An Introduction to Mathematical Cryptography

Second Edition

Solution Manual

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

January 19, 2015

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.)

(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.

AOLYLHYLUVZLJYLAZILAALYAOHUAOLZLJYLAZAOHALCLYFIVKFNBLZZLZ

(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) apageofhistoryisworthavolumeoflogic
LALRPZQSTDEZCJTDHZCESLGZWFXPZQWZRTN

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

(b) therearenosecretsbetterthanthesecretsthateverybodyguesses
AOLYLHYLUVZLJYLAZILAALYAOHUAOLZLJYLAZAOHALCLYFIVKFNBLZZLZ

> 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) `LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBDVDWUHH`

(b) `UXENRBWXCUXENFQRLQJUCNABFQNWRCJUCNAJCRXWORWMB`

(c) `BGUTBMBGZTFHNLXMKTIPBMAVAXXLXTEPTRLEXTOXKHHFYHKMAXFHNLX`

Solution to Exercise 1.2.

(a)

```
ithinkthatishallneverseeabillboardlovelyasatree
LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBDVDWUHH
```

> 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
BGUTBMBGZTFHNLXMKTIPBMAVAXXLXTEPTRLEXTOXKHHFYHKMAXFHNLX
```

> 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 GKBJT
QDIQS LWJNR OLGRI EZJGK ZRBGS MJLDG IMNZT OIHRK MOSOT QHIJL
QBRJN IJJNT ZFIZL WIZTO MURZM RBTRZ ZKBNN LFRVR GIZFL KUHIM
MRIGJ LJNRB GKHRT QJRUU RBJLW JNRZI TULGI EZLUK JRUST QZLUK
EURFT JNLKJ JNRXR S
```

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 LNMRG 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 OIDLV JXGAK CGJCG
SASUB FVQAV CIAWN VWOVP SNSXV JGPCV NODIX GJQAE VOOXC SXXCG
OGOVA XGNVU BAVKX QZVQD LVJXQ EXCQO VKCQG AMVAX VWXCG OOBOX
VZCSO SPPSN VAXUB DVVAX QJQAJ VSUXC SXXCV OVJCS NSJXV NOJQA
MVBSZ VOOSH VSAWX QHGMV GWVSX CSXXC VBSNV ZVNVN 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.

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

(b) A letter in the alphabet is said to be *fixed* if the encryption of the letter is the letter itself. How many simple substitution ciphers are there that leave:

(i) no letters fixed?

(ii) at least one letter fixed?

(iii) exactly one letter fixed?

(iv) 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,

$$\mathbf{S}(n,k) = \binom{n}{k}(n-k)! \quad \longleftarrow \textbf{Incorrect Formula}.$$

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:

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

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:

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

Now if we notice that

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

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

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

we see that

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

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

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

Now noticing that

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

the formula for $!n$ becomes

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

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

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

Multiplying by $n!$ and using the formula for $!n$ yields

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

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

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

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

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

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

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

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

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

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

Hence

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

(b-iii) Exactly 1 letter fixed is

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

so

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

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

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

Hence

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

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

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

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 $0 \le r < g$. 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 $0 \le r < g$ 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

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

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

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

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

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

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 $0 \le t < y$
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 $a_1, a_2, \ldots, a_k$ be integers with $\gcd(a_1, a_2, \ldots, a_k) = 1$, i.e., the largest positive integer dividing all of $a_1, \ldots, a_k$ is 1. Prove that the equation

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

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

Solution to Exercise 1.13.

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

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

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

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

To ease notation, we let $b = \gcd(a_1, \ldots, a_{k-1})$. 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 subtituting this equation gives

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

Hence

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

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

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

1.14. Let a and b be integers with $b > 0$. We've been using the "obvious fact" that a divided by b has a unique quotient and remainder. In this exercise you will give a proof.

(a) Prove that the set
$$\{a - bq : q \in \mathbb{Z}\}$$
contains at least one non-negative integer.

(b) Let r be the smallest non-negative integer in the set described in (a). Prove that $0 \le r < b$.

(c) Prove that there are integers q and r satisfying
$$a = bq + r \quad \text{and} \quad 0 \le r < b.$$

(d) Suppose that
$$a = bq_1 + r_1 = bq_2 + r_2 \quad \text{with} \quad 0 \le r_1 < b \quad \text{and} \quad 0 \le r_2 < b.$$
Prove that $q_1 = q_2$ and $r_1 = r_2$.

Solution to Exercise 1.14.

(a) The quantity $a - bq$ will be non-negative if we take any $q < a/b$. (Note that $b > 0$ by assumption.) So we just need to take an integer $q < a/b$. (If $a < 0$, then $q < 0$, but that's okay.)

(b) Since r is in the set from (a), we know that $r = a - bq$ for some integer q. The integer r is non-negative by assumption, so we just need to show that $r < b$. Suppose to the contrary that $r \ge b$. Then
$$r = a - bq > a - b(q+1) = r - b \ge 0,$$
so the number $a - b(q+1)$ is a non-negative element of the set in (a) that is strictly smaller than r. This contradicts the assumption that r is the smallest non-negative element of the set in (a). Hence $r < b$.

(c) We just need to combine (a) and (b). From (a) we know the set contains some non-negative integers, and from (b) we know that the smallest non-negative element r satisfies $0 \le r < b$. Since r is in the set, it has the form $r = a - bq$ for some q, and hence $a = bq + r$.

(d) We have
$$0 = a - a = (bq_1 + r_1) - (bq_2 + r_2) = b(q_1 - q_2) + (r_1 - r_2).$$
The fact that $0 \le r_1 < b$ and $0 \le r_2 < b$ implies that $|r_1 - r_2| < b$, so we have
$$b > |r_1 - r_2| = \bigl|b(q_1 - q_2)\bigr|.$$
Since $b \ge 1$, this implies that
$$1 > |q_1 - q_2|.$$
But q_1 and q_2 are integers, and the only integer t satisfying $1 > |t|$ is $t = 0$. Therefore $q_1 = q_2$, and then also $r_1 = a - bq_1 = a - bq_2 = r_2$.

Section. Modular arithmetic

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

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

Prove that

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

(This is Proposition 1.13(a).)

Solution to Exercise 1.15.

1.16. 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 1.16.

(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

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

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

(b) $3274 + 1238 + 7231 + 6437 \equiv \boxed{} \pmod{9254}$.

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

(d) $357 \cdot 862 \cdot 193 \equiv \boxed{} \pmod{943}$.

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

(f) $137^2 \equiv \boxed{} \pmod{327}$.

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

(h) $23^3 \cdot 19^5 \cdot 11^4 \equiv \boxed{} \pmod{97}$.

Solution to Exercise 1.17.

(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) $23^3 \cdot 19^5 \cdot 11^4 \equiv \boxed{93} \pmod{97}$.

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

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

(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 $0 \le x \le 34$.)

Solution to Exercise 1.18.

(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 $x = 0, 1, 2, \ldots, 10$ 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 $x = 0, 1, 2, \ldots, 34$. A faster method is to list the solutions to $x \equiv 1 \pmod 5$, namely $1, 6, 11, 16, 21, 26, 31, \ldots$ 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 $\boxed{x = 16}$.

1.19. 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 1.19.

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

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

1.20. Prove that if a_1 and a_2 are units modulo m, then a_1a_2 is a unit modulo m.

Solution to Exercise 1.20.

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

$$a_1b_1 \equiv 1 \pmod m \quad \text{and} \quad a_2b_2 \equiv 1 \pmod m.$$

Then

$$(a_1a_2)(b_1b_2) \equiv (a_1b_1)(a_2b_2) \equiv 1 \cdot 1 \equiv 1 \pmod m,$$

so a_1a_2 is a unit. Its inverse is b_1b_2.

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

Solution to Exercise 1.21.

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 $1 \le k < m$, 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

$$\phi(m) = \#\bigl\{1 \le k < m : \gcd(k, m) = 1\bigr\} = \#\{1, 2, 3, \ldots, m - 1\} = m - 1.$$

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 $d \ne m$. Then $1 \le d \le m - 1$, 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.

1.22. 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 1.22.

(a) The fact that m is odd means that $\boxed{\frac{m+1}{2}}$ 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 $\boxed{\frac{1+(b-1)m}{b}}$.

1.23. 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 1.23.

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.

1.24. (a) Find a single value x that simultaneously solves the two congruences

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

(*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

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

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

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

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

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

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 1.24.

(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.

1.25. 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 1.25.

A solution for this exercise is not currently available.

1.26. Use the square-and-multiply algorithm described in Section 1.3.2, or the more efficient version in Exercise 1.25, to compute the following powers.
(a) $17^{183} \pmod{256}$.
(b) $2^{477} \pmod{1000}$.
(c) $11^{507} \pmod{1237}$.

Solution to Exercise 1.26.

$$\begin{array}{lll}
\text{(a)} & 183 = 1 + 2 + 2^2 + 2^4 + 2^5 + 2^7, & 17^{183} \pmod{256} = \boxed{113}. \\
\text{(b)} & 477 = 1 + 2^2 + 2^3 + 2^4 + 2^6 + 2^7 + 2^8, & 2^{477} \pmod{1000} = \boxed{272} \\
\text{(c)} & 507 = 1 + 2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7 + 2^8, & 11^{507} \pmod{1237} = \boxed{322}.
\end{array}$$

1.27. Consider the congruence

$$ax \equiv c \pmod{m}.$$

(a) Prove that there is a solution if and only if $\gcd(a, m)$ divides c.
(b) If there is a solution, prove that there are exactly $\gcd(a, m)$ distinct solutions modulo m.
(*Hint.* Use the extended Euclidean algorithm (Theorem 1.11).)

Solution to Exercise 1.27.

A solution for this exercise is not currently available.

Section. Prime numbers, unique factorization, and finite fields

1.28. Let $\{p_1, p_2, \ldots, p_r\}$ 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 1.28.

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 $p_1, p_2, \ldots, p_r$. 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.

1.29. 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 1.29.

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 $a \mid c$.

1.30. Compute the following ord_p values:
(a) $\mathrm{ord}_2(2816)$.
(b) $\mathrm{ord}_7(2222574487)$.
(c) $\mathrm{ord}_p(46375)$ for each of $p = 3$, 5, 7, and 11.

Solution to Exercise 1.30.

(a) $\mathrm{ord}_2(2816) = 8$.

(b) $\mathrm{ord}_7(2222574487) = 5$.

(c) Let $a = 46375$. Then $\mathrm{ord}_3(a) = 0$, $\mathrm{ord}_5(a) = 3$, $\mathrm{ord}_7(a) = 1$, $\mathrm{ord}_{11}(a) = 0$.

1.31. Let p be a prime number. Prove that ord_p has the following properties.

(a) $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$. (Thus ord_p resembles the logarithm function, since it converts multiplication into addition!)

(b) $\mathrm{ord}_p(a+b) \ge \min\bigl\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\bigr\}$.

(c) If $\mathrm{ord}_p(a) \ne \mathrm{ord}_p(b)$, then $\mathrm{ord}_p(a+b) = \min\bigl\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\bigr\}$.

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

Solution to Exercise 1.31.

(a) By definition of ord_p, we have

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

Then

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

so by definition,

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

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

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

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

$$\mathrm{ord}_p(a+b) \ge \mathrm{ord}_p(b).$$

(Note that we've set things up so that $\mathrm{ord}_p(b) = \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}$, 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 $\mathrm{ord}_p(a) > \mathrm{ord}_p(b)$. We also know that $p \nmid B$, so it follows that

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

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

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

Section. Powers and primitive roots in finite fields

1.32. 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 1.27.)

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

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

(c) $p = 104801$ and $a = 78467$.

Solution to Exercise 1.32.

(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

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

1.33. 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 1.29.)

(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 1.30.)

Solution to Exercise 1.33.

(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 1.29 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 $0 \le i < p-1$. We'll count the number of a with $a^{(p-1)/q} = 1$. Thus

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

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

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

Hence

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

It follows that

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

Hence

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

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

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

(a) For which of the following primes is 2 a primitive root modulo p?
(i) $p = 7$ (ii) $p = 13$ (iii) $p = 19$ (iv) $p = 23$

(b) For which of the following primes is 3 a primitive root modulo p?
(i) $p = 5$ (ii) $p = 7$ (iii) $p = 11$ (iv) $p = 17$

(c) Find a primitive root for each of the following primes.
(i) $p = 23$ (ii) $p = 29$ (iii) $p = 41$ (iv) $p = 43$

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

(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 $\phi(228)$ 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 1.34.
(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

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

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.

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

$$g \not\equiv 0 \pmod{p} \qquad \text{and} \qquad g \not\equiv \pm 1 \pmod{p} \qquad \text{and} \qquad g^q \not\equiv 1 \pmod{p}.$$

Prove that g is a primitive root modulo p.

Solution to Exercise 1.35.

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 1.29. Since $p - 1 = 2q$ with q prime, this means that

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

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.

1.36. 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 1.36.

(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.

1.37. 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

$$X^2 \equiv b \pmod{p^e} \tag{1.1}$$

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 β and β' be two solutions as in (b). Prove that $\beta \equiv \beta' \pmod{p^e}$.

(d) Use Exercise 1.36 to deduce that the congruence (1.14) has either two solutions or no solutions modulo p^e.

Solution to Exercise 1.37.

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 $\beta \bmod p^e$ satisfying both

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

The case $e = 1$ is given to us, we must take $\beta = \alpha$. Now suppose that we have a value of β that works for e, and we ask for all solutions that work for $e+1$. Note that if γ is a solution for $e+1$, then $\gamma \bmod p^e$ 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 γ for $e+1$, then γ is forced to have the form

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

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

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

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

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

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

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 $e \ge 1$ there exists a unique value of β (mod p^e) satisfying

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

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 there certainly aren't any solutions to $X^2 \equiv b \pmod{p^e}$ for $e \ge 2$, 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 $e \ge 1$, 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.

1.38. Compute the value of

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

for every prime $3 \le p < 20$. 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 1.38.

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

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

1.39. 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 1.39.
A solution for this exercise will not be provided.

1.40. 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	↗	▷	◇	∧			↘	Δ	∇	8	♣		Ω	∨	⊗	♠				♭	
Θ				∞		⇑		♮					•	⊙				◁	⊕	⇐					
↙				⇓														⇒	↖						

Decrypt the following message.

(% Δ ♠ ⇒ ♮ # 4 ∞ : ◇ 6 ↗ ⊙ [ℵ 8 % 2 [7 ⇓ ♣ ↘ ♡ 5 ⊙ ∇

Solution to Exercise 1.40.

(	%	Δ	♠	⇒	♮	#	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...`

1.41. A *transposition cipher* is a cipher in which the letters of the plaintext remain the same, but their order is rearranged. Here is a simple example in which the message is encrypted in blocks of 25 letters at a time.[1] Take the given 25 letters and arrange them in a 5-by-5 block by writing the message horizontally on the lines. For example, the first 25 letters of the message

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

is written as

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

Now the cipehrtext 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 1.41.

(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

[1] 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.

(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

1.42. 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 1.42.

`B`	`a`	`d`		`d`	`a`	`y`	`,`
66	97	100	32	100	97	121	44
01000010	01100001	01100100	00100000	01100100	01100001	01111001	00101100

	`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

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

(a) Let $p = 541$ and let the key be $k = (34, 71)$. Encrypt the message $m = 204$. Decrypt the ciphertext $c = 431$.

(b) Assuming that p is public knowledge, explain why the affine cipher is vulnerable to a known 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?

(c) 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 $m_3 = 173$.

(d) Suppose now that p is not public knowledge. Is the affine cipher still vulnerable to a known plaintext attack? If so, how many plaintext/ciphertext pairs are likely to be needed in order to recover the private key?

Solution to Exercise 1.43.

(a) The encryption of $m = 204$ is $c \equiv 34\cdot204+71 \equiv 7007 \equiv 515 \pmod{541}$. 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

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

for the two unknowns k_1 and k_2.

(c) Eve knows that

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

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

$$\begin{aligned}
c_1 &\equiv k_1 m_1 + k_2 \pmod{p}\\
c_2 &\equiv k_1 m_2 + k_2 \pmod{p}\\
c_3 &\equiv k_1 m_3 + k_2 \pmod{p}
\end{aligned}$$

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 $D_1, \ldots, D_{n-2}$ 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 $\gcd(D_1, \ldots, D_{n-2})$ is equal to p.

1.44. Consider the Hill cipher defined by (1.11),

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

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 $k_1 = \left(\begin{smallmatrix} 1 & 3\\ 2 & 2 \end{smallmatrix}\right)$ and $k_2 = \left(\begin{smallmatrix} 5\\ 4 \end{smallmatrix}\right)$.

  (i) Encrypt the message $m = \left(\begin{smallmatrix} 2\\ 1 \end{smallmatrix}\right)$.

  (ii) What is the matrix k_1^{-1} used for decryption?

  (iii) Decrypt the message $c = \left(\begin{smallmatrix} 3\\ 5 \end{smallmatrix}\right)$.

(b) Explain why the Hill cipher is vulnerable to a known 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.

$$m_1 = \left(\begin{smallmatrix} 5\\ 4 \end{smallmatrix}\right), \quad c_1 = \left(\begin{smallmatrix} 1\\ 8 \end{smallmatrix}\right), \quad m_2 = \left(\begin{smallmatrix} 8\\ 10 \end{smallmatrix}\right), \quad c_2 = \left(\begin{smallmatrix} 8\\ 5 \end{smallmatrix}\right), \quad m_3 = \left(\begin{smallmatrix} 7\\ 1 \end{smallmatrix}\right), \quad c_3 = \left(\begin{smallmatrix} 8\\ 7 \end{smallmatrix}\right).$$

(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 1.44.

(a)(i) $e_k(m) = \left(\begin{smallmatrix} 5 & 3 \end{smallmatrix}\right)$.

