  $\mathbf{s}$ ?

- (c) What is Samantha's public verification key  $\mathbf{h}$ ?
- (d) Compute  $\mathbf{t} \equiv \mathbf{h} \star \mathbf{s} \pmod{q}$  and determine the distance from the lattice vector  $(\mathbf{s}, \mathbf{t})$  to the target vector  $\mathbf{D}$ .

*Solution to Exercise 7.17.*

(a) First she computes

$$\begin{aligned}\mathbf{f}_1 &= (1363, -944, 786, 358, 482, 80, -133, 368, 955, 126, 476), \\ \mathbf{f}_2 &= (-2554, 419, 1205, 1563, 682, 343, 368, 955, 126, 476, 0), \\ \mathbf{g}_1 &= (-63, 121, -173, -232, 208, -251, 96, 172, 620, 799, 574), \\ \mathbf{g}_2 &= (-1808, -121, 110, 290, -197, -275, 53, -46, -799, -574, 0).\end{aligned}$$

The resultants are  $R_f = 3917$  and  $R_g = 1871$ , and then  $S_f = -866$  and  $S_g = 1813$  satisfies  $S_f R_f + S_g R_g = 1$ . Then we find that

$$\begin{aligned}\mathbf{A} &= (2627037, -5045579, 7213927, 9674168, -8673392, 10466449, \\ &\quad -4003104, -7172228, -25853380, -33317501, -23935226), \\ \mathbf{B} &= (-27148234, 18802592, -15655548, -7130644, -9600476, -1593440, \\ &\quad 2649094, -7329824, -19021690, -2509668, -9480968).\end{aligned}$$

Next we use

$$\begin{aligned}\mathbf{f}^{-1} &= (0.35, -0.24, 0.20, 0.09, 0.12, 0.02, -0.03, 0.09, 0.24, 0.03, 0.12), \\ \mathbf{g}^{-1} &= (-0.03, 0.06, -0.09, -0.12, 0.11, -0.13, 0.05, 0.09, 0.33, 0.43, 0.31),\end{aligned}$$

to compute

$$\begin{aligned}\mathbf{C} &= (-2522997, -13372262, 753797, -4259685, -6431876, -1572245, \\ &\quad -16151212, -8516655, -12881295, -9762142, -3302247).\end{aligned}$$

Using this yields

$$\begin{aligned}\mathbf{F} &= (-1, -1, 1, 2, 0, 2, 0, 0, -3, -5, -5), \\ \mathbf{G} &= (4, -4, 3, 2, 1, 0, 0, 2, 3, 0, 2).\end{aligned}$$

These are reasonably short,  $\|F\| = 8.36660$  and  $\|G\| = 7.93725$ .

(b)

$$\begin{aligned}\mathbf{v}_1 &= \left\lfloor \left( \frac{-2}{23}, \frac{-117}{23}, \frac{-116}{23}, \frac{-37}{23}, \frac{51}{23}, \frac{-40}{23}, \frac{7}{23}, \frac{7}{23}, 1, \frac{-22}{23}, \frac{-2}{23} \right) \right\rfloor \\ &= (0, -5, -5, -2, 2, -2, 0, 0, 1, -1, 0) \\ \mathbf{v}_2 &= \left\lfloor \left( \frac{-4}{23}, \frac{55}{23}, \frac{1}{23}, \frac{-53}{23}, \frac{21}{23}, \frac{5}{23}, \frac{-21}{23}, \frac{-15}{23}, \frac{37}{23}, \frac{31}{23}, \frac{-22}{23} \right) \right\rfloor \\ &= (0, 2, 0, -2, 1, 0, -1, -1, 2, 1, -1)\end{aligned}$$

Then

$$\mathbf{s} = (7, 3, -4, -10, 4, -6, -3, 1, 1, -5, -10).$$

(c) We have

$$\begin{aligned}\mathbf{f}^{-1} \bmod 23 &= (-9, -10, -6, -8, -10, -5, 4, 0, 5, -5, -1), \\ \mathbf{h} &= (-3, -2, 2, -1, 3, -5, 11, -10, -2, -6, -9).\end{aligned}$$

(d)

$$\mathbf{t} = (9, 6, -9, -7, 4, -4, 0, 4, 5, -2, -5).$$

$$\|(\mathbf{s}, \mathbf{t}) - \mathbf{D}\| = 8.48528.$$

**7.18.** Let  $\mathbf{a} \in \mathbb{R}^N$  be a fixed vector.

- (a) Suppose that  $\mathbf{b}$  is an  $N$ -dimensional vector whose coefficients are chosen randomly from the set  $\{-1, 0, 1\}$ . Prove that the expected values of  $\|\mathbf{b}\|^2$  and  $\|\mathbf{a} \star \mathbf{b}\|^2$  are given by

$$E(\|\mathbf{b}\|^2) = \frac{2}{3}N \quad \text{and} \quad E(\|\mathbf{a} \star \mathbf{b}\|^2) = \|\mathbf{a}\|^2 E(\|\mathbf{b}\|^2).$$

- (b) More generally, suppose that the coefficients of  $\mathbf{b}$  are chosen at random from the set of integers  $\{-T, -T+1, \dots, T-1, T\}$ . Compute the expected values of  $\|\mathbf{b}\|^2$  and  $\|\mathbf{a} \star \mathbf{b}\|^2$  as in (a).



- (c) Suppose now that the coefficients of  $\mathbf{b}$  are real numbers that are chosen uniformly and independently in the interval from  $-R$  to  $R$ . Prove that

$$E(\|\mathbf{b}\|^2) = \frac{R^2 N}{3} \quad \text{and} \quad E(\|\mathbf{a} \star \mathbf{b}\|^2) = \|\mathbf{a}\|^2 E(\|\mathbf{b}\|^2).$$

(*Hint.* The most direct way to do (c) is to use continuous probability theory. As an alternative, let the coefficients of  $\mathbf{b}$  be chosen uniformly and independently from the set  $\{jR/T : -T \leq j \leq T\}$ , redo the computation from (b), and then let  $T \rightarrow \infty$ .)

Solution to Exercise 7.18.

Let  $\mathbf{c} = \mathbf{a} \star \mathbf{b}$ . Then

$$\begin{aligned} \|\mathbf{c}\|^2 &= \sum_{k \bmod N} c_k^2 \\ &= \sum_{k \bmod N} \left( \sum_{i+j \equiv k \pmod{N}} a_i b_j \right)^2 \\ &= \sum_{k \bmod N} \sum_{i+j \equiv k \pmod{N}} a_i b_j \sum_{u+v \equiv k \pmod{N}} a_u b_v \\ &= \sum_{i+j \equiv u+v \pmod{N}} a_i a_u b_j b_v. \end{aligned}$$

Note that this last sum is over all 4-tuples  $(i, j, u, v) \bmod N$  satisfying  $i + j \equiv u + v \pmod{N}$ . We suppose now that the coefficients of  $\mathbf{b}$  are independent random variables whose average value is 0, i.e., we assume that  $E(b_i) = 0$ . This is a valid assumption in (a), (b), and (c). Since the coefficients of  $\mathbf{a}$  are fixed, we can compute

$$\begin{aligned} E(\|\mathbf{a} \star \mathbf{b}\|^2) &= \sum_{i+j \equiv u+v \pmod{N}} E(a_i a_u b_j b_v) \\ &= \sum_{i+j \equiv u+v \pmod{N}} a_i a_u E(b_j b_v) \\ &= \sum_{\substack{i+j \equiv u+v \pmod{N} \\ j \neq v}} a_i a_u E(b_j) E(b_v) + \sum_{i \bmod N} \sum_{j \bmod N} a_i^2 E(b_j^2) \\ &= \sum_{i \bmod N} a_i^2 \sum_{j \bmod N} E(b_j^2) \\ &= \|\mathbf{a}\|^2 E(b_0^2 + \cdots + b_{N-1}^2) \\ &= \|\mathbf{a}\|^2 E(\|\mathbf{b}\|^2). \end{aligned}$$

Hence in all cases we have

$$E(\|\mathbf{a} \star \mathbf{b}\|^2) = \|\mathbf{a}\|^2 E(\|\mathbf{b}\|^2).$$

It remains to compute  $E(\|\mathbf{b}\|^2)$  under the various scenarios.