(a) (ii) $k_1^{-1} = \left(\begin{smallmatrix} 3 & 6 \\ 4 & 5 \end{smallmatrix}\right)$.

(a) (iii) $d_k(c) = \left(\begin{smallmatrix} 0 & 4 \end{smallmatrix}\right)$.

(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 $k_1 = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ and $k_2 = \left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$. 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

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

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

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

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

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

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:

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

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

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

Hence

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

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

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

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

1.45. 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 1.45.

(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 possibly 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.

1.46. (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 1.46.

(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)

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

1.47. 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 8.12 for further information about DES and AES.

Solution to Exercise 1.47.
(a)

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

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)

$$\begin{aligned}
&\left(\frac{10{,}000{,}000{,}000 \text{ keys}}{1 \text{ second}}\right) \cdot \left(\frac{60 \text{ seconds}}{1 \text{ minute}}\right) \cdot \left(\frac{60 \text{ minutes}}{1 \text{ hour}}\right) \\
&\qquad \cdot \left(\frac{24 \text{ hours}}{1 \text{ day}}\right) \cdot \left(\frac{365.25 \text{ days}}{1 \text{ year}}\right) \cdot (100 \text{ years}) \\
&\qquad = 31557600000000000000 \text{ keys} \approx 2^{64.775} \text{ keys}.
\end{aligned}$$

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.

1.48. Explain why the cipher

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

defined by XOR of bit strings is not secure against a known 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 $m = 0010010000101100$.

<u>*Solution to Exercise* 1.48</u>.

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,

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

1.49. 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

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

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 α be this d-digit number. (For example, if $k = 87$ and $d = 6$, then $\sqrt{87} = 9.32737905\ldots$ and $\alpha = 327379$.)

Alice encrypts a message m as

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

Since Bob knows k, he can also find α, 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 α 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 α, 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 1.49.

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

(b) $\sqrt{23} = 4.7958315233127195\ldots$, 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

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

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 $k = \frac{1}{4}A^2 - B$.

1.50. 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:

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

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

Solution to Exercise 1.50.

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 65 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 $n \in \mathbb{Z}$.

<u>Solution to Exercise 2.3</u>.

(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 65 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 $n \log_g(h) = \log_g(h^n)$.

2.4. Compute the following discrete logarithms.

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

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

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

Solution 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 $p-1$ is even.

Solution to Exercise 2.5.

This solution is taken from the proof of Proposition 3.61.

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 1.24) 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 progammable 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 $\sqrt{1373} = 37.04\ldots$. 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 *Decision Diffie–Hellman Problem* is as follows. Supoose that you are given three numbers A, B, and C, and suppose that A and B are equal to

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

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

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

(b) Do you think that the decision Diffie–Hellman problem is hard or easy? Why?

See Exercise 6.40 for a related example in which the decision problem is easy, but it is believed that the associated computational problem is hard.

Solution 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 decision Diffie–Hellman 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 random element $k = 877$. What is the ciphertext (c_1, c_2) that Alice sends to Bob?

(c) Alice decides to choose a new private key $a = 299$ with associated public key $A \equiv 2^{299} \equiv 34 \pmod{1373}$. Bob encrypts a message using Alice's public key and sends her the ciphertext $(c_1, c_2) = (661, 1325)$. Decrypt the message.

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

Solution to Exercise 2.8.

(a) $A \equiv 2^{947} \equiv 177 \pmod{1373}$, so Alice's public key is $\boxed{A = 177}$.

(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 $\boxed{(c_1, c_2) = (719, 623)}$ 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 $\boxed{\text{m=332}}$. It turns out that the random element is $k = 566$, but Alice does not know this value.

(d) The solution to $2^b \equiv 893 \pmod{1373}$ is $\boxed{b = 219}$, which is Bob's private key. (At this point in the text, the only way to find b would be use a computer to compute $2^k \bmod 1373$ for $k = 1, 2, \ldots$ until finding the solution.) 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 $\boxed{m = 365}$. (The random element was $k = 932$.)

2.9. Suppose that Eve is able to solve the Diffie–Hellman problem described on page 69. More precisely, assume that if Eve is given two powers g^u and g^v mod p, then she is able to compute g^{uv} mod p. Show that Eve can break the Elgamal PKC.

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 random element. You thus know the values of g^a and g^k, so solving the Diffie–Hellman problem oracle gives 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.

(a) 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?

(b) Formulate a general version of this cryptosystem, i.e., using variables, and show that it works in general.

(c) What is the disadvantage of this cryptosystem over Elgamal? (*Hint.* How many times must Alice and Bob exchange data?)

(d) 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.

(a) Alice's and Bob's exponents satisfy

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

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

(b) In the general formulation, a public prime p is fixed. Alice choose a plaintext m mod p and a random exponent a satisfying $\gcd(a, p-1) = 1$. She send

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

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

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

and send 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 $a' = a^{-1} \bmod p-1$. 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 $w^{b'} \bmod p$ 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

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

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

(c) Elgamal only require 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

$$\sigma^3 = e, \qquad \tau^2 = e, \qquad \tau\sigma = \sigma^2\tau.$$

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.)

<u>Solution to Exercise</u> 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 succintly 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

$$(g_1g_2)^d = g_1g_2g_1g_2 \cdots g_1g_2 = g_1^dg_2^d = ee = e.$$

Therefore $g_1g_2 \in G[d]$.

(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 form 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 $A = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ satisfies $A^2 = I$ and the matrix $B = \left(\begin{smallmatrix}1&-1\\0&-1\end{smallmatrix}\right)$ satisfies $B^2 = I$, but $AB = \left(\begin{smallmatrix}1&-1\\0&-1\end{smallmatrix}\right)$ actually has order 3, i.e., $(AB)^3 = I$.

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

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

(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

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

(b) Let G be a commutative group. Prove that the map $\phi : G \to G$ 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 $\phi : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ that sends $a \in \mathbb{Z}$ to $a \bmod N$ in $\mathbb{Z}/N\mathbb{Z}$.

(b) The map $\phi : \mathbb{R}^* \to \mathrm{GL}_2(\mathbb{R})$ defined by $\phi(a) = \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$.

(c) The discrete logarithm map $\log_g : \mathbb{F}_p^* \to \mathbb{Z}/(p-1)\mathbb{Z}$, 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 $\mathrm{GL}_2(\mathbb{F}_p)$ is a group.

(b) Show that $\mathrm{GL}_2(\mathbb{F}_p)$ is a noncommutative group for every prime p.

(c) Describe $\mathrm{GL}_2(\mathbb{F}_2)$ completely. That is, list its elements and describe the multiplication table.

(d) How many elements are there in the group $\mathrm{GL}_2(\mathbb{F}_p)$?

(e) How many elements are there in the group $\mathrm{GL}_n(\mathbb{F}_p)$?

Solution to Exercise 2.15.

(a) The identity element is the usual matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. The definition of $\mathrm{GL}_2(\mathbb{F}_p)$ 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 $\mathrm{GL}_2(\mathbb{F}_2)$ has 6 elements:

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

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 $\mathrm{GL}_2(\mathbb{F}_2)$ is the same as the group $\mathcal{S}_3$ described in that exercise, we've just named the generating elements α and γ instead of σ and τ.

(d) Let α be a matrix in $\mathrm{GL}_2(\mathbb{F}_p)$. 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

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

(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

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

Section. How hard is the discrete logarithm problem?

2.16. Verify the following assertions from Example 2.16.

(a) $x^2+\sqrt{x} = \mathcal{O}\left(x^2\right)$.

(b) $5+6x^2-37x^5 = \mathcal{O}\left(x^5\right)$.

(c) $k^{300} = \mathcal{O}\left(2^k\right)$.

(d) $(\ln k)^{375} = \mathcal{O}\left(k^{0.001}\right)$.

(e) $k^2 2^k = \mathcal{O}\left(e^{2k}\right)$.

(f) $N^{10}2^N = \mathcal{O}\left(e^N\right)$.

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 $\boxed{\text{x=37}}$.

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

(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

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

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 $\boxed{\text{x=59}}$.

(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 $k = 1, 2, \ldots$. 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 $\boxed{\text{x=319}}$.

Section. The Chinese remainder theorem

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

(a) $x \equiv 3 \pmod 7$ and $x \equiv 4 \pmod 9$.

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

k	h^k	$a \cdot H^k$	k	h^k	$a \cdot H^k$	k	h^k	$a \cdot H^k$	k	h^k	$a \cdot H^k$
1	650	3393	6	1650	694	11	2815	2430	16	2476	677
2	1122	166	7	1200	396	12	1398	3311	17	2450	3381
3	816	1731	8	1522	1677	13	1666	**3011**	18	3405	2063
4	1892	432	9	133	41	14	887	442	19	2801	323
5	1376	3128	10	746	363	15	1619	952	20	**3011**	421

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

(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 84.

Solution to Exercise 2.19.

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

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

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 $x = a + cm$ is a solution to

$$x \equiv a \pmod m \qquad \text{and} \qquad x \equiv b \pmod n, \tag{2.1}$$

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

Solution to Exercise 2.20.

A solution for this exercise is not currently available.

2.21. (a) Let a, b, c be positive integers and suppose that

$$a \mid c, \quad b \mid c, \quad \text{and} \quad \gcd(a,b) = 1.$$

Prove that $ab \mid c$.

(b) Let $x = c$ and $x = c'$ be two solutions to the system of simultaneous congruences (2.7) in the Chinese remainder theorem (Theorem 2.24). Prove that

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

Solution to Exercise 2.21.

(a) Factor $a = \prod p_i^{e_i}$ and $b = \prod q_j^{f_j}$ into products of primes. Since $\gcd(a,b) = 1$, they have no prime factors in common. And since $a \mid c$ and $b \mid c$, every prime power dividing a or b appears in the factorization of c into primes.

(b) Use (a) and induction on k.

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

(a) Prove that the map

$$\begin{array}{ccc} \dfrac{\mathbb{Z}}{m\mathbb{Z}} & \longrightarrow & \dfrac{\mathbb{Z}}{m_1\mathbb{Z}} \times \dfrac{\mathbb{Z}}{m_2\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{m_k\mathbb{Z}} \\ a \bmod m & \longrightarrow & (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_k) \end{array} \qquad (2.2)$$

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 $m_1, \ldots, m_k$ 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 $m_1, \ldots, m_k$ 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 2.24) 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, let a be an integer that is not divisible by p, 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 distinct odd 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 that 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) The Chinese Remainder Theorem says that the solutions to $x^2 \equiv a \pmod{n}$ match up with the pairs of values (y, z) satisfying $y^2 \equiv a \pmod{p}$ and $z^2 \equiv a \pmod{q}$. We're given that $x^2 \equiv a \pmod{n}$ has at least one solution, call it x_1, so we get a pair (y_1, z_1) determined by

$$y_1 \equiv x_1 \pmod{p} \quad \text{and} \quad z_1 \equiv x_1 \pmod{q}.$$

Since $\gcd(a, pq) = 1$, it follows that $\gcd(x_1, pq) = 1$, so $\gcd(y_1, p) = 1$ and $\gcd(z_1, q) = 1$. In other words, y_1 and z_1 are nonzero. So we get four *different* solutions

$$(y_1, z_1), \quad (-y_1, z_1), \quad (y_1, -z_1), \quad (-y_1, -z_1)$$

to the pair of congruences

$$y^2 \equiv a \pmod{p} \qquad \text{and} \qquad z^2 \equiv a \pmod{q}.$$

The Chinese Remainder Theorem tells us that they correspond to four different solutions of $x^2 \equiv a \pmod{pq}$.
(b) Let x_1, x_2, x_3, x_4 be the four solutions to $x^2 \equiv a \pmod{pq}$. If x is a solution, then $-x$ is also a solution, so after relabeling, the four solutions look like $x_1, x_2, -x_1, -x_2$. Consider the quantities

$$A \equiv x_1 - x_2 \pmod{p} \qquad \text{and} \qquad B \equiv x_1 - x_2 \pmod{q}.$$

We can't have $A = 0$ and $B = 0$, since that would imply that $x_1 \equiv x_2 \pmod{pq}$, so x_1 and x_2 wouldn't be different solutions. On the other, at least one of them is zero, since as noted in (a), when we look at the four solutions modulo p and modulo q, they look like

$$(y, z), \quad (-y, z), \quad (y, -z), \quad (-y, -z).$$

Hence $\gcd(pq, x_1 - x_2)$ is equal to either p or q, which gives the factorization of n.

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 2.31) to solve the discrete logarithm problem

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

in each of the following cases.

(a) $p = 433, \quad g = 7, \quad a = 166$.
(b) $p = 746497, \quad g = 10, \quad a = 243278$.
(c) $p = 41022299, \quad g = 2, \quad a = 39183497$. (*Hint.* $p = 2 \cdot 29^5 + 1$.)
(d) $p = 1291799, \quad g = 17, \quad a = 192988$. (*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

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

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

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

The solution is $\boxed{\text{x=223755}}$.
(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 $18794375^{u_0} = \left(11844727\right)^{29^4} = 987085$. The solution is $u_0 = 7$. The value of u so far is $u = 7$.

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

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

Solve $18794375^{u_3} = \left(11844727 \cdot 4^{-22105}\right)^{29^1} = 585477$. 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 $18794375^{u_4} = \left(11844727 \cdot 4^{-461107}\right)^{29^0} = 585477$. 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

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

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

(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

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

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

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 2.55, 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 $R \to R$ 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.

(a) 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 $a \in R$.

(b) Prove that the multiplicative identity element $1 \in R$ is unique.

(c) Prove that every element of R has a unique additive inverse.

(d) Prove that $0 \star a = a \star 0 = 0$ for all $a \in R$.

(e) We denote the additive inverse of a by $-a$. Prove that $-(-a) = a$.

(f) Let -1 be the additive inverse of the multiplicative identity element $1 \in R$. Prove that $(-1) \star (-1) = 1$.

(g) Prove that $b \mid 0$ for every nonzero $b \in R$.

(h) Prove that an element of R has at most one multiplicative inverse.

Solution to Exercise 2.30.

(a) 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. Let R and S be rings. A function $\phi : R \to S$ is called a (*ring*) *homomorphism* if it satisfies

$$\phi(a + b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(a \star a) = \phi(a) \star \phi(a) \qquad \text{for all } a, b, \in R.$$

(a) Let 0_R, 0_S, 1_R and 1_S denote the additive and multiplicative identities of R and S, respectively. Prove that

$$\phi(0_R) = 0_S, \quad \phi(1_R) = 1_S, \quad \phi(-a) = -\phi(a), \quad \phi(a^{-1}) = \phi(a)^{-1},$$

where the last equality holds for those $a \in R$ that have a multiplicative inverse.

(b) Let p be a prime, and let R be a ring with the property that $pa = 0$ for every $a \in R$. (Here pa means to add a to itself p times.) Prove that the map

$$\phi : R \longrightarrow R, \qquad \phi(a) = a^p$$

is a ring homomorphism. It is called the *Frobenius homomorphism.*

Solution to Exercise 2.31.

A solution for this exercise is not currently available.

2.32. Prove Proposition 2.41.

Solution to Exercise 2.32.

A solution for this exercise is not currently available.

2.33. Prove Proposition 2.43. (*Hint.* First use Exercise 2.32 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 2.33.

A solution for this exercise is not currently available.

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

(a) Prove that $\deg(\boldsymbol{a} \cdot \boldsymbol{b}) = \deg(\boldsymbol{a}) + \deg(\boldsymbol{b})$.

(b) Prove that $\boldsymbol{a}$ has a multiplicative inverse in $\mathbb{F}[x]$ if and only if $\boldsymbol{a}$ is in $\mathbb{F}$, i.e., if and only if $\boldsymbol{a}$ is a constant polynomial.

(c) 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 $\boldsymbol{a}$ and $\boldsymbol{b}$ in $R[x]$.

Solution to Exercise 2.34.

(a) *A solution for this exercise is not currently available.*

(b) If $\boldsymbol{a} \cdot \boldsymbol{b} = 1$, then taking degrees and using (a) gives

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

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

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

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

so the degree formula in (a) is false.

2.35. Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be the polynomials

$$\begin{aligned}\boldsymbol{a} &= x^5+3x^4-5x^3-3x^2+2x+2,\\ \boldsymbol{b} &= x^5+x^4-2x^3+4x^2+x+5.\end{aligned}$$

Use the Euclidean algorithm to compute $\gcd(\boldsymbol{a},\boldsymbol{b})$ 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 2.35.
(a) $\gcd_{\mathbb{F}_2[x]}(\boldsymbol{a},\boldsymbol{b}) = x^3+x^2+x+1$.
(b) $\gcd_{\mathbb{F}_3[x]}(\boldsymbol{a},\boldsymbol{b}) = x^2+x+2$.
(c) $\gcd_{\mathbb{F}_5[x]}(\boldsymbol{a},\boldsymbol{b}) = x+4$.
(d) $\gcd_{\mathbb{F}_7[x]}(\boldsymbol{a},\boldsymbol{b}) = 1$.

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

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

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

Solution to Exercise 2.36.
(a) $\boldsymbol{u} = 1$ and $\boldsymbol{v} = 1$.
(b) $\boldsymbol{u} = x+1$ and $\boldsymbol{v} = 2x$.
(c) $\boldsymbol{u} = 3x^3+4x^2+x+2$ and $\boldsymbol{v} = 2x^3+x$.
(d) $\boldsymbol{u} = 3x^4+3x^3+x^2+5x+4$ and $\boldsymbol{v} = 4x^4+5x^3+x^2+2x$.

2.37. 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 2.37.

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

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

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 $\mathbb{F}_2[x]$.

2.38. 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 2.57. You can download and print a copy of Table 2.5 at `www.math.brown.edu/~jhs/MathCrypto/Table2.5.pdf`.)

Solution to Exercise 2.38.

Note that it's not necessary to compute both $\boldsymbol{a} \cdot \boldsymbol{b}$ and $\boldsymbol{b} \cdot \boldsymbol{a}$. 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 $\mathbb{F}_2[x]/(x^3 + x + 1)$

2.39. 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 2.58 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 2.39.

(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, $(1+x)^{24} = 1$.

2.40. 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 2.40.

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 α 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 $\alpha^{p^e} = 0$.

2.41. 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 $1,\ 1+1,\ 1+1+1, \ldots$ 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 2.41.

(a) The fact that $\mathbb{F}$ is finite means that when we look at
$$1, \quad 1+1, \quad 1+1+1, \quad 1+1+1+1, \ldots$$

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

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

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 $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_d$ 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

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

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 $70 \cdot 112 = 7840$. 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. This exercise investigates what happens if we drop the assumption that $\gcd(e, p-1) = 1$ in Proposition 3.2. So let p be a prime, let $c \not\equiv 0 \pmod{p}$, let $e \ge 1$, and consider the congruence

$$x^e \equiv c \pmod{p}. \tag{3.1}$$

(a) Prove that if (3.36) has one solution, then it has exactly $\gcd(e, p-1)$ distinct solutions. (*Hint.* Use primitive root theorem (Theorem 1.30), combined with the extended Euclidean algorithm (Theorem 1.11) or Exercise 1.27.)

(b) For how many non-zero values of $c \pmod{p}$ does the congruence (3.36) have a solution?

Solution to Exercise 3.2.

A solution for this exercise is not currently available.

3.3. Let p and q be distinct primes and let e and d be positive 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 3.5.

Solution to Exercise 3.3.

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.

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

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

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.

(a) Compute the values of $\phi(6)$, $\phi(9)$, $\phi(15)$, and $\phi(17)$.
(b) If p is prime, what is the value of $\phi(p)$?
(c) 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 1.24), 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* 3.4.
A solution for this exercise is not currently available.

3.5. Euler's phi function has many beautiful properties.
(a) 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 $p_1, p_2, \ldots, p_r$ 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* 3.5.
(a)–(d) *A solution for this exercise is not currently available.*
(e) (i) $\phi(1728) = 576$, (ii) $\phi(1575) = 720$, (iii) $\phi(889056) = 254016$.

3.6. Let N, c, and e be positive integers satisfying the conditions $\gcd(N, c) = 1$ and $\gcd\bigl(e, \phi(N)\bigr) = 1$.
(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 3.4(c).)
(b) Solve the following congruences. (The formula in Exercise 3.5(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 3.6.

(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

3.7. 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 3.7.

(a) Bob sends $c = m^e = 892383^{103} \equiv \boxed{45293}$ (mod 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 $d \equiv \boxed{810367}$ (mod 2035800).

(c) Alice needs to solve

$$m^{103} \equiv 317730 \pmod{2038667}.$$

Raising both sides to the d^{th} power, where $d = 810367$ is her decryption exponent, yields

$$m \equiv 317730^{810367} \equiv \boxed{514407} \pmod{2038667}.$$

3.8. 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 3.8.

The modulus factors as $N = 12191 = 73 \cdot 167$, so $\phi(N) = 72 \cdot 168 = 11952$. 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

$$m \equiv 587^{5653} \equiv \boxed{4894} \pmod{12191}.$$

3.9. For each of the given values of $N = pq$ and $(p-1)(q-1)$, use the method described in Remark 3.11 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 3.9.

(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 $N = 172205490419 = 407893 \cdot 422183$.

3.10. 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 3.10.

Let $e_1, e_2, \ldots, e_n$ be a bunch of random encryption exponents, and suppose that Eve uses her magic box to create decryption exponents $d_1, d_2, \ldots, d_n$. The numbers K with the property that $a^K \equiv a \pmod{N}$ for all a satisfying $\gcd(a, N) = 1$ are numbers satisfying

$$K \equiv 1 \left(\operatorname{mod} \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} \right).$$

Thus $d_i e_i - 1$ is a multiple of $(p-1)(q-1)/\gcd(p-1, q-1)$ for all $1 \le i \le n$. Assuming that the e_i's are reasonably random, Eve will find that

$$T = \gcd(d_1 e_1 - 1, d_2 e_2 - 1, d_3 e_3 - 1, \ldots, d_n e_n - 1) \tag{3.2}$$

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 $N + 1 - 1 \cdot \text{gcd} = 19381152$, but $x^2 - 19381152x + 38749709$ is irreducible. Next she tries $N + 1 - 2 \cdot \text{gcd} = 12594$, and this time she finds that $x^2 - 12594x + 38749709 = (x - 7247)(x - 5347)$. Hence $N = 38749709 = 7247 \cdot 5347$.

(c)

$$\begin{aligned}\gcd(&4911157 \cdot 70583995 - 1, 7346999 \cdot 173111957 - 1,\\ &\qquad\qquad\qquad\qquad 29597249 \cdot 180311381 - 1)\\ &= \gcd(346649081132214, 1271853374967042, 5336720840990868)\\ &= 37498566\end{aligned}$$

Eve computes $(\sqrt{225022969} - 1)^2/37498566 \approx 6.00004193$, which suggests that she should try $N + 1 - 6 \cdot \gcd = 31574$. This given

$$x^2 - 31574x + 225022969 = (x - 20707)(x - 10867).$$

Hence $N = 225022969 = 20707 \cdot 10867$.
(d)

$$\begin{aligned}\gcd(&76923209 \cdot 1103927639 - 1, 106791263 \cdot 1022313977 - 1,\\ &\qquad\qquad\qquad\qquad 7764043 \cdot 387632407 - 1)\\ &= \gcd(84917656495673550, 109174200786382950, 3009594676141500)\\ &= 129112350\end{aligned}$$

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 $N = 1291233941 = 97151 \cdot 13291$.

3.11. Here is an example of a public key system that was proposed at a cryptography conference. It was designed to be 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

$$g_1 \equiv g^{r_1(p-1)} \pmod{N} \qquad \text{and} \qquad g_2 \equiv g^{r_2(q-1)} \pmod{N}.$$

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

$$c_1 \equiv m g_1^{s_1} \pmod{N} \qquad \text{and} \qquad c_2 \equiv m g_2^{s_2} \pmod{N}.$$

Bob sends the ciphertext (c_1, c_2) to Alice.

Decryption is extremely fast and easy. Alice uses the Chinese remainder theorem to solve the pair of congruences

$$x \equiv c_1 \pmod{p} \qquad \text{and} \qquad x \equiv c_2 \pmod{q}.$$

(a) Prove that Alice's solution x is equal to Bob's plaintext m.

(b) Explain why this cryptosystem is not secure.

Solution to Exercise 3.11.

(a) 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 $x \equiv m \pmod{pq}$.

(b) 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

3.12. Formulate a man-in-the-middle attack, similar to the attack described in Example 3.13 on page 126, for the following public key cryptosystems.

(a) The Elgamal public key cryptosystem (Table 2.3 on page 72).

(b) The RSA public key cryptosystem (Table 3.1 on page 123).

Solution to Exercise 3.12.

A solution for this exercise is not currently available.

3.13. 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 3.15 to help Eve recover Bob's plaintext without finding a factorization of N.

Solution to Exercise 3.13.

With notation as in Example 3.15, 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

3.14. 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 3.14.

(a) Fermat tells us that $a^{p-1} \equiv 1 \pmod{p}$ for every prime p and every number a with $p \nmid a$. In particular, if $3 \nmid a$, then

$$a^2 \equiv 1 \pmod{3}, \quad \text{so} \quad a^{561} = a \cdot (a^2)^{180} \equiv a \cdot 1^{180} \equiv a \pmod{3}.$$

Of course, if $3 \mid a$, we also clearly have $a^{561} \equiv a \pmod{3}$, since both sides are 0. Similarly, if $11 \nmid a$, then $a^{10} \equiv 1 \pmod{11}$, so

$$a^{561} = a \cdot (a^{10})^{56} \equiv a \cdot 1^{56} \equiv a \pmod{11}.$$

And if $17 \nmid a$, then $a^{16} \equiv 1 \pmod{11}$, so

$$a^{561} = a \cdot (a^{16})^{35} \equiv a \cdot 1^{35} \equiv a \pmod{17}.$$

So we have now proven that $a^{561} - a$ is divisible by 3 and by 11 and by 17, so it is divisible by their product $3 \cdot 11 \cdot 17 = 561$. This completes the proof that

$$a^{561} \equiv a \pmod{561} \quad \text{for all integers } a.$$

(b) We illustrate by doing (ii), the others are similar. If $5 \nmid a$, then $a^4 \equiv 1 \pmod{5}$, so

$$a^{10585} = a \cdot (a^4)^{2646} \equiv a \cdot 1^{2646} \equiv a \pmod{5}.$$

If $29 \nmid a$, then $a^{28} \equiv 1 \pmod{29}$, so

$$a^{10585} = a \cdot (a^{28})^{378} \equiv a \cdot 1^{378} \equiv a \pmod{29}.$$

If $73 \nmid a$, then $a^{72} \equiv 1 \pmod{73}$, so

$$a^{10585} = a \cdot (a^{72})^{147} \equiv a \cdot 1^{147} \equiv a \pmod{73}.$$

And of course, if 5 or 29 or 73 does divide a, then $a^{10585} \equiv a$ is automatically true modulo that prime, since both sides are 0. So we have now proven that $a^{10585} - a$ is divisible by 5 and by 29 and by 73, so it is divisible by their product $5 \cdot 29 \cdot 73 = 10585$. This completes the proof that

$$a^{10585} \equiv a \pmod{10585} \quad \text{for all integers } a.$$

(c) If N is a Carmichael number, then $a^N \equiv a \pmod{N}$ for all values of a. In particular, this is true for $a = -1$, so $(-1)^N \equiv -1 \pmod{N}$. Suppose that N is even. Then $1 \equiv -1 \pmod{N}$, so $2 \equiv 0 \pmod{N}$, so $N \mid 2$. This means that N is 1 or 2, which isn't possible, since Carmichael numbers are composite numbers, not primes. Hence N must be odd.

(d) Suppose that N is a Carmichael number, but that it is not a product of distinct primes. This means that there is some prime p so that N factors as $N = p^2M$. We now consider the Carmichael congruence $a^N \equiv a \pmod{N}$ with $a = p$. It says that

$$N \text{ divides } p^N - p.$$

Since $p^2 \mid N$, it follows that p^2 divides $p^N - p$. This means that we can write $p^N - p = p^2k$ for some k. But then

$$p = p^N - p^2k = p^2(p^N - k),$$

so p^2 would divide p. This is a contradiction, which completes the proof that N is a product of distinct primes.

Here is a list of all Carmichael up to 100000, plus a few others.

- $561 = 3 \cdot 11 \cdot 17$
- $1105 = 5 \cdot 13 \cdot 17$
- $1729 = 7 \cdot 13 \cdot 19$
- $2465 = 5 \cdot 17 \cdot 29$
- $2821 = 7 \cdot 13 \cdot 31$
- $6601 = 7 \cdot 23 \cdot 41$
- $8911 = 7 \cdot 19 \cdot 67$

- $10585 = 5 \cdot 29 \cdot 73$
- $15841 = 7 \cdot 31 \cdot 73$
- $29341 = 13 \cdot 37 \cdot 61$
- $41041 = 7 \cdot 11 \cdot 13 \cdot 41$
- $46657 = 13 \cdot 37 \cdot 97$
- $52633 = 7 \cdot 73 \cdot 103$
- $62745 = 3 \cdot 5 \cdot 47 \cdot 89$
- $63973 = 7 \cdot 13 \cdot 19 \cdot 37$
- $75361 = 11 \cdot 13 \cdot 17 \cdot 31$
- $294409 = 37 \cdot 73 \cdot 109$
- $56052361 = 211 \cdot 421 \cdot 631$
- $118901521 = 271 \cdot 541 \cdot 811$
- $172947529 = 307 \cdot 613 \cdot 919$
- $1024651 = 19 \cdot 199 \cdot 271$

3.15. 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) $n = 294439$
(d) $n = 118901509$ (e) $n = 118901521$
(f) $n = 118901527$ (g) $n = 118915387$

Solution to Exercise 3.15.
(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) $n - 1 = 118901526 = 2^1 \cdot 59450763$.

$$\begin{aligned}
2^{59450763} &\equiv 1 \quad &&\pmod{118901527}\\
3^{59450763} &\equiv -1 \quad &&\pmod{118901527}\\
5^{59450763} &\equiv -1 \quad &&\pmod{118901527}\\
7^{59450763} &\equiv 1 \quad &&\pmod{118901527}\\
11^{59450763} &\equiv 1 \quad &&\pmod{118901527}
\end{aligned}$$

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 $n = 6571 \cdot 18097$.

3.16. Looking back at Exercise 3.10, 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 3.16.

We are given an encryption/decryption pair (e,d), which means that

$$a^{de} \equiv a \pmod{N} \qquad \text{for all } 1 \le a < N.$$

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

$$a^r,\ a^{2r},\ a^{4r}, \dots,\ a^{2^k r} \bmod N.$$

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

$$a^r \equiv 1 \pmod{p}, \quad \text{or else} \quad a^{2^i r} \equiv -1 \pmod{p} \quad \text{for some } 0 \le i < k.$$

(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

$$a^r \equiv 1 \pmod q, \quad \text{or else} \quad a^{2^j r} \equiv -1 \pmod p \quad \text{for some } 0 \le j < k,$$

where again we choose the smallest such j.

We now consider several cases. If $a^r \equiv 1 \pmod p$ and $\alpha^r \not\equiv 1 \pmod q$, then we recover p by computing

$$\gcd(N, a^r - 1) = p.$$

Similarly, if $a^r \not\equiv 1 \pmod p$ and $\alpha^r \equiv 1 \pmod q$, 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 $\alpha^r \not\equiv 1 \pmod q$. 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 are done.
5. For each $0 \le i < k$, 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.

3.17. 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 3.17.

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

3.18. 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 $X \to \infty$?

Solution to Exercise 3.18.

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 $\lim_{X\to\infty} \pi_3(X)/\pi_1(X) = 1$. 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 $\lim_{X\to\infty} \pi_{a,N}(X)/\pi(X) = 1/\phi(N)$.

3.19. 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 3.21) for this problem.

(a) Fix a (large) number N and suppose that Bob chooses a random number n in the interval $\frac{1}{2}N \le n \le \frac{3}{2}N$. If he repeats this process many times, prove that approximately $1/\ln(N)$ of his numbers will be prime. More precisely, define

$$\begin{aligned} P(N) &= \frac{\text{number of primes between } \frac{1}{2}N \text{ and } \frac{3}{2}N}{\text{number of integers between } \frac{1}{2}N \text{ and } \frac{3}{2}N} \\ &= \left[\begin{array}{l}\text{Probability that an integer } n \text{ in the} \\ \text{interval } \frac{1}{2}N \le n \le \frac{3}{2}N \text{ is a prime num-} \\ \text{ber}\end{array}\right], \end{aligned}$$

and prove that

$$\lim_{N\to\infty} \frac{P(N)}{1/\ln(N)} = 1.$$

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 $c_2 > c_1 > 0$. Bob chooses random numbers n in the interval $c_1N \le n \le c_2N$. Keeping c_1 and c_2 fixed, let

$$P(c_1, c_2; N) = \left[\begin{array}{l}\text{Probability that an integer } n \text{ in the in-} \\ \text{terval } c_1N \le n \le c_2N \text{ is a prime num-} \\ \text{ber}\end{array}\right].$$

In the following formula, fill in the box with a simple function of N so that the statement is true:

$$\lim_{N\to\infty} \frac{P(c_1, c_2; N)}{\boxed{}} = 1.$$

<u>*Solution to Exercise* 3.19</u>.

We will just write $P(N)$, instead of $P(c_1, c_2; N)$.

$$\begin{aligned} P(N) &= \frac{\#\text{ of primes between } c_1N \text{ and } c_2N}{(c_2 - c_1)N} \\ &= \frac{\pi(c_2N) - \pi(c_1N)}{(c_2 - c_1)N} \\ &= \frac{1}{c_2 - c_1}\left(\frac{c_2}{\ln(c_2N)} - \frac{c_1}{\ln(c_1N)}\right) + o\left(\frac{1}{\ln(N)}\right) \qquad \text{from the prime number theorem} \\ &= \frac{\ln(N) + O(1)}{\ln(c_1N)\ln(c_2N)} + o\left(\frac{1}{\ln(N)}\right) \\ &= \frac{1}{\ln(N)} + o\left(\frac{1}{\ln(N)}\right). \end{aligned}$$

Hence $P(N)$ divided by $1/\ln(N)$ goes to 1 as $N \to \infty$, or equivalently,

$$\lim_{N\to\infty} \frac{P(N)}{1/\ln(N)} = c_2 - c_1.$$

For part (a), we have $c_1 = \frac{1}{2}$ and $c_2 = \frac{3}{2}$, so the limit is 1.

3.20. 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 (3.37) correct? Why?

A randomly chosen number N satisfying $N \equiv k \pmod{m}$ has probability $\boxed{}/\ln(N)$ of being prime. (3.3)

(e) Same question, but for arbitrary m, not just for m that are products of distinct primes.

<u>Solution to Exercise</u> 3.20.

(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

$$\prod_{p\mid m} \left(\frac{p}{p-1}\right) \cdot \frac{1}{\ln(N)}.$$

This is often written as

$$\prod_{p\mid m} \left(1 - \frac{1}{p}\right)^{-1} \cdot \frac{1}{\ln(N)},$$

which is also equal to $N/(\phi(N)\ln(N))$, where $\phi(N)$ is Euler's phi function.

3.21. The *logarithmic integral function* $\mathrm{Li}(X)$ is defined to be

$$\mathrm{Li}(X) = \int_2^X \frac{dt}{\ln t}.$$

(a) Prove that

$$\mathrm{Li}(X) = \frac{X}{\ln X} + \int_2^X \frac{dt}{(\ln t)^2} + O(1).$$

(*Hint*. Integration by parts.)