(a) The coefficients of  $\mathbf{b}$  are independent random variables taking values in  $\{-1, 0, 1\}$  with equal probabilities, so

$$\begin{aligned} E(b_i) &= \frac{1}{3} \cdot (-1) + \frac{1}{3} \cdot 0 + \frac{1}{3} \cdot 1 = 0, \\ E(b_i^2) &= \frac{1}{3} \cdot (-1)^2 + \frac{1}{3} \cdot 0^2 + \frac{1}{3} \cdot 1^2 = \frac{2}{3}, \\ E(\|\mathbf{b}\|^2) &= E(b_0^2 + \cdots + b_{N-1}^2) = E(b_0^2) + \cdots + E(b_{N-1}^2) = \frac{2}{3}N. \end{aligned}$$

(b) Similar to (a), but now the values are integers between  $-T$  and  $T$ . So

$$E(b_i^2) = \frac{1}{2T+1} \sum_{j=-T}^T j^2 = \frac{2}{2T+1} \sum_{j=1}^T j^2 = \frac{2}{2T+1} \frac{T(T+1)(2T+1)}{6} = \frac{T^2+T}{3}.$$

Hence

$$E(\|\mathbf{b}\|^2) = \sum_{i=0}^{N-1} E(b_i^2) = \frac{T^2+T}{3}N.$$

(c) The computation using continuous probability is

$$E(b_i^2) = \frac{1}{2R} \int_{-R}^R b^2 db = \frac{1}{2R} \cdot \frac{b^3}{3} \Big|_{-R}^R = \frac{R^2}{3}.$$

Hence  $E(\|\mathbf{b}\|^2) = R^2N/3$ .

The alternative computation using the hint gives, for any particular value of  $T$ ,

$$\begin{aligned} E(b_i^2) &= \frac{1}{2T+1} \sum_{j=-T}^T \left(\frac{jR}{T}\right)^2 = \frac{2R^2}{(2T+1)T^2} \sum_{j=1}^T j^2 \\ &= \frac{2R^2}{(2T+1)T^2} \frac{T(T+1)(2T+1)}{6} = \frac{R^2(T+1)}{3T}. \end{aligned}$$

Letting  $T \rightarrow \infty$  yields  $E(b_i^2) = R^2/3$ , and then

$$E(\|\mathbf{b}\|^2) = NR^2/3.$$

**7.19.** Let  $(\mathbf{f}, \mathbf{g}, \mathbf{F}, \mathbf{G})$  be an NTRU digital signature private key and let

$$\mathbf{h} \equiv \mathbf{f}^{-1} \star \mathbf{g} \pmod{q}$$

be the associated public key. Suppose that  $(\mathbf{s}, \mathbf{t})$  is the signature on the document  $\mathbf{D} = (\mathbf{D}_1, \mathbf{D}_2)$ , so in particular, the vector  $(\mathbf{s}, \mathbf{t})$  is in the NTRU lattice  $L_{\mathbf{h}}^{\text{NTRU}}$ .

- (a) Prove that for every vector  $\mathbf{w} \in \mathbb{Z}^N$ , the vector

$$(\mathbf{s} + \mathbf{w} \star \mathbf{f}, \mathbf{t} + \mathbf{w} \star \mathbf{g})$$

is in the NTRU lattice  $L_{\mathbf{h}}^{\text{NTRU}}$ .

- (b) Let  $\mathbf{f}^{-1}$  be the inverse of  $\mathbf{f}$  in the ring  $\mathbb{R}[x]/(x^N - 1)$  (cf. Table 7.6). Prove that the vector

$$\mathbf{s}' = \mathbf{s} + \lfloor -\mathbf{f}^{-1} \star \mathbf{D}_1 \rfloor \star \mathbf{f}$$

is a signature on a document of the form  $\mathbf{D}' = (\mathbf{0}, \mathbf{D}_2 + \mathbf{D}_3)$  for some  $\mathbf{D}_3$  that depends on  $\mathbf{D}_1$ .

- (c) Conclude that anyone who can sign documents of the form  $(\mathbf{0}, \mathbf{D}')$  is also able to sign documents of the form  $(\mathbf{D}_1, \mathbf{D}_2)$ . Hence in the NTRU digital signature scheme (Table 7.5), we might as well assume that the document being signed is of the form  $(\mathbf{0}, \mathbf{D}_2)$ . This has several benefits, including speeding the computation of  $\mathbf{v}_1$  and  $\mathbf{v}_2$ .

*Solution to Exercise 7.19.*

- (a) The NTRU lattice is characterized as the set of vectors

$$L_{\mathbf{h}}^{\text{NTRU}} = \{(\mathbf{u}, \mathbf{v}) : \mathbf{v} \equiv \mathbf{u} \star \mathbf{h} \pmod{q}\}.$$

We are given that  $(\mathbf{s}, \mathbf{t}) \in L_{\mathbf{h}}^{\text{NTRU}}$ , so

$$(\mathbf{s} + \mathbf{w} \star \mathbf{f}) \star \mathbf{h} \equiv \mathbf{s} \star \mathbf{h} + \mathbf{w} \star \mathbf{f} \star \mathbf{h} \equiv \mathbf{t} + \mathbf{w} \star \mathbf{g} \pmod{q},$$

where we have used the fact that  $\mathbf{h} \equiv \mathbf{f}^{-1} \star \mathbf{g} \pmod{q}$ .