(b) Compute the limit

$$\lim_{X\to\infty} \frac{\mathrm{Li}(X)}{X/\ln X}.$$

(*Hint*. Break the integral in (a) into two pieces, $2 \le t \le \sqrt{X}$ and $\sqrt{X} \le t \le X$, and estimate each piece separately.)

(c) Use (b) to show that formula (3.12) on page 135 implies the prime number theorem (Theorem 3.21).

Solution to Exercise 3.21.

A solution for this exercise is not currently available.

Section. Pollard's $p-1$ factorization algorithm

3.22. 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 3.22.

(a)

$$\begin{aligned}
2^{3!} - 1 &\equiv 63 \pmod{1739} & \gcd(2^{3!}-1, 1739) &= 1\\
2^{4!} - 1 &\equiv 1082 \pmod{1739} & \gcd(2^{4!}-1, 1739) &= 1\\
2^{5!} - 1 &\equiv 1394 \pmod{1739} & \gcd(2^{5!}-1, 1739) &= 1\\
2^{6!} - 1 &\equiv 1443 \pmod{1739} & \gcd(2^{6!}-1, 1739) &= 37
\end{aligned}$$

This give $1739 = 37\cdot 47$. Note that $p-1 = 36 = 2^2\cdot 3^2$ and $q-1 = 46 = 2\cdot 23$.

(b)

$$\begin{aligned}
2^{3!} - 1 &\equiv 63 \pmod{220459} & \gcd(2^{3!}-1, 220459) &= 1\\
2^{4!} - 1 &\equiv 22331 \pmod{220459} & \gcd(2^{4!}-1, 220459) &= 1\\
2^{5!} - 1 &\equiv 85053 \pmod{220459} & \gcd(2^{5!}-1, 220459) &= 1\\
2^{6!} - 1 &\equiv 4045 \pmod{220459} & \gcd(2^{6!}-1, 220459) &= 1\\
2^{7!} - 1 &\equiv 43102 \pmod{220459} & \gcd(2^{7!}-1, 220459) &= 1\\
2^{8!} - 1 &\equiv 179600 \pmod{220459} & \gcd(2^{8!}-1, 220459) &= 449
\end{aligned}$$

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)

$$\begin{array}{lll}
2^{15!} - 1 \equiv 46983890 & \pmod{48356747} & \gcd(2^{15!} - 1, 48356747) = 1 \\
2^{16!} - 1 \equiv 8398520 & \pmod{48356747} & \gcd(2^{16!} - 1, 48356747) = 1 \\
2^{17!} - 1 \equiv 9367159 & \pmod{48356747} & \gcd(2^{17!} - 1, 48356747) = 1 \\
2^{18!} - 1 \equiv 17907955 & \pmod{48356747} & \gcd(2^{18!} - 1, 48356747) = 1 \\
2^{19!} - 1 \equiv 13944672 & \pmod{48356747} & \gcd(2^{19!} - 1, 48356747) = 6917
\end{array}$$

This gives $48356747 = 6917 \cdot 6991$. Note that $p-1 = 6916 = 2^2 \cdot 7 \cdot 13 \cdot 19$ and $q - 1 = 6990 = 2 \cdot 3 \cdot 5 \cdot 233$.

3.23. A prime of the form $2^n - 1$ is called a *Mersenne prime*.
(a) Factor each of the numbers $2^n - 1$ for $n = 2, 3, \ldots, 10$. Which ones are Mersenne primes?
(b) Find the first seven Mersenne primes. (You may need a computer.)
(c) If n is even and $n > 2$, prove that $2^n - 1$ is not prime.
(d) If $3 \mid n$ and $n > 3$, prove that $2^n - 1$ is not prime.
(e) 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`.)
(g) Write a one page essay on Mersenne primes, starting with the discoveries of Father Mersenne and ending with GIMPS.

Solution to Exercise 3.23.
The factorization of $2^n - 1$ for $2 \le n \le 20$ is

$$\begin{array}{ll}
 & 2^{11} - 1 = 2047 = 23 \cdot 89 \\
2^2 - 1 = 3 = 3 & 2^{12} - 1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13 \\
2^3 - 1 = 7 = 7 & 2^{13} - 1 = 8191 = 8191 \\
2^4 - 1 = 15 = 3 \cdot 5 & 2^{14} - 1 = 16383 = 3 \cdot 43 \cdot 127 \\
2^5 - 1 = 31 = 31 & 2^{15} - 1 = 32767 = 7 \cdot 31 \cdot 151 \\
2^6 - 1 = 63 = 3^2 \cdot 7 & 2^{16} - 1 = 65535 = 3 \cdot 5 \cdot 17 \cdot 257 \\
2^7 - 1 = 127 = 127 & 2^{17} - 1 = 131071 = 131071 \\
2^8 - 1 = 255 = 3 \cdot 5 \cdot 17 & 2^{18} - 1 = 262143 = 3^3 \cdot 7 \cdot 19 \cdot 73 \\
2^9 - 1 = 511 = 7 \cdot 73 & 2^{19} - 1 = 524287 = 524287 \\
2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31 & 2^{20} - 1 = 1048575 = 3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41
\end{array}$$

Thus the first few Mersenne primes are

$$\begin{array}{llll} 2^2-1=3, & 2^3-1=7, & 2^5-1=31, & 2^7-1=127, \\ 2^{13}-1=8191, & 2^{17}-1=131071, & 2^{19}-1=524287. & \end{array}$$

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.

$$\begin{aligned} 2^{23}-1 &= 8388607 = 47\cdot 178481 \\ 2^{29}-1 &= 536870911 = 233\cdot 1103\cdot 2089 \\ 2^{31}-1 &= 2147483647 = 2147483647 \\ 2^{37}-1 &= 137438953471 = 223\cdot 616318177 \\ 2^{41}-1 &= 2199023255551 = 13367\cdot 164511353 \\ 2^{43}-1 &= 8796093022207 = 431\cdot 9719\cdot 2099863 \\ 2^{47}-1 &= 140737488355327 = 2351\cdot 4513\cdot 13264529 \end{aligned}$$

(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

3.24. For each of the following numbers N, compute the values of

$$N+1^2,\quad N+2^2,\quad N+3^2,\quad N+4^2,\quad \ldots$$

as we did in Example 3.34 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 3.24.

(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.

$$\begin{array}{ll}
64213 + 1^2 = 64214 & \text{not a square} \\
64213 + 2^2 = 64217 & \text{not a square} \\
64213 + 3^2 = 64222 & \text{not a square} \\
64213 + 4^2 = 64229 & \text{not a square} \\
\vdots & \vdots \\
64213 + 121^2 = 78854 & \text{not a square} \\
64213 + 122^2 = 79097 & \text{not a square} \\
64213 + 123^2 = 79342 & \text{not a square} \\
64213 + 124^2 = 79589 & \text{not a square} \\
64213 + 125^2 = 79838 & \text{not a square} \\
64213 + 126^2 = 80089 = 283^2 & \text{** square **}
\end{array}$$

Thus

$$64213 = 283^2 - 126^2 = (283 + 126)(283 - 126) = 409 \cdot 157.$$

3.25. For each of the listed values of N, k, and b_{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 3.35.

(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 3.25.

(a)

$$\begin{array}{ll}
247 \cdot 143041 + 1^2 = 35331128 & \text{not a square} \\
247 \cdot 143041 + 2^2 = 35331131 & \text{not a square} \\
247 \cdot 143041 + 3^2 = 35331136 = 5944^2 & \text{** square **}
\end{array}$$

Thus

$$247 \cdot 143041 = 5944^2 - 3^2 = (5944 + 3)(5944 - 3) = 5947 \cdot 5941.$$

$$\gcd(143041, 5947) = 313, \qquad \gcd(143041, 5941) = 457$$

(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

$$3 \cdot 1226987 = 1919^2 - 40^2 = (1919 + 40)(1919 - 40) = 1959 \cdot 1879.$$

$$\gcd(1226987, 1959) = 653, \qquad \gcd(1226987, 1879) = 1879$$

(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

$$21 \cdot 2510839 = 7262^2 - 95^2 = (7262 + 95)(7262 - 95) = 7357 \cdot 7167.$$

$$\gcd(2510839, 7357) = 1051, \qquad \gcd(2510839, 7167) = 2389$$

3.26. 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 3.37 and 3.38.
(a) $N = 61063$

$$\begin{array}{rlcr}
1882^2 \equiv 270 & \pmod{61063} & \text{and} & 270 = 2 \cdot 3^3 \cdot 5 \\
1898^2 \equiv 60750 & \pmod{61063} & \text{and} & 60750 = 2 \cdot 3^5 \cdot 5^3
\end{array}$$

(b) $N = 52907$

$$\begin{array}{rlcr}
399^2 \equiv 480 & \pmod{52907} & \text{and} & 480 = 2^5 \cdot 3 \cdot 5 \\
763^2 \equiv 192 & \pmod{52907} & \text{and} & 192 = 2^6 \cdot 3 \\
773^2 \equiv 15552 & \pmod{52907} & \text{and} & 15552 = 2^6 \cdot 3^5 \\
976^2 \equiv 250 & \pmod{52907} & \text{and} & 250 = 2 \cdot 5^3
\end{array}$$

(c) $N = 198103$

$$\begin{array}{llcl}
1189^2 \equiv 27000 & \pmod{198103} & \text{and} & 27000 = 2^3 \cdot 3^3 \cdot 5^3 \\
1605^2 \equiv 686 & \pmod{198103} & \text{and} & 686 = 2 \cdot 7^3 \\
2378^2 \equiv 108000 & \pmod{198103} & \text{and} & 108000 = 2^5 \cdot 3^3 \cdot 5^3 \\
2815^2 \equiv 105 & \pmod{198103} & \text{and} & 105 = 3 \cdot 5 \cdot 7
\end{array}$$

(d) $N = 2525891$

$$\begin{array}{llcl}
1591^2 \equiv 5390 & \pmod{2525891} & \text{and} & 5390 = 2 \cdot 5 \cdot 7^2 \cdot 11 \\
3182^2 \equiv 21560 & \pmod{2525891} & \text{and} & 21560 = 2^3 \cdot 5 \cdot 7^2 \cdot 11 \\
4773^2 \equiv 48510 & \pmod{2525891} & \text{and} & 48510 = 2 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11 \\
5275^2 \equiv 40824 & \pmod{2525891} & \text{and} & 40824 = 2^3 \cdot 3^6 \cdot 7 \\
5401^2 \equiv 1386000 & \pmod{2525891} & \text{and} & 1386000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11
\end{array}$$

Solution to Exercise 3.26.

(a)

$$\begin{aligned}
1882^2 \cdot 1898^2 &\equiv (2 \cdot 3^3 \cdot 5)(2 \cdot 3^5 \cdot 5^3) \pmod{61063} \\
&= (2 \cdot 3^4 \cdot 5^2)^2 \\
&= 4050^2
\end{aligned}$$

$$\gcd(61063, 1882 \cdot 1898 - 4050) = 227 \qquad \text{Eureka!}$$

(b) The most natural combination to try first is

$$\begin{aligned}
763^2 \cdot 773^2 &\equiv (2^6 \cdot 3)(2^6 \cdot 3^5) \pmod{52907} \\
&= (2^6 \cdot 3^3)^2 \\
&= 1728^2
\end{aligned}$$

$$\gcd(52907, 763 \cdot 773 - 1728) = 277 \qquad \text{Eureka!}$$

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

$$\gcd(52907, 399 \cdot 763 \cdot 976 - 4800) = 52907 \qquad \text{No help}$$

(c) First we try

$$\begin{aligned} 1189^2 \cdot 2378^2 &\equiv (2^3 \cdot 3^3 \cdot 5^3)(2^5 \cdot 3^3 \cdot 5^3) \pmod{198103} \\ &= (2^4 \cdot 3^3 \cdot 5^3)^2 \\ &= 54000^2 \end{aligned}$$

$$\gcd(198103, 1189 \cdot 2378 - 54000) = 198103 \qquad \text{No help}$$

This didn't work, so next we try

$$\begin{aligned} 1189^2 \cdot 1605^2 \cdot 2815^2 &\equiv (2^3 \cdot 3^3 \cdot 5^3)(2 \cdot 7^3)(3 \cdot 5 \cdot 7) \pmod{198103} \\ &= (2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2)^2 \\ &= 44100^2 \end{aligned}$$

$$\gcd(198103, 1189 \cdot 1605 \cdot 2815 - 44100) = 499 \qquad \text{Eureka!}$$

(d) First we try

$$\begin{aligned} 1591^2 \cdot 3182^2 &\equiv (2 \cdot 5 \cdot 7^2 \cdot 11)(2^3 \cdot 5 \cdot 7^2 \cdot 11) \pmod{2525891} \\ &= (2^2 \cdot 5 \cdot 7^2 \cdot 11)^2 \\ &= 10780^2 \end{aligned}$$

$$\gcd(2525891, 1591 \cdot 3182 - 10780) = 2525891 \qquad \text{No help}$$

Next we try

$$\begin{aligned} 1591^2 \cdot 4773^2 &\equiv (2 \cdot 5 \cdot 7^2 \cdot 11)(2 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11) \pmod{2525891} \\ &= (2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11)^2 \\ &= 16170^2 \end{aligned}$$

$$\gcd(2525891, 1591 \cdot 4773 - 16170) = 2525891 \qquad \text{No help}$$

Finally we win when we try

$$\begin{aligned} &1591^2 \cdot 5275^2 \cdot 5401^2 \\ &\qquad \equiv (2 \cdot 5 \cdot 7^2 \cdot 11)(2^3 \cdot 3^6 \cdot 7)(2^4 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11) \pmod{2525891} \\ &\qquad = (2^4 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11)^2 \\ &\qquad = 17463600^2 \end{aligned}$$

$$\gcd(2525891, 1591 \cdot 5275 \cdot 5401 - 17463600) = 1637 \qquad \text{Eureka!}$$

Section. Smooth numbers, sieves, and building relations for factorization

3.27. Compute the following values of $\psi(X, B)$, the number of B-smooth numbers between 2 and X (see page 150).

(a) $\psi(25, 3)$ (b) $\psi(35, 5)$ (c) $\psi(50, 7)$ (d) $\psi(100, 5)$
(e) $\psi(100, 7)$

Solution to Exercise 3.27.
(a) $\psi(25, 3) = 10$
(b) $\psi(35, 5) = 18$
(c) $\psi(50, 7) = 30$
(d) $\psi(100, 5) = 33$
(e) $\psi(100, 7) = 45$

3.28. An integer M is called *B-power-smooth* if every prime power p^e dividing M satisfies $p^e \le B$. 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 $[1, 2, \ldots, B]$. (The *least common multiple* of a list of numbers $k_1, \ldots, k_r$ is the smallest number K that is divisible by every number in the list.)

Solution to Exercise 3.28.
(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 $378 = 2 \cdot 3^3 \cdot 7$.

3.29. 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 3.29.
(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.

3.30. 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 α, no matter how large, $L(X) = \Omega\big((\ln X)^\alpha\big)$.
(b) For every positive constant β, no matter how small, $L(X) = \mathcal{O}\big(X^\beta\big)$.

Solution to Exercise 3.30.

(a) We want to show that $L(X) \ge (\ln X)^\alpha$ when X is large. Since the logarithm function is an increasing function, it suffices to show that $\ln L(X) \ge \ln\big((\ln X)^\alpha\big)$. Using laws of logarithms, this is equivalent to showing that

$$\sqrt{(\ln X)(\ln\ln X)} \ge \alpha \ln(\ln X).$$

Dividing by $\ln(\ln X)$, this is equivalent to showing that

$$\sqrt{\frac{\ln X}{\ln\ln X}} \ge \alpha$$

when X is large. But it is clear that

$$\lim_{X\to\infty} \frac{\ln X}{\ln\ln X} = \infty,$$

which gives us the desired result. If it's not clear to you that the limit is ∞, use L'Hopital's rule to compute

$$\lim_{X\to\infty} \frac{\ln X}{\ln\ln X} = \lim_{X\to\infty} \frac{1/X}{1/(X\ln X)} = \lim_{X\to\infty} \ln X = \infty.$$

(b) Similarly, taking logs, we need to show that

$$\ln L(X) = \sqrt{(\ln X)(\ln\ln X)} \quad \text{is smaller than} \quad \ln(X^\beta) = \beta \ln X.$$

Dividing both sides by $\ln X$, this means showing that

$$\sqrt{\frac{\ln\ln X}{\ln X}} \le \beta$$

when X is large. This is true, since (using the calculation in (a)) we have

$$\lim_{X\to\infty} \frac{\ln\ln X}{\ln X} = 0.$$

3.31. 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 $F_{a,b}(X) = \Omega(X^\alpha)$ for every $\alpha > 0$. Thus $F_{a,b}(X)$ grows faster than every exponential function, so one says that $F_{a,b}(X)$ has *superexponential growth*.
(c) What happens if $a < 1$?

Solution to Exercise 3.31.
A solution for this exercise is not currently available.