- (b) For notational convenience, we let  $\mathbf{w} = \lfloor -\mathbf{f}^{-1} \star \mathbf{D}_1 \rfloor$ . Then

$$\mathbf{w} \star \mathbf{f} = -\mathbf{D}_1 + \boldsymbol{\epsilon} \star \mathbf{f},$$

where the coefficients of  $\boldsymbol{\epsilon}$  are between  $-\frac{1}{2}$  and  $\frac{1}{2}$ . Hence

$$\mathbf{s}' = \mathbf{s} + \mathbf{w} \star \mathbf{f} = \mathbf{s} - \mathbf{D}_1 + \boldsymbol{\epsilon} \star \mathbf{f}.$$

We know that  $\|\mathbf{s} - \mathbf{D}_1\|$  is small, so we find that

$$\|\mathbf{s}'\| \leq \|\mathbf{s} - \mathbf{D}_1\| + \|\boldsymbol{\epsilon} \star \mathbf{f}\| \approx \|\mathbf{s} - \mathbf{D}_1\| + \|\boldsymbol{\epsilon}\| \|\mathbf{f}\|$$

is also small.

Next we compute

$$\mathbf{t}' \equiv \mathbf{s}' \star \mathbf{h} \equiv \mathbf{s} \star \mathbf{h} + \mathbf{w} \star \mathbf{f} \star \mathbf{h} \equiv \mathbf{t} + \mathbf{w} \star \mathbf{g} \pmod{q}.$$

Since  $\mathbf{t}$  is close to  $\mathbf{D}_2$ , we find that  $\mathbf{t}'$  is close to  $\mathbf{D}_2 + \mathbf{D}_3$ , where

$$\mathbf{D}_3 = \mathbf{w} \star \mathbf{g} = \lfloor -\mathbf{f}^{-1} \star \mathbf{D}_1 \rfloor \star \mathbf{g}.$$

- (c) Suppose that Eve knows how to sign documents of the form  $(\mathbf{0}, \mathbf{D}')$  and that she wants to sign  $(\mathbf{D}_1, \mathbf{D}_2)$ . She starts by finding a signature  $\mathbf{s}'$  to the document

$$(\mathbf{0}, \mathbf{D}_2 + \lfloor -\mathbf{f}^{-1} \star \mathbf{D}_1 \rfloor \star \mathbf{g}).$$

Then from the calculations in (b), she sees that

$$\mathbf{s} = \mathbf{s}' - \lfloor -\mathbf{f}^{-1} \star \mathbf{D}_1 \rfloor \star \mathbf{g}$$

is a signature on  $(\mathbf{D}_1, \mathbf{D}_2)$ .

**7.20.** Verify the identity

$$\begin{pmatrix} \bar{\mathbf{f}} & \bar{\mathbf{F}} \\ \bar{\mathbf{g}} & \bar{\mathbf{G}} \end{pmatrix} \begin{pmatrix} \mathbf{f} & \mathbf{g} \\ \mathbf{F} & \mathbf{G} \end{pmatrix} = \begin{pmatrix} \mathbf{f} \star \bar{\mathbf{f}} + \mathbf{F} \star \bar{\mathbf{F}} & \mathbf{g} \star \bar{\mathbf{f}} + \mathbf{G} \star \bar{\mathbf{F}} \\ \mathbf{f} \star \bar{\mathbf{g}} + \mathbf{F} \star \bar{\mathbf{G}} & \mathbf{g} \star \bar{\mathbf{g}} + \mathbf{G} \star \bar{\mathbf{G}} \end{pmatrix},$$

where bar indicates reversal of a vector as in Remark 7.13. Prove that the corresponding  $2N$ -by- $2N$  matrix is the Gram matrix associated to the  $2N$ -by- $2N$  matrix  $\begin{pmatrix} \mathbf{f} & \mathbf{g} \\ \mathbf{F} & \mathbf{G} \end{pmatrix}$ . (See Exercise 6.14 for the definition of the Gram matrix.)



## Chapter 8

# Additional Topics in Cryptography

An Introduction to Mathematical Cryptography

Hoffstein, J.; Pipher, J.; Silverman, J.H.

2008, XVI, 524 p. 29 illus., Hardcover

ISBN: 978-0-387-77993-5