3.32. This exercise asks you to verify an assertion in the proof of Corollary 3.45. 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

$$(\ln X)^\epsilon < \ln L(X) < (\ln X)^{1-\epsilon} \qquad \text{for all } X > 10.$$

(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 3.32.
(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

$$\begin{aligned} u\ln u &= \frac{1}{c}\sqrt{\frac{\ln X}{\ln\ln X}}\ln\left(\frac{1}{c}\sqrt{\frac{\ln X}{\ln\ln X}}\right) \\ &= \frac{1}{c}\sqrt{\frac{\ln X}{\ln\ln X}}\left[\frac{1}{2}\ln\ln X - \frac{1}{2}\ln\ln\ln X - \ln c\right] \\ &= \frac{1}{2c}\sqrt{\ln X\ln\ln X}\bigl(1+o(1)\bigr) \\ &= \frac{1}{2c}\bigl(\ln L(X)\bigr)\bigl(1+o(1)\bigr). \end{aligned}$$

Hence

$$u^u = L(X)^{\frac{1}{2c}(1+o(1))}.$$

3.33. Proposition 3.48 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

$$a = \lfloor \sqrt{N} \rfloor + k \qquad \text{for } 1 \le k \le K.$$

(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 $a^2 - N \le 2K\sqrt{N} + K^2$, 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

$$\lim_{N\to\infty} \frac{\log L(\sqrt{N}\,)}{\log L(N)^{1/\sqrt{2}}} = 1.$$

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 3.48 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?

<u>*Solution to Exercise* 3.33</u>.

(a) We have $a = \sqrt{N} + \epsilon + k$ for some $0 \le \epsilon < 1$. Hence $a^2 - N = 2(\epsilon + k)\sqrt{N} + (\epsilon + k)^2 \le 2K\sqrt{N} + K^2$.

(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 $N \to \infty$.

(c) We mimic the proof of Proposition 3.48. 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

$$\frac{\pi(B)}{\psi(\sqrt{N},B)/\sqrt{N}} \quad \text{numbers.} \tag{3.4}$$

We set $B = L(\sqrt{N})^c$, substitute into **??**, and use Theorem **??** and the prime number theorem (Theorem 3.21) 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 $O(L(N))$.

3.34. Illustrate the quadratic sieve, as was done in Figure 3.3 (page 161), by sieving prime powers up to B on the values of $F(T) = T^2 - N$ in the indicated range.

(a) 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.

(b) 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?

<u>Solution to Exercise</u> 3.34.

(a) 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

$$F(23) \equiv 36 \equiv 2^2{\cdot}3^2 \pmod{493} \qquad \text{and} \qquad F(25) \equiv 132 \equiv 2^2{\cdot}3{\cdot}11 \pmod{493}.$$

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

$$F(31) = 468 \equiv 2^2{\cdot}3^2{\cdot}13 \pmod{493} \qquad \text{and} \qquad F(47) = 1716 \equiv 2^2{\cdot}3{\cdot}11{\cdot}13 \pmod{493}.$$

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.

3.35. Let $\mathbb{Z}[\beta]$ be the ring described in Example 3.55, i.e., β 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 β up to β^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) $u = 6 - 5\beta + 3\beta^2 + 3\beta^3$ and $v = -2 + 7\beta + 6\beta^2$.

Solution to Exercise 3.35.

(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

3.36. This exercise asks you to use the index calculus to solve a discrete logarithm problem. Let $p = 19079$ and $g = 17$.

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 $N = 493$

(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 $19 \cdot 17^{-12400} \pmod{p}$ 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 3.36.

(a) We have

$$g^{3030} \equiv 2^2 \cdot 3^6 \cdot 5, \qquad g^{6892} \equiv 2^{11} \cdot 3^2, \qquad g^{18312} \equiv 2^4 \cdot 3 \cdot 5^3.$$

(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

$$19 \cdot g^{-12400} \equiv 2^7 \cdot 3 \pmod{19079}.$$

(d) Hence

$$\log_g(19) = 12400+7\cdot\log_g(2)+\log_g(3) = 12400+7\cdot 8195+1299 \equiv 13830 \pmod{p-1}.$$

We check that $17^{13830} \equiv 19 \pmod{19079}$. ✓
Remark: Another exponent that works is

$$h \cdot g^{-12224} \equiv 2^{13} \pmod{19079}.$$

Section. Quadratic residues and quadratic reciprocity

3.37. 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 3.61, 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 3.62(a), that is, prove that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

<u>*Solution to Exercise* 3.37</u>.

A solution for this exercise is not currently available.

3.38. Prove that the three parts of the quadratic reciprocity theorem (Theorem 3.62) are equivalent to the following three concise formulas, where p and q are odd primes:

(a) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (b) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ (c) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

<u>*Solution to Exercise* 3.38</u>.

A solution for this exercise is not currently available.

3.39. 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 3.37.) 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 3.39.

This was proven in Chapter 2, see Proposition 2.26, 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 $3502^2 \equiv -9109 \pmod{10663}$.

3.40. Let p be an odd prime, let $g \in \mathbb{F}_p^*$ be a primitive root, and let $h \in \mathbb{F}_p^*$. Write $p - 1 = 2^s m$ with m odd and $s \geq 1$, and write the binary expansion of $\log_g(h)$ as

$$\log_g(h) = \epsilon_0 + 2\epsilon_2 + 4\epsilon_2 + 8\epsilon_3 + \cdots \quad \text{with} \quad \epsilon_0, \epsilon_1, \ldots \in \{0, 1\}.$$

Give an algorithm that generalizes Example 3.69 and allows you to rapidly compute $\epsilon_0, \epsilon_1, \ldots, \epsilon_{s-1}$, thereby proving that the first s bits of the discrete logarithm are insecure. You may assume that you have a fast algorithm to compute square roots in $\mathbb{F}_p^*$, as provided for example by Exercise 3.39(a) if $p \equiv 3 \pmod{4}$. (*Hint.* Use Example 3.69 to compute the 0^{th} bit, take the square root of either h or $g^{-1}h$, and repeat.)

Solution to Exercise 3.40.

A solution for this exercise is not currently available.

3.41. Let p be a prime satisfying $p \equiv 1 \pmod 3$. We say that a is a *cubic residue modulo* p if $p \nmid a$ and there is an integer c satisfying $a \equiv c^3 \pmod p$.

(a) Let a and b be cubic residues modulo p. Prove that ab is a cubic residue modulo p.

(b) 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.

(c) 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 to the base g.

(d) Suppose instead that $p \equiv 2 \pmod 3$. Prove that for every integer a there is an integer c satisfying $a \equiv c^3 \pmod p$. In other words, if $p \equiv 2 \pmod 3$, show that every number is a cube modulo p.

Solution to Exercise 3.41.

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

$$a \equiv c^3 \mod p \qquad \text{and} \qquad b \equiv d^3 \pmod p.$$

Then $ab = (cd)^3 \pmod p$, so ab is also a cubic residue modulo p.

(b,c,d) *A solution for this exercise is not currently available.*

Section. Probabilistic encryption and the Goldwasser–Micali cryptosystem

3.42. Perform the following encryptions and decryptions using the Goldwasser–Micali public key cryptosystem (Table 3.9).

(a) 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 3.42.

(a) Decrypt $c = 1794677960$ by computing $\bigl(\frac{1794677960}{32411}\bigr) = -1$, which gives the plaintext bit $m = 1$. Decrypt $c = 525734818$ by computing $\bigl(\frac{525734818}{32411}\bigr) = 1$, which gives the plaintext bit $m = 0$. Decrypt $c = 420526487$ by computing $\bigl(\frac{420526487}{32411}\bigr) = -1$, 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 $\bigl(\frac{2322}{47}\bigr) = -1$, which gives the plaintext bit $m = 1$. Decrypt $c = 719$ by computing $\bigl(\frac{719}{47}\bigr) = 1$, which gives the plaintext bit $m = 0$. Decrypt $c = 202$ by computing $\bigl(\frac{202}{47}\bigr) = 1$, 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 $(517254876, 4308279, 660699010)$.

3.43. 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 $m = r \| (r \oplus m')$, where $\|$ denotes concatenation[1] 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.

(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 μ, what is the message expansion ratio of the new probabilistic cryptosystem?

[1] The *concatenation* of two bit strings is formed by placing the first string before the second string. For example, 1101 $\|$ 1001 is the bit string 11011001.

Solution to Exercise 3.43.

(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 μ, 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

Digital Signatures

Exercises for Chapter 4

Section. RSA digital signatures

4.1. Samantha uses the RSA signature scheme with primes $p = 541$ and $q = 1223$ and public verification exponent $e = 159853$.
(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 4.1.
(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

$$ed \equiv 1 \pmod{(p-1)(q-1)}, \qquad 159853 \cdot d \equiv 1 \pmod{659880},$$

for the private signing key $d = 561517$.
(b) Samantha takes the document $D = 630579$ and computes

$$S = D^d \pmod{N}, \qquad 630579^{561517} \equiv 206484 \pmod{661643}.$$

So the signature is $S = 206484$.

She can check that this is correct by computing

$$C \equiv S^e \pmod{N}, \qquad C \equiv 206484^{159853} \equiv 630579 \pmod{661643}$$

and noting that this value agrees with $D = 630579$.

4.2. Samantha uses the RSA signature scheme with public modulus $N = 1562501$ and public verification exponent $e = 87953$. 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 4.2.

Victor uses Samantha's public key $(N, e) = (1562501, 87953)$ to compute:

$$\begin{aligned}
C &\equiv S^e \pmod{N}, & C &\equiv 876453^{87953} \equiv 772481 \pmod{1562501},\\
C' &\equiv S'^e \pmod{N}, & C' &\equiv 870099^{87953} \equiv 161153 \pmod{1562501},\\
C'' &\equiv S''^e \pmod{N}, & C'' &\equiv 602754^{87953} \equiv 586036 \pmod{1562501}.
\end{aligned}$$

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 $d = 261617$.

4.3. Samantha uses the RSA signature scheme with public modulus and public verification exponent

$$N = 27212325191 \quad \text{and} \quad e = 22824469379.$$

Use whatever method you want to factor N, and then forge Samantha's signature on the document $D = 12910258780$.

Solution to Exercise 4.3.

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

$$ed \equiv 1 \pmod{(p-1)(q-1)}, \qquad 22824469379 \cdot d \equiv 1 \pmod{27211984800}$$

for Samantha's private signing exponent $d = 18408628619$. We can then sign the document $D = 12910258780$ by computing

$$S \equiv D^d \pmod{N},$$
$$12910258780^{18408628619} \equiv 22054770669 \pmod{27212325191}.$$

To check that this signature is correct, we compute

$$\begin{aligned}
&C \equiv S^e \pmod{N},\\
&C \equiv 22054770669^{22824469379} \equiv 12910258780 \pmod{27212325191}
\end{aligned}$$

and note that it agrees with $D = 12910258780$.

4.4. Suppose that Alice and Bob communicate using the RSA PKC. This means that Alice has a public modulus $N_A = p_A q_A$, a public encryption exponent e_A, and a private decryption exponent d_A, where p_A and q_A are primes and e_A and d_A satisfy

$$e_A d_A \equiv 1 \pmod{(p_A - 1)(q_A - 1)}.$$

Similarly, Bob has a public modulus $N_B = p_B q_B$, a public encryption exponent e_B, and a private decryption exponent d_B.

In this situation, Alice can simultaneously encrypt and sign a message in the following way. Alice chooses her plaintext m and computes the usual RSA ciphertext

$$c \equiv m^{e_B} \pmod{N_B}.$$

She next applies a hash function to to her plaintext and uses her private decryption key to compute

$$s \equiv \mathsf{Hash}(m)^{d_A} \pmod{N_A}.$$

She sends the pair (c, s) to Bob.

Bob first decrypts the ciphertext using his private decryption exponent d_B,

$$m \equiv c^{d_B} \pmod{N_B}.$$

He then uses Alice's public encryption exponent e_A to verify that

$$\mathsf{Hash}(m) \equiv s^{e_A} \pmod{N_A}.$$

Explain why verification works, and why it would be difficult for anyone other than Alice to send Bob a validly signed message.

Solution to Exercise 4.4.

A solution for this exercise is not currently available.

Section. Discrete logarithm digital signatures

4.5. Samantha uses the Elgamal signature scheme with prime $p = 6961$ and primitive root $g = 437$.

(a) Samantha's private signing key is $a = 6104$. What is her public verification key?

(b) Samantha signs the digital document $D = 5584$ using the random element $k = 4451$. What is the signature?

Solution to Exercise 4.5.

(a)

$$A \equiv 437^{6104} \equiv 2065 \pmod{6961}.$$

(b)

$$S_1 \equiv 437^{4451} \equiv 3534 \pmod{6961},$$
$$S_2 \equiv (5584 - 6104 \cdot 3534)4451^{-1} \equiv 5888 \pmod{6960}.$$

So the signature on D is $(3534, 5888)$.

4.6. Samantha uses the Elgamal signature scheme with prime $p = 6961$ and primitive root $g = 437$. Her public verification key is $A = 4250$. 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 4.6.

(a)

$$\begin{aligned} A^{S_1} \cdot S_1^{S_2} &\equiv (4250^{4129}) \cdot 4129^{5575} \equiv 231 \pmod{6961}. \\ g^D &\equiv 437^{1521} \equiv 231 \pmod{6961}. \end{aligned}$$

So the signature is valid. (The random element was $k = 5627$.)

(b)

$$\begin{aligned} A^{S_1} \cdot S_1^{S_2} &\equiv (4250^{3145}) \cdot 3145^{1871} \equiv 6208 \pmod{6961}. \\ g^D &\equiv 437^{1837} \equiv 2081 \pmod{6961}. \end{aligned}$$

So the signature is *not* valid.

(c)

$$\begin{aligned} A^{S_1} \cdot S_1^{S_2} &\equiv (4250^{2709}) \cdot 2709^{2994} \equiv 2243 \pmod{6961}. \\ g^D &\equiv 437^{1614} \equiv 2243 \pmod{6961}. \end{aligned}$$

So the signature is valid. (The random element was $k = 3997$.)

(Samantha's private signing key is $a = 4804$.)

4.7. Let p be a prime, let i and j be integers with $\gcd(j, p-1) = 1$, and let A be arbitrary. Set

$$S_1 \equiv g^i A^j \pmod{p}, \quad S_2 \equiv -S_1 j^{-1} \pmod{p-1}, \quad D \equiv -S_1 i j^{-1} \pmod{p-1}.$$

Prove that (S_1, S_2) is a valid Elgamal signature on the document D for the verification key A. Thus Eve can produce signatures on random documents.

Solution to Exercise 4.7.

We compute

$$\begin{aligned} A^{S_1} S_1^{S_2} &\equiv A^{S_1} (g^i A^j)^{-S_1 j^{-1}} \pmod{p} \\ &\equiv A^{S_1} g^{-ij^{-1} S_1} A^{-S_1} \pmod{p} \\ &\equiv g^D \pmod{p}. \end{aligned}$$

4.8. Suppose that Samantha is using the Elgamal signature scheme and that she is careless and uses the same random element k to sign two documents D and D'.

(a) Explain how Eve can tell at a glance whether Samantha has made this mistake.

(b) 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 a, Samantha's private signing key.

(c) Apply your method from (b) to the following example and recover Samantha's signing key a, where Samantha is using the prime $p = 348149$, base $g = 113459$, and verification key $A = 185149$.

$$\begin{aligned} D &= 153405, & S_1 &= 208913, & S_2 &= 209176, \\ D' &= 127561, & S_1' &= 208913, & S_2' &= 217800. \end{aligned}$$

Solution to Exercise 4.8.

(a) Since $S_1 \equiv g^k$ and $S_1' = g^{k'}$, Eve can check if the two signatures used the same random element by checking if $S_1 = S_1'$.

(b) Using discrete logarithms to the base g, the verification conditions are

$$\begin{aligned} S_1 \log(A) + S_2 \log(S_1) &\equiv D \pmod{p-1}, \\ S_1' \log(A) + S_2' \log(S_1') &\equiv D' \pmod{p-1}. \end{aligned}$$

Since $S_1 = S_1'$ from (a), this becomes

$$\begin{aligned} S_1 a + S_2 \log(S_1) &\equiv D \pmod{p-1}, \\ S_1 a + S_2' \log(S_1) &\equiv D' \pmod{p-1}, \end{aligned}$$

where $a = \log_g(A)$ is Samantha's secret signing key. Taking S_2' times the first congruence and subtracting S_2 times the second congruence, we obtain

$$S_1(S_2' - S_2)a \equiv S_2'D - S_2D' \pmod{p-1}.$$

For notational convenience we write this congruence as

$$Ca \equiv B \pmod{p-1},$$

where we know the values of C and B. If $\gcd(C, p-1) = 1$, we can solve uniquely for a. In general, if $\gcd(C, p-1) > 1$ (it's unlikely to be too large), then there are $\gcd(C, p-1)$ solutions for a, and after computing them, we can decide which one is correct by checking which one yields $g^a \equiv A \pmod{p}$.

(c) From (b) we begin by computing

$$\begin{aligned} C &\equiv S_1(S_2' - S_2) \equiv 347960 \pmod{p-1}, \\ B &\equiv S_2'D - S_2D' \equiv 252868 \pmod{p-1}. \end{aligned}$$

We need to solve $Ca \equiv B \pmod{p-1}$, so we need to solve

$$347960a \equiv 252868 \pmod{348148}.$$

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

$$a \equiv 72729 \pmod{87037}.$$

Adding on multiples of $(p-1)/4 = 87037$ yields the four solutions

$$a \equiv 72729,\ 159766,\ 246803,\ 333840 \pmod{348148}$$

to the original congruence. We can pick out which solution is correct from the relation $g^a \equiv A \pmod{p}$, i.e., the correct value of a should satisfy

$$113459^a \equiv 185149 \pmod{348149}.$$

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

$$a = 72729.$$

4.9. Samantha uses DSA with public parameters $(p, q, g) = (22531, 751, 4488)$. She chooses the secret signing key $a = 674$.

(a) What is Samantha's public verification key?

(b) Samantha signs the document $D = 244$ using the random element $k = 574$. What is the signature?

Solution to Exercise 4.9.

(a) Samantha's public verification key is

$$A \equiv 4488^{674} \equiv 4940 \text{ (mod } 22531).$$

(b) The signature is

$$\begin{aligned} S_1 &= (4488^{574} \bmod 22531) \bmod 751 = 444, \\ S_2 &\equiv (244 + 674 \cdot 444)574^{-1} \equiv 56 \text{ (mod } 751). \end{aligned}$$

4.10. Samantha uses DSA with public parameters $(p, q, g) = (22531, 751, 4488)$. Her public verification key is $A = 22476$.

(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 4.10.

(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

$$g^{V_1} A^{V_2} \equiv 4488^{293} \cdot 22476^{252} \equiv 6191 \pmod{22531}$$

and verifies that $6191 \bmod 751 = 183$ is equal to S_1. So the signature is valid. (Samantha's secret signing key happens to be $a = 38$.)

(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

$$g^{V_1} A^{V_2} \equiv 4488^{709} \cdot 22476^{428} \equiv 3979 \pmod{22531}.$$

Then he observes that

$$(g^{V_1} A^{V_2} \bmod p) \bmod q = 3979 \bmod 751 = 224$$

is not equal to $S_1 = 211$. So the signature is not valid.

4.11. Samantha's DSA public parameters are $(p, q, g) = (103687, 1571, 21947)$, and her public verification key is $A = 31377$. 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 random element $k = 1105$.

Solution to Exercise 4.11.

Solving $31377 \equiv 21947^a \pmod{103687}$ gives $a = 602$. Then the signature on $D = 510$ using the random element $k = 1105$ is

$$\begin{aligned} S_1 &= (21947^{1105} \bmod 103687) \bmod 1571 = 439 \\ S_2 &\equiv (510 + 602 \cdot 439)1105^{-1} \equiv 1259 \pmod{1571}. \end{aligned}$$

Chapter 5

Combinatorics, Probability, and Information Theory

Exercises for Chapter 5

Section. Basic principles of counting

5.1. 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[1]; each spelt seed would have produced seven hekat[2] of spelt. What is the sum of all of the named items? Solve this 3500 year old problem.

Solution to Exercise 5.1.

$$\underbrace{7}_{\text{houses}} + \underbrace{7^2}_{\text{cats}} + \underbrace{7^3}_{\text{mice}} + \underbrace{7^4}_{\text{spelt}} + \underbrace{7^5}_{\text{hekat}} = 19607.$$

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

[1] *Spelt* is an ancient type of wheat.

[2] 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.

5.2. (a) How many n-tuples $(x_1, x_2, \dots, x_n)$ are there if the coordinates are required to be integers satisfying $0 \le x_i < q$?

(b) Same question as (a), except now there are separate bounds $0 \le x_i < q_i$ for each coordinate.

(c) How many n-by-n matrices are there if the entries $x_{i,j}$ of the matrix are integers satisfying $0 \le x_{i,j} < q$?

(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 5.2.

(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

$$307200 = \underbrace{12}_{\text{students}} \cdot \underbrace{4}_{\text{classes}} \cdot \underbrace{2}_{\text{notebooks}} \cdot \underbrace{100}_{\text{sheets}} \cdot \underbrace{32}_{\text{lines}}.$$

5.3. (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 $\{1, 2, \ldots, 20\}$?

(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 5.3.

(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) (1,2,4,3) (1,3,2,4) (1,3,4,2) (1,4,2,3) (1,4,3,2)
(2,1,3,4) (2,1,4,3) (2,3,1,4) (2,3,4,1) (2,4,1,3) (2,4,3,1)
(3,1,2,4) (3,1,4,2) (3,2,1,4) (3,2,4,1) (3,4,1,2) (3,4,2,1)
(4,1,2,3) (4,1,3,2) (4,2,1,3) (4,2,3,1) (4,3,1,2) (4,3,2,1)

(c) There are $20! = 2432902008176640000 \approx 2.43 \cdot 10^{18}$ permutations of $\{1, 2, \ldots, 20\}$.

(d) If the rooms are labeled $1, 2, \ldots, 7$, 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.

5.4. (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 5.4.

(a) Here are the 24 permutations.

$$\begin{array}{llll}
(A_1, A_2, B_1, B_2) & (A_1, A_2, B_2, B_1) & (A_2, A_1, B_1, B_2) & (A_2, A_1, B_2, B_1) \\
(A_1, B_1, A_2, B_2) & (A_1, B_2, A_2, B_1) & (A_2, B_1, A_1, B_2) & (A_2, B_2, A_1, B_1) \\
(A_1, B_1, B_2, A_2) & (A_1, B_2, B_1, A_2) & (A_2, B_1, B_2, A_1) & (A_2, B_2, B_1, A_1) \\
(B_1, B_2, A_2, A_1) & (B_1, B_2, A_1, A_2) & (B_2, B_1, A_1, A_2) & (B_2, B_1, A_2, A_1) \\
(B_1, A_1, A_2, B_2) & (B_1, A_2, A_1, B_2) & (B_2, A_1, A_2, B_1) & (B_2, A_2, A_1, B_1) \\
(B_1, A_1, B_2, A_2) & (B_1, A_2, B_2, A_1) & (B_2, A_1, B_1, A_2) & (B_2, A_2, B_1, A_1)
\end{array}$$

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

$$\{A,A,A,A,B\}, \qquad \{A,A,A,B,B\}, \qquad \text{and} \qquad \{A,A,B,B,B\}.$$

So there are

$$\binom{5}{4} + \binom{5}{3} + \binom{5}{2} = 25 \quad \text{different five letter words.}$$

5.5. (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 5.5.
(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

$$\frac{100\cdot 99\cdot 98}{3!}\cdot 5\cdot 5\cdot 5 = 20212500 \approx 10^{7.31}.$$

5.6. Use the binomial theorem (Theorem 5.10) to compute each of the following quantities.
(a) $(5z+2)^3$ (b) $(2a-3b)^4$ (c) $(x-2)^5$

Solution to Exercise 5.6.
(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) $(x-2)^5 = x^5 - 10x^4 + 40x^3 - 80x^2 + 80x - 32$.

5.7. 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 5.10) and compare the coefficients of x^jy^{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 5.7.
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:

$$\begin{aligned}\sum_{j=0}^{n}\binom{n}{j}x^jy^{n-j} &= (x+y)\sum_{j=0}^{n-1}\binom{n-1}{j}x^jy^{n-1-j}\\ &= \sum_{j=0}^{n-1}\binom{n-1}{j}x^{j+1}y^{n-1-j} + \sum_{j=0}^{n-1}\binom{n-1}{j}x^jy^{n-j}\\ &= \sum_{j=1}^{n}\binom{n-1}{j-1}x^jy^{n-j} + \sum_{j=0}^{n-1}\binom{n-1}{j}x^jy^{n-j}\\ &= x^n + \sum_{j=1}^{n-1}\left[\binom{n-1}{j-1} + \binom{n-1}{j}x^jy^{n-j}\right] + y^n.\end{aligned}$$

Comparing the coefficients of x^jy^{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 $n = 0, 1, 2, 3, \ldots$ in the form of a triangle called Pascal's triangle.

Proof #3: Let the n objects be $A_1, \cdots, A_n$. Treat the last one as special, so label them as $A_1, \ldots, A_{n-1}, B$. 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.

5.8. Let p be a prime number. This exercise sketches another proof of Fermat's little theorem (Theorem 1.24).

(a) If $1 \le j \le p-1$, prove that the binomial coefficient $\binom{p}{j}$ is divisible by p.

(b) Use (a) and the binomial theorem (Theorem 5.10) to prove that

$$(a+b)^p \equiv a^p + b^p \pmod{p} \qquad \text{for all } a, b \in \mathbb{Z}.$$

(c) Use (b) with $b = 1$ and induction on a to prove that $a^p \equiv a \pmod{p}$ for all $a \ge 0$.

(d) Use (c) to deduce that $a^{p-1} \equiv 1 \pmod{p}$ for all a with $\gcd(p, a) = 1$.

Solution to Exercise 5.8.

(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)

$$(a+b)^p = \sum_{j=0}^{p}\binom{p}{j}a^jb^{p-j} \equiv a^p + b^p \pmod{p},$$

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 $a^{-1} \bmod p$.

5.9. We know that there are $n!$ different permutations of the set $\{1, 2, \ldots, n\}$.

(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.)

<u>*Solution to Exercise* 5.9</u>.

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 $!n = R(n,0)$. See the solution to Exercise 1.5 for the derivation of the following formulas:

$$\begin{aligned}
!n &= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = \lfloor n!/e \rceil, \\
\mathbf{R}(n,k) &= \binom{n}{k} !(n-k) = \binom{n}{k} \left\lfloor \frac{(n-k)!}{e} \right\rceil, \\
\mathbf{S}(n,k) &= \sum_{j=k}^{n} \mathbf{R}(n,j) = n! - \sum_{j=0}^{k-1} \mathbf{R}(n,j).
\end{aligned}$$

(a) No letters fixed is $\mathbf{R}(n,0) =!n$. This is called the n^{th} *derangement number*. For $n = 10$ we get

$$\mathbf{R}(10,0) =!10 = \lfloor 10!/e \rceil = \lfloor 1334960.916 \rceil = 1334961.$$

For $n = 26$ we get

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

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

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

Hence

$$\begin{aligned}\mathbf{S}(10,1) &= 10! - \lfloor 10!/e \rceil = 2293839,\\ \mathbf{S}(26,1) &= 26! - \lfloor 26!/e \rceil = 254928823778135499762712175.\end{aligned}$$

(c) Exactly 1 letter fixed is

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

so

$$\begin{aligned}\mathbf{R}(10,1) &= 10\left\lfloor \frac{9!}{e} \right\rceil = 1334960,\\ \mathbf{R}(26,1) &= 26\left\lfloor \frac{25!}{e} \right\rceil = 148362637348470135821287824.\end{aligned}$$

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

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

Hence

$$\begin{aligned}\mathbf{S}(10,1) &= 10! - \lfloor 10!/e \rceil - 10 \cdot \lfloor 9!/e \rceil = 958879,\\ \mathbf{S}(26,1) &= 26! - \lfloor 26!/e \rceil - 26 \cdot \lfloor 25!/e \rceil = 106566186429665363941424351.\end{aligned}$$

Section. The Vigenère cipher

5.10. Encrypt each of the following Vigenère plaintexts using the given keyword and the Vigenère tableau (Table 5.1).

(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 5.10.

(a) Vigenère Keyword: hamlet

```
t o 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
```

5.11. Decrypt each of the following Vigenère ciphertexts using the given keyword and the Vigenère tableau (Table 5.1).

(a) Keyword: `condiment`
Ciphertext: `rsghz bmcxt dvfsq hnigq xrnbm`
`pdnsq smbtr ku`

(b) Keyword: `rabbithole`
Ciphertext: `khfeq ymsci etcsi gjvpw ffbsq`
`moapx zcsfx epsox yenpk daicx`
`cebsm ttptx zooeq laflg kipoc`
`zswqm taujw ghboh vrjtq hu`

<u>*Solution to Exercise* 5.11</u>.

(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.*)

5.12. Explain how a cipher wheel with rotating inner wheel (see Figure 1.1 on page 3) can be used in place of a Vigeǹere tableau (Table 5.1) 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 5.12.

A solution for this exercise is not currently available.

5.13. Let

$$\boldsymbol{s} = \text{“I am the very model of a modern major general.”}$$
$$\boldsymbol{t} = \text{“I have information vegetable, animal, and mineral.”}$$

(a) Make frequency tables for $\boldsymbol{s}$ and $\boldsymbol{t}$.
(b) Compute IndCo($\boldsymbol{s}$) and IndCo($\boldsymbol{t}$).
(c) Compute MutIndCo($\boldsymbol{s}, \boldsymbol{t}$).

Solution to Exercise 5.13.

Note: This solution is not correct, because it was computed using “vegatable” instead of “vegetable”!

(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
Freq $\boldsymbol{s}$	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 $\boldsymbol{t}$	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) $IC(\boldsymbol{s}) = 0.0424$ and $IC(\boldsymbol{t}) = 0.0544$.
(c) $MIC(\boldsymbol{s}, \boldsymbol{t}) = 0.0517$

5.14. 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 MutIndCo($\boldsymbol{s}_i, \boldsymbol{s}_j$) for $1 \le i < j \le 3$ and use these values to deduce which two strings were encrypted using the same shift.

$$\boldsymbol{s}_1 = \texttt{iwseesetftuonhdptbunnybioeatneghictdnsevi}$$
$$\boldsymbol{s}_2 = \texttt{qibfhroeqeickxmirbqlflgkrqkejbejpepldfjbk}$$
$$\boldsymbol{s}_3 = \texttt{iesnnciiheptevaireittuevmhooottrtaaflnatg}$$

Solution to Exercise 5.14.

(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
Freq $\boldsymbol{s}_1$	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 $\boldsymbol{s}_2$	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 $\boldsymbol{s}_3$	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

$$\begin{aligned}
\text{MutIndCo}(\boldsymbol{s}_1, \boldsymbol{s}_2) &= 0.0375,\\
\text{MutIndCo}(\boldsymbol{s}_1, \boldsymbol{s}_3) &= 0.0744,\\
\text{MutIndCo}(\boldsymbol{s}_2, \boldsymbol{s}_3) &= 0.0369.
\end{aligned}$$

Thus $\boldsymbol{s}_1$ and $\boldsymbol{s}_3$ were probably encrypted using the same shift, so the first and third letters of the keyword are probably the same.

5.15. (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.

$$s_1 = \mathtt{RCZBWBFHSLPSCPILHBGZJTGBIBJGLYIJIBFHCQQFZBYFP},$$
$$s_2 = \mathtt{KHQWGIZMGKPOYRKHUITDUXLXCWZOTWPAHFOHMGFEVUEJJ}.$$

(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.

$$\begin{aligned} s_1 &= \mathtt{NTDCFVDHCTHKGUNGKEPGXKEWNECKEGWEWETWKUEVHDKK} \\ & \mathtt{CDGCWXKDEEAMNHGNDIWUVWSSCTUNIGDSWKE} \\ s_2 &= \mathtt{IGWSKGEHEXNGECKVWNKVWNKSUTEHTWHEKDNCDXWSIEKD} \\ & \mathtt{AECKFGNDCPUCKDNCUVWEMGEKWGEUTDGTWHD} \end{aligned}$$

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 5.15.

(a) The Indices of Coincidence of the two strings are $\mathrm{IndCo}(s_1) = 0.0576$ and $\mathrm{IndCo}(s_2) = 0.0303$, 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, $\mathrm{IndCo}(s_1) = \mathrm{IndCo}(s_2) = 0.0672$. In general, let $A = \{a_1, a_2, \ldots, a_k\}$ be a set of distinct objects (letters, bigrams, turtles, etc.) and let $B = (b_1, b_2, \ldots, b_n)$ be a list of elements from A, where the b_i do not need to be distinct. For each $1 \le i \le k$, 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

$$\mathrm{IndCo}(B) = \frac{1}{n(n-1)} \sum_{i=1}^{k} F_i(F_i - 1).$$

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

$$\mathrm{IndCo}(\text{Bigrams in } s_1) = 0.004,$$
$$\mathrm{IndCo}(\text{Bigrams in } s_2) = 0.010.$$

```
nhqrk  vvvfe  fwgjo  mzjgc  kocgk  lejrj  wossy  wgvkk  hnesg  kwebi
bkkcj  vqazx  wnvll  zetjc  zwgqz  zwhah  kwdxj  fgnyw  gdfgh  bitig
mrkwn  nsuhy  iecru  ljjvs  qlvvw  zzxyv  woenx  ujgyr  kqbfj  lvjzx
dxjfg  nywus  rwoar  xhvvx  ssmja  vkrwt  uhktm  malcz  ygrsz  xwnvl
lzavs  hyigh  rvwpn  ljazl  nispv  jahym  ntewj  jvrzg  qvzcr  estul
fkwis  tfylk  ysnir  rddpb  svsux  zjgqk  xouhs  zzrjj  kyiwc  zckov
qyhdv  rhhny  wqhyi  rjdqm  iwutf  nkzgd  vvibg  oenwb  kolca  mskle
cuwwz  rgusl  zgfhy  etfre  ijjvy  ghfau  wvwtn  xlljv  vywyj  apgzw
trggr  dxfgs  ceyts  tiiih  vjjvt  tcxfj  hciiv  voaro  lrxij  vjnok
mvrgw  kmirt  twfer  oimsb  qgrgc
```

Table 5.1: A Vigenère ciphertext for Exercise 5.16

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).

5.16. Table 5.13 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 5.16.

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 $\boxed{17}$. The keyword used for encryption was

$$\boxed{\texttt{fourscoreandseven}}.$$

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

```
togmg gbymk kcqiv dmlxk kbyif vcuek cuuis vvxqs pwwej koqgg
phumt whlsf yovww knhhm rcqfq vvhkw psued ugrsf ctwij khvfa
thkef fwptj ggviv cgdra pgwvm osqxg hkdvt whuev kcwyj psgsn
gfwsl jsfse ooqhw tofsh aciin gfbif gabgj adwsy topml ecqzw
asgvs fwrqs fsfvq rhdrs nmvmk cbhrv kblxk gzi
```

Table 5.2: A Vigenère ciphertext for Exercise 5.17

> 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, 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.

5.17. We applied a Kasiski test to the Vigenère ciphertext listed in Table 5.14 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 5.15. (This is the same type of table as Table 5.5 in the text, except that we haven't underlined the large values.) Use Table 5.15 to guess the relative rotations of the blocks, as we did in Table 5.6. This will give you a rotated version of the keyword. Try rotating it, as we did in Table 5.7, to find the correct keyword and decrypt the text.

Solution to Exercise 5.17.

The table of likely shift relations gives

$$\beta_2 = \beta_1 + 12, \quad \beta_3 = \beta_1 + 1, \quad \beta_4 = \beta_1 + 2, \quad \beta_5 = \beta_1 + 16.$$

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

5.18. Table 5.16 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.

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 5.3: Mutual indices of coincidence for Exercise 5.17

(a) Make a list of matching trigrams as we did in Table 5.3. Use the Kasiski test on matching trigrams to find the likely key length.

(b) Make a table of indices of coincidence for various key lengths, as we did in Table 5.4. Use your results to guess the probable key length.

(c) 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 5.5. Pick the largest indices from your table and use them to guess the relative rotations of the blocks, as we did in Table 5.6.

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 5.4: Large indices of coincidence and shift relations

Shift	Keyword	Decrypted Text
0	AMBCQ	tcfkqgpxkukqpgfdakvukpxgpvqtcucitgcvjwocpk
1	BNCDR	sbejpfowjtjpofeczjutjowfoupsbtbhsfbuivnboj
2	CODES	radioenvisionedbyitsinventorasagreathumani
3	DPEFT	qzchndmuhrhnmdcaxhsrhmudmsnqzrzfqdzsgtlzmh
4	EQFGU	pybgmcltgqgmlcbzwgrqgltclrmpyqyepcyrfskylg
5	FRGHV	oxaflbksfpflkbayvfqpfksbkqloxpxdobxqerjxkf
6	GSHIW	nwzekajreoekjazxuepoejrajpknwowcnawpdqiwje
7	HTIJX	mvydjziqdndjizywtdondiqziojmvnvbmzvocphvid
8	IUJKY	luxciyhpcmcihyxvscnmchpyhnilumualyunboguhc
⋮	⋮	⋮

Table 5.5: Decryption using shifts of the keyword AJCHWJZ

```
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 uwlrx psgiy ytpsf rjfuw
igxhr oyazd rakce dxeyr pdobr buehr uwcue ekfic zehrq ijezr
xsyor tcylf egcy
```

Table 5.6: A Vigenère ciphertext for Exercise 5.18

(d) Use your results from (c) to guess a rotated version of the keyword, and then try the different rotations as we did in Table 5.7 to find the correct keyword and decrypt the text.

Solution to Exercise 5.18.

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 to find β_7, we look at the mutual indices that involve Block 7 and are greater than 0.058. There are three of them:

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 5.7: Repeated trigrams in the ciphertext

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 5.8: 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	**.065**	.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	**.071**	.022	.026	.062	.033	.039
2	4	.038	.045	**.070**	.029	.034	.044	.035	.037	.042	.038	.030	.042	.037
2	5	.041	.038	.051	.032	.021	.028	.043	.025	.031	.049	.039	.031	.044
2	6	**.067**	.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	**.070**	.043	.030	.046	.038	.028	.030	.039	.029
1	3	.033	.051	.030	.047	.044	.032	.026	.055	.031	.016	.046	**.080**	.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	**.066**	.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	**.072**	.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	**.073**	.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	**.065**	.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	**.065**	.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 5.9: 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 5.10: Large indices of coincidence and shift relations

Shift	Keyword	Decrypted Text
0	AJCHWJZ	mxmwxsfiuyiwxmsrihalixlivmrxlialspipirkxle
1	BKDIXKA	lwlvwrehtxhvwlrqhgzkhwkhulqwkhzkrohohqjwkd
2	CLEJYLB	kvkuvqdgswguvkqpgfyjgvjgtkpvjgyjqngngpivjc
3	DMFKZMC	jujtupcfrvftujpofexifuifsjouifxipmfmfohuib
4	ENGLAND	itistobequestionedwhetherinthewholelengtha
5	FOHMBOE	hshrsnadptdrshnmdcvgdsgdqhmsgdvgnkdkdmfsgz
6	GPINCPF	grgqrmzcoscqrgmlcbufcrfcpglrfcufmjcjclerfy
7	HQJODQG	fqfpqlybnrbpqflkbatebqebofkqebtelibibkdqex
8	IRKPERH	epeopkxamqaopekjazsdapdanejpdasdkhahajcpdw
9	JSLQFSI	dodnojwzlpznodjizyrczoczmdioczrcjgzgzibocv
⋮	⋮	⋮

Table 5.11: Decryption using shifts of the keyword AJCHWJZ

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

5.19. 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:

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 [65], Vigenère invented the autokey cipher in 1586, but his invention was ignored and forgotten before being reinvented in the 1800s.

(a) Encrypt the following message using the autokey cipher:
    Keyword: `LEAR`
    Plaintext: `Come not between the dragon and his wrath.`

(b) Decrypt the following message using the autokey cipher:
    Keyword: `CORDELIA`
    Ciphertext: `pckkm yowvz ejwzk knyzv vurux cstri tgac`

(c) Eve intercepts an autokey ciphertext and manages to steal the accompanying plaintext:

Plaintext	`ifmusicbethefoodofloveplayon`
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 known plaintext attacks.

(d) 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 5.19.
(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

5.20. Use the definition (5.15) 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

$$\begin{aligned}\Pr(E_1 \cup E_2 \cup E_3) = \Pr(E_1) + \Pr(E_2) + \Pr(E_3) - \Pr(E_1 \cap E_2) \\ - \Pr(E_1 \cap E_3) - \Pr(E_2 \cap E_3) + \Pr(E_1 \cap E_2 \cap E_3).\end{aligned}$$

The formulas in (b) and (d) and their generalization to n events are known as the *inclusion–exclusion principle.*

Solution to Exercise 5.20.

A solution for this exercise is not currently available.

5.21. We continue with the coin tossing scenario from Example 5.23, 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 5.21.

We label the events in the parts of this problem as $E_{(\mathrm{a})}$, $E_{(\mathrm{b})}$, $E_{(\mathrm{c},k)}$, etc.

(a) $\Pr(E_{(\mathrm{a})}) = \frac{1}{4}$.

(b) $\Pr(E_{(\mathrm{b})}) = 1 - \Pr(E^c_{(\mathrm{b})}) = 1 - \frac{1}{4} = \frac{3}{4}$.

(c) $\Pr(E_{(\mathrm{c})}) = \Pr(E_{(\mathrm{b})}) - \Pr(E_{(\mathrm{a})}) = \frac{1}{2}$.

(d)

$$\Pr(E_{(\mathrm{d},0)}) = \binom{10}{0} \cdot \frac{1}{2^{10}} = \frac{1}{1024} = \frac{1}{1024} \approx 0.0010$$

$$
\begin{aligned}
\Pr(E_{(\mathrm{d},1)}) &= \binom{10}{1}\cdot\frac{1}{2^{10}} = \frac{10}{1024} = \frac{5}{512} \approx 0.0098\\
\Pr(E_{(\mathrm{d},2)}) &= \binom{10}{2}\cdot\frac{1}{2^{10}} = \frac{45}{1024} = \frac{45}{1024} \approx 0.0439\\
\Pr(E_{(\mathrm{d},3)}) &= \binom{10}{3}\cdot\frac{1}{2^{10}} = \frac{120}{1024} = \frac{15}{128} \approx 0.1172\\
\Pr(E_{(\mathrm{d},4)}) &= \binom{10}{4}\cdot\frac{1}{2^{10}} = \frac{210}{1024} = \frac{105}{512} \approx 0.2051\\
\Pr(E_{(\mathrm{d},5)}) &= \binom{10}{5}\cdot\frac{1}{2^{10}} = \frac{252}{1024} = \frac{63}{256} \approx 0.2461\\
\Pr(E_{(\mathrm{d},6)}) &= \binom{10}{6}\cdot\frac{1}{2^{10}} = \frac{210}{1024} = \frac{105}{512} \approx 0.2051\\
\Pr(E_{(\mathrm{d},7)}) &= \binom{10}{7}\cdot\frac{1}{2^{10}} = \frac{120}{1024} = \frac{15}{128} \approx 0.1172\\
\Pr(E_{(\mathrm{d},8)}) &= \binom{10}{8}\cdot\frac{1}{2^{10}} = \frac{45}{1024} = \frac{45}{1024} \approx 0.0439\\
\Pr(E_{(\mathrm{d},9)}) &= \binom{10}{9}\cdot\frac{1}{2^{10}} = \frac{10}{1024} = \frac{5}{512} \approx 0.0098\\
\Pr(E_{(\mathrm{d},10)}) &= \binom{10}{10}\cdot\frac{1}{2^{10}} = \frac{1}{1024} = \frac{1}{1024} \approx 0.0010
\end{aligned}
$$

(e)

$$\Pr(E_{(\mathrm{e})}) = \Pr(\text{Even number of heads}) = \sum_{k\text{ even}} \Pr(E_{(\mathrm{c},k)}) = \frac{1}{2}.$$

(f) $\Pr(E_{(\mathrm{f})}) = \Pr(E_{(\mathrm{d})}) = \frac{1}{2}$.

5.22. 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 5.22.

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.

5.23. Let E and F be events.

(a) Prove that $\Pr(E \mid E) = 1$. Explain in words why this is reasonable.

(b) If E and F are disjoint, prove that $\Pr(F \mid E) = 0$. 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

$$F_1 \cup \cdots \cup F_n = \Omega,$$

where recall that Ω is the entire sample space. Prove the following general version of the decomposition formula (5.20) in Proposition 5.24(a):

$$\Pr(E) = \sum_{i=1}^{n} \Pr(E \mid F_i) \Pr(F_i).$$

(e) Prove a general version of Bayes's formula:

$$\Pr(F_i \mid E) = \frac{\Pr(E \mid F_i) \Pr(F_i)}{\Pr(E \mid F_1)\Pr(F_1) + \Pr(E \mid F_2)\Pr(F_2) + \cdots + \Pr(E \mid F_n)\Pr(F_n)}.$$

<u>*Solution to Exercise* 5.23</u>.

(a) $\Pr(E \mid E) = \dfrac{\Pr(E \cap E)}{\Pr(E)} = \dfrac{\Pr(E)}{\Pr(E)} = 1$. It is clear that if we know that E occurs, then the probability that E occurs is 1.

(b) $\Pr(F \mid E) = \dfrac{\Pr(F \cap E)}{\Pr(E)} = \dfrac{\Pr(\emptyset)}{\Pr(E)} = 0$. 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

$$E = \bigcup_{i=1}^{n} (E \cap F_i) \qquad \text{and} \qquad (E \cap F_i) \cap (E \cap E_j) = \emptyset \quad \text{for } i \neq j.$$

Hence

$$\begin{aligned}\Pr(E) &= \Pr\left(\bigcup_{i=1}^{n}(E\cap F_i)\right)\\ &= \sum_{i=1}^{n}\Pr(E\cap F_i) \qquad \text{since the } E\cap F_i \text{ are disjoint from one another,}\\ &= \sum_{i=1}^{n}\Pr(E\mid F_i)\Pr(F_i).\end{aligned}$$

5.24. 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 5.24.

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

$$\Pr(F \text{ and } G) = \Pr(F)\Pr(G \mid F).$$

We already know $\Pr(F) = 31/60$ from (a). To compute $\Pr(G \mid F)$, we do a calculation similar to the calculation in (a). Thus

$$\begin{aligned}
\Pr(G \mid F) &= \Pr(G \mid F\&E)\Pr(F\&E) + \Pr(G \mid F\&E^c)\Pr(F\&E^c) \\
&= \Pr(G \mid F\&E)\Pr(F \mid E)\Pr(E) + \Pr(G \mid F\&E^c)\Pr(F \mid E^c)\Pr(E^c) \\
&= \frac{6}{9}\cdot\frac{7}{10}\cdot\frac{1}{2} + \frac{3}{11}\cdot\frac{4}{12}\cdot\frac{1}{2} \\
&= \frac{46}{165} \approx 0.279.
\end{aligned}$$

5.25. 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 5.25.

(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 $\Pr(F \mid E)$ and we will use Baye's law in the form

$$\Pr(F \mid E) = \frac{\Pr(E \mid F)\Pr(F)}{\Pr(E)}.$$

As already explained, $\Pr(E) = 1/3$. Similarly, it is easy to compute $\Pr(E \mid F)$. 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 $\Pr(E \mid F) = 10/25 = 2/5$.

Finally, to compute $\Pr(F)$, define events $F_1, \ldots, F_5$ by

$$F_i = \{\text{Person } \#i \text{ draws a silver coin}\}.$$

Then

$$\begin{aligned}\Pr(F) &= \Pr(F_1\&F_2\&F_3\&F_4\&F_5)\\ &= \Pr(F_1)\cdot\Pr(F_2 \mid F_1)\cdot\Pr(F_3 \mid F_1\&F_2)\cdot\Pr(F_4 \mid F_1\&F_2\&F_3)\\ &\qquad\qquad\qquad\qquad\qquad\cdot\Pr(F_5 \mid F_1\&F_2\&F_3\&F_4)\\ &= \frac{20}{30}\cdot\frac{19}{29}\cdot\frac{18}{28}\cdot\frac{17}{27}\cdot\frac{16}{26}\\ &= \frac{2584}{23751}\approx 0.109.\end{aligned}$$

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%.

5.26. Consider the three prisoners scenario described in Example 5.26. Let A, B, and C denote respectively the events that Alice is to be released, Bob is to be released, and Carl is to be released, which we assume to be equally likely, so $\Pr(A) = \Pr(B) = \Pr(C) = \frac{1}{3}$. Also let J be the event that the jailer tells Aice that Bob is to stay in jail.

(a) Compute the values of $\Pr(B \mid J)$, $\Pr(J \mid B)$, and $\Pr(J \mid C)$.

(b) Compute the values of $\Pr(J \mid A^c)$ and $\Pr(J^c \mid A^c)$, where the event A^c is the event that Alice stays in jail.

(c) Suppose that if Alice is the one who is to be released, then the jailer flips a fair coin to decide whether to tell Alice that Bob stays in jail or that Carl stays in jail. What is the value of $\Pr(A \mid J)$?

(d) Suppose instead that if Alice is the one who is to be released, then the jailer always tells her that Bob will stay in jail. Now what is the value of $\Pr(A \mid J)$?

Other similar problems with counterintuitive conclusions include the Monty Hall problem (Exercise 5.27), Bertrand's box paradox, and the principle of restricted choice in contract bridge.

Solution to Exercise 5.26.

(a) Since we are assuming that the jailer doesn't lie, if he tells Alice that Bob will stay in jail, then Bob will stay in jail, so he cannot go free. Hence $\Pr(B \mid J) = 0$. Similarly, if Bob is to go free, then the jailer can't tell Alice that Bob will stay in jail, so $\Pr(J \mid B) = 0$. Finally, if Carl is to go free, then the jailer has no choice but to tell Alice that Bob will stay in jail (since he never tells Alice that she stays in jail), or $\Pr(J \mid C) = 1$.

(b) If Alice is to stay in jail, which is the event A^c, then it is equally likely that Bob and Carl will be the other person who stays in jail, so it is equally likely that the jailer tells her that Bob or Carl is to stay in jail. Hence

$$\Pr(J \mid A^c) = \Pr(J^c \mid A^c) = \frac{1}{2}$$

(c) We use Baye's formula. The assumption that the jailer flips a coin when Alice is to go free means that

$$\Pr(J \mid A) = \Pr(J^c \mid A) = \frac{1}{2},$$

that is, if Alice is to go free, then there's an equal probability that the jailer tells her that Bob or Carl is to say in jail. Using this and (b), we can compute

$$\Pr(J) = \Pr(J \mid A)\Pr(A) + \Pr(J \mid A^c)\Pr(A^c) = \frac{1}{2}\cdot\frac{1}{3} + \frac{1}{2}\cdot\frac{2}{3} = \frac{1}{2}.$$

Now Baye's formula gives

$$\Pr(A \mid J) = \frac{\Pr(J \mid A)\Pr(A)}{\Pr(J)} = \frac{\frac{1}{2}\cdot\frac{1}{3}}{\frac{1}{2}} = \frac{1}{3}.$$

So Alice's chances of being released are still $\frac{1}{3}$, despite the information provided by the jailer.

(d) Now the situation is a bit different. If event A is true, then event J is true, i.e.,

$$\Pr(J \mid A) = 1 \quad \text{and} \quad \Pr(J^c \mid A) = 0.$$

On the other hand, we still have $\Pr(J \mid A^c) = \frac{1}{3}$ from (b). So now when we compute $\Pr(J)$, we get

$$\Pr(J) = \Pr(J \mid A)\Pr(A) + \Pr(J \mid A^c)\Pr(A^c) = 1\cdot\frac{1}{3} + \frac{1}{2}\cdot\frac{2}{3} = \frac{2}{3}.$$

Then Baye's formula gives

$$\Pr(A \mid J) = \frac{\Pr(J \mid A)\Pr(A)}{\Pr(J)} = \frac{1\cdot\frac{1}{3}}{\frac{2}{3}} = \frac{1}{2}.$$

So in this scenario, Alice's chance of being released has increased to $\frac{1}{2}$.

5.27. (*The Monty Hall Problem*) Monty Hall gives Dan the choice of three curtains. Behind one curtain is a car, while behind the other two curtains are goats. Dan chooses a curtain, but before it is opened, Monty Hall opens one of the other curtains and reveals a goat. He then offers Dan the option of keeping his original curtain or switching to the remaining closed curtain. The Monty Hall problem is to figure out Dan's best strategy: "To stick or to switch?"

(a) What is the probability that Dan wins the car if he always sticks to his first choice of curtain? What is the probability that Dan wins the car if he always switches curtains? Which is his best strategy? (If the answer seems counter-intuitive, suppose instead that there are 1000 curtains and that Monty Hall opens 998 goat curtains. Now what are the winning probabilities for the two strategies?)

(b) Suppose that we give Monty Hall another option, namely he's allowed to force Dan to stick with his first choice of curtain. Assuming that Monty Hall dislikes giving away cars, now what is Dan's best strategy, and what is his probability of winning a car?

(c) More generally, suppose that there are N curtains and M cars, and suppose that Monty Hall opens K curtains that have goats behind them. Compute the probabilities

$$\Pr(\text{Dan wins a car} \mid \text{Dan sticks}), \quad \Pr(\text{Dan wins a car} \mid \text{Dan switches}).$$

Which is the better strategy?

<u>*Solution to Exercise*</u> <u>5.27</u>.

(a) This can be done formally using conditional probabilities, but it's just as easy to calculate directly. Dan has a $\frac{1}{3}$ chance of choosing the car initially. So if Dan sticks with his first choice, then his probability of winning the car remains at $\frac{1}{3}$. On the other hand, if he initially chooses a goat, which happens $\frac{2}{3}$ of the time, then since Monty Hall is required to reveal the other goat, when Dan switches he is guaranteed to win the car. Hence switches gets Dan the car $\frac{2}{3}$ of the time. Thus

$$\begin{aligned}\Pr(\text{Dan wins a car} \mid \text{Dan sticks}) &= \frac{1}{3},\\ \Pr(\text{Dan wins a car} \mid \text{Dan switches}). &= \frac{2}{3}.\end{aligned}$$

If instead there are 1000 curtains, still only one car, and Monty Hall opens 998 curtains with goats, then a similar argument gives

$$\begin{aligned}\Pr(\text{Dan wins a car} \mid \text{Dan sticks}) &= \frac{1}{1000},\\ \Pr(\text{Dan wins a car} \mid \text{Dan switches}). &= \frac{999}{1000}.\end{aligned}$$

(b) Now things have changed. If Dan initially chooses a goat, then Monty Hall is going to force him to keep the goat. So the only time that Monty Hall gives Dan an option to switch is when Dan initially chose the car. Hence the switching strategy guarantees that Dan gets a goat! This means that if he's playing against this evil Monty Hall, then

$$\begin{aligned}\Pr(\text{Dan wins a car} \mid \text{Dan sticks}) &= \frac{1}{3},\\ \Pr(\text{Dan wins a car} \mid \text{Dan switches}). &= 0.\end{aligned}$$

(c) Using the sticking strategy, the probability that Dan wins a car is simply his probability of choosing a winning ticket, so when there are M winning tickets and N total tickets, this gives

$$\Pr(\text{Dan wins a car} \mid \text{Dan sticks}) = \frac{M}{N}.$$

Now consider the switching strategy. This means that Dan picks a curtain, Monty Hall opens K goat curtains, and Dan then chooses one of the remaining curtains at random. We define events

$$\begin{aligned} W &= \text{Dan wins a car if he switches,} \\ C &= \text{Dan's initial curtain is a car curtain.} \end{aligned}$$

We want to compute $\Pr(W)$. We compute it as

$$\Pr(W) = \Pr(W \mid C)\Pr(C) + \Pr(W \mid C^c)\Pr(C^c).$$

In the given scenario, there are N curtains and M cars, so

$$\Pr(C) = \frac{M}{N} \quad \text{and} \quad \Pr(C^c) = \frac{N-M}{N}.$$

Next suppose that Dan's initial curtain is a car. Monty Hall reveals K of the goat curtains, so the remaining $N - K - 1$ curtains have $M - 1$ cars. Dan picks one at random, so his chance of winning a car in this scenario is

$$\Pr(W \mid C) = \frac{M-1}{N-K-1}.$$

Similarly, if Dan's initial curtain is a goat, then after Monty Hall opens K goat curtains, the remaining $N - K - 1$ curtains still have M cars, so

$$\Pr(W \mid C^c) = \frac{M}{N-K-1}.$$

We can now compute

$$\begin{aligned} \Pr(W) &= \Pr(W \mid C)\Pr(C) + \Pr(W \mid C^c)\Pr(C^c) \\ &= \frac{M-1}{N-K-1} \cdot \frac{M}{N} + \frac{M}{N-K-1} \cdot \frac{N-M}{N} \\ &= \frac{M(N-1)}{N(N-K-1)} \\ &= \frac{M}{N} + \frac{MK}{N(N-K-1)}. \end{aligned}$$

The last line shows that the switching strategy is always best, since it is strictly larger than $\frac{M}{N}$, which is the probability of winning a car using the sticking strategy.

5.28. Let $\mathcal{S}$ be a set, let A be a property of interest, and suppose that for $m \in \mathcal{S}$, we have

$$\Pr(m \text{ does not have property } A) = \delta.$$

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) $\Pr(m \text{ has property } A \mid \text{algorithm returns } \mathsf{Yes}) = 1$,

(2) $\Pr(\text{algorithm returns } \mathsf{Yes} \mid m \text{ has property } A) \ge p$.

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 δ, 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 5.3.3 with $\delta = 0.01$ and $p = \frac{1}{2}$. Be careful to distinguish p from $1-p$ in your calculations.)

<u>*Solution to Exercise* 5.28</u>.

Let

$$E = \{\text{an element } m \in \mathcal{S} \text{ does not have property } A\}.$$
$$F = \{\text{the algorithm returns } \mathsf{No}\ N \text{ times in a row}\}.$$

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 not having property A is δ, so

$$\Pr(E) = \Pr(\text{not } A) = \delta \qquad \text{and} \qquad \Pr(E^c) = \Pr(A) = 1 - \delta.$$

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

$$\Pr(\mathsf{No} \mid \text{not } A) = \Pr(A \mid \mathsf{Yes}) = 1,$$

from which it follows that $\Pr(F \mid E) = \Pr(\mathsf{No} \mid \text{not } A)^N = 1$.

Finally, we must compute the value of $\Pr(F \mid E^c)$. Since the algorithm is run N independent times, we have

$$\begin{aligned}\Pr(F \mid E^c) &= \Pr(\text{Output is } \mathsf{No} \mid m \text{ has property } A)^N \\ &= \bigl(1 - \Pr(\text{Output is } \mathsf{Yes} \mid m \text{ has property } A)\bigr)^N \\ &\le (1-p)^N \qquad \text{from Property (2) of the Monte Carlo method.}\end{aligned}$$

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

$$\Pr(E \mid F) \geq \frac{1 \cdot \delta}{1 \cdot \delta + (1-p)^N \cdot (1-\delta)} = \frac{\delta}{\delta + (1-p)^N \cdot (1-\delta)}.$$

If δ and p are not too small and N is large, this can be approximated by

$$\Pr(E \mid F) \geq 1 - \frac{(1-p)^N \cdot (1-\delta)}{\delta + (1-p)^N \cdot (1-\delta)} \approx 1 - \frac{(1-p)^N \cdot (1-\delta)}{\delta} = 1-(1-p)^N \cdot (\delta^{-1}-1).$$

5.29. We continue with the setup described in Exercise 5.28.

(a) 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?

(b) Same question as (a), but this time we run the algorithm 100 times.

(c) 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?

(d) Same question as (c), except now we want to be 99.9999% confident.

Solution to Exercise 5.29.

A solution for this exercise is not currently available.

5.30. 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 5.28 with appropriate choices of A, $\mathcal{S}$, δ, 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 5.30.

In Exercise 5.28 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 δ 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)

$$\begin{aligned}
&\Pr(n \text{ is prime} \mid \text{the Miller–Rabin test fails } N \text{ times}) \\
&\qquad \ge 1 - \frac{(1-p)^N}{\delta^{-1} - 1} \\
&\qquad \approx 1 - \frac{\ln(n) - 1}{4^N} \\
&\qquad \approx 1 - \frac{\ln(n)}{4^N}.
\end{aligned}$$

5.31. It is natural to assume that if $\Pr(E \mid F)$ is significantly larger than $\Pr(E)$, then somehow F is causing E. Baye's formula illustrates the fallacy of this sort of reasoning, since it says that

$$\frac{\Pr(E \mid F)}{\Pr(E)} = \frac{\Pr(F \mid E)}{\Pr(F)}.$$

So if F is "causing" E, then the same reasoning shows that E is "causing" F. All that one can really say is that E and F are correlated with one another, in the sense that either one of them being true makes it more likely that the other one is true. It is incorrect to deduce a cause-and-effect relation.

Here is a concrete example. Testing shows that first graders are more likely to be good spellers if their shoe sizes are larger than average. This is an experimental fact. Hence if we stretch a child's foot, it will make them a better speller! Alternatively, by Baye's formula, if we give them extra spelling lessons, then their feet will grow faster! Explain why these last two assertions are nonsense, and describe what's really going on.

Solution to Exercise 5.31.

In a first grade class, some of the children are as much as a year older than other children. And older children have, on average, both larger feet and better congnitive functions, which is reflected in better spelling ability. Thus the correct cause-and-effect deduction is that greater age causes greater body growth, which in turn causes both larger feer and more brain development.

5.32. Let $f_X(k)$ be the binomial density function (5.23). Prove directly, using the binomial theorem, that $\sum_{k=0}^{n} f_X(k) = 1$.

Solution to Exercise 5.32.

Let $q = 1 - p$, so $p + q = 1$. Then we use the binomial theorem to compute

$$\sum_{k=0}^{n} f_X(k) = \sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} = \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} = (p+q)^n = 1^n = 1.$$

5.33. In Example 5.37 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

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x} \qquad \text{for } |x| < 1 \tag{5.1}$$

and the differential operator

$$\mathcal{D} = x\frac{d}{dx}.$$

(a) Using the fact that $\mathcal{D}(x^n) = nx^n$, prove that

$$\sum_{n=1}^{\infty} nx^n = \frac{x}{(1-x)^2} \tag{5.2}$$

by applying $\mathcal{D}$ to both sides of (5.57). For which x does the left-hand side of (5.58) converge? (*Hint.* Use the ratio test.)

(b) Applying $\mathcal{D}$ again, prove that

$$\sum_{n=0}^{\infty} n^2x^n = \frac{x+x^2}{(1-x)^3}. \tag{5.3}$$

(c) More generally, prove that for every value of k there is a polynomial $F_k(x)$ such that

$$\sum_{n=0}^{\infty} n^kx^n = \frac{F_k(x)}{(1-x)^{k+1}}. \tag{5.4}$$

(*Hint.* Use induction on k.)

(d) The first few polynomials $F_k(x)$ in (c) are $F_0(x) = 1$, $F_1(x) = x$, and $F_2(x) = x + x^2$. These follow from (5.57), (5.58), and (5.59). Compute $F_3(x)$ and $F_4(x)$.

(e) Prove that the polynomial $F_k(x)$ in (c) has degree k.

Solution to Exercise 5.33.

In general we have

$$\Theta^k\left(\frac{1}{1-x}\right) = \Theta^k\left(\sum_{n=0}^{\infty} x^n\right) = \sum_{n=0}^{\infty} n^kx^n.$$

The series on the right is absolutely convergant for $|x| < 1$ via the ratio test

$$\rho = \lim_{n\to\infty} \frac{|(n+1)^kx^{n+1}|}{|n^kx^n|} = \lim_{n\to\infty}\left(\frac{n+1}{n}\right)^k |x| = |x|,$$

which justifies the term-by-term differentiation in this interval. The series clearly diverges for $|x| = 1$ (unless $k = 0$, in which case it is conditionally convergent at $x = -1$).

We now need merely observe that applying $\mathcal{D}^k$ to $1/(1-x)$ gives a rational function $F_k(x)/(1-x)^{k+1}$. More formally, we have by induction

$$\begin{aligned}
\mathcal{D}^k\left(\frac{1}{1-x}\right) &= \mathcal{D}\left(\frac{F_{k-1}(x)}{(1-x)^k}\right) \\
&= x\Big(F_{k-1}(x)(k(1-x)^{-k-1}) + F'_{k-1}(x)(1-x)^{-k}\Big) \\
&= \frac{kxF_{k-1}(x) + (x-x^2)F'_{k-1}(x)}{(1-x)^{k+1}}
\end{aligned}$$

So if we define $F_k(x)$ inductively by the recursion

$$F_0(x) = 1 \quad \text{and} \quad F_k(x) = kxF_{k-1}(x) + (x-x^2)F'_{k-1}(x),$$

then

$$\mathcal{D}^k\left(\frac{1}{1-x}\right) = \frac{F_k(x)}{(1-x)^{k+1}}.$$

It's a simple matter to use the recursion, or apply $\mathcal{D}$ several times to $1/(1-x)$, to compute the first few $F_i(x)$. Thus

$$\begin{aligned}
&F_0(x) = 1 \\
&F_1(x) = x \\
&F_2(x) = x^2 + x \\
&F_3(x) = x^3 + 4 * x^2 + x \\
&F_4(x) = x^4 + 11 * x^3 + 11 * x^2 + x \\
&F_5(x) = x^5 + 26 * x^4 + 66 * x^3 + 26 * x^2 + x \\
&F_6(x) = x^6 + 57 * x^5 + 302 * x^4 + 302 * x^3 + 57 * x^2 + x \\
&F_7(x) = x^7 + 120 * x^6 + 1191 * x^5 + 2416 * x^4 + 1191 * x^3 + 120 * x^2 + x
\end{aligned}$$

It remains to show that $\deg F_k(x) = k$. It's clear from the recursion that $\deg F_k \le \deg F_{k-1} + 1$, so $\deg F_k \le k$. But xF_{k-1} and $(x-x^2)F'_{k-1}$ have the same degree, so in principle there could be some cancelation. However, using the recursion, it is in fact easy to check that $F_k(x) = x^k +$(lower order terms). This is true for $k = 0$, and then by induction (writing *lot* for lower order terms)

$$\begin{aligned}
F_k &= kxF_{k-1} + (x-x^2)F'_{k-1} \\
&= kx(x^{k-1} + lot) + (x-x^2)((k-1)x^{k-2} + lot) \\
&= kx^k + lot - (k-1)x^k + lot \\
&= x^k + lot.
\end{aligned}$$

5.34. In each case, compute the expectation of the random variable X.

(a) The values of X are uniformly distributed on the set $\{0, 1, 2, \ldots, N-1\}$. (See Example 5.28.)

(b) The values of X are uniformly distributed on the set $\{1, 2, \ldots, N\}$.

(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 formula (5.23) in Example 5.29 on page 240.

<u>*Solution to Exercise* 5.34</u>.

(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.

5.35. Let X be a random variable on the probability space Ω. It might seem more natural to define the expected value of X by the formula

$$\sum_{\omega \in \Omega} X(\omega) \cdot \Pr(\omega). \tag{5.5}$$

Prove that the formula (5.61) gives the same value as equation (5.27) on page 244, which we used in the text to define $E(X)$.

Solution to Exercise 5.35.

We compute (the key step comes in the middle where we reverse the order of summation):

$$\begin{aligned} E(X) &= \sum_{i=1}^{n} x_i \cdot f_X(x_i) \\ &= \sum_{i=1}^{n} x_i \cdot \Pr(X = x_i) \\ &= \sum_{i=1}^{n} x_i \Pr\bigl\{\omega \in \Omega : X(\omega) = x_i\bigr\} \\ &= \sum_{i=1}^{n} x_i \sum_{\substack{\omega\in\Omega \\ X(\omega)=x_i}} \Pr(\omega) \\ &= \sum_{\omega\in\Omega} \Pr(\omega) \sum_{\substack{1\le i\le n \\ x_i=X(\omega)}} x_i \\ &= \sum_{\omega\in\Omega} \Pr(\omega) \cdot X(\omega), \end{aligned}$$

where for the final equality we use that fact that $x_1, \ldots, x_n$ are distinct, so each $X(\omega)$ is equal to exactly one of the x_i values.

Section. Collision algorithms and the birthday paradox

5.36. (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 5.4.1.)

(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 (5.28), for the probability that at least two of them have the same birthday. (*Hint.* Do a calculation similar to the proof of (5.28) in the collision theorem (Theorem 5.38), 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

$$\Pr(\text{at least one match}) \ge 1 - e^{-(\text{some function of } n \text{ and } N)}$$

for the probability in (b), analogous to the estimate (5.29).

Solution to Exercise 5.36.

We start by doing (b).

$$\begin{aligned}
\Pr\begin{pmatrix}\text{at least one match}\\ \text{in } n \text{ attempts}\end{pmatrix} &= 1 - \Pr\begin{pmatrix}\text{all } n \text{ birthdays}\\ \text{are different}\end{pmatrix}\\
&= 1 - \prod_{i=1}^{n} \Pr\begin{pmatrix} i^{\text{th}} \text{ birthday is different}\\ \text{from all of the}\\ \text{previous } i-1 \text{ birthdays}\end{pmatrix}\\
&= 1 - \prod_{i=1}^{n} \frac{N-(i-1)}{N}\\
&= 1 - \prod_{i=1}^{n-1}\left(1 - \frac{i}{N}\right).
\end{aligned}$$

Then the answer to the first part of (a) is obtained by setting $N = 365$ and $n = 23$, which gives

$$\text{(a)} \qquad \Pr(\text{match}) = 1 - \prod_{i=1}^{22}\left(1 - \frac{i}{365}\right) \approx 50.73\%.$$

Similarly, $N = 365$ and $n = 40$ gives the answer to the second part of (a),

$$\text{(b)} \qquad \Pr(\text{match}) = 1 - \prod_{i=1}^{39}\left(1 - \frac{i}{365}\right) \approx 89.12\%.$$

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 $e^{-x} \ge 1 - x$ with $x = i/N$ to compute

$$\begin{aligned}
\Pr\begin{pmatrix}\text{at least one match}\\ \text{in } n \text{ attempts}\end{pmatrix} &= 1 - \prod_{i=1}^{n-1}\left(1 - \frac{i}{N}\right)\\
&\ge 1 - \prod_{i=1}^{n-1} e^{-i/N}\\
&= 1 - e^{-(1+2+\cdots+(n-1))/N}\\
&= 1 - e^{-(n-1)n/2N}\\
&\approx 1 - e^{-n^2/2N}.
\end{aligned}$$

Notice that we have used the well known formula

$$1 + 2 + \cdot + (n-1) = \frac{n(n-1)}{2}.$$

5.37. 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 5.39 because the cards in the second deck are not being replaced.)

Solution to Exercise 5.37.

A solution for this exercise is not currently available.

5.38. (a) Prove that

$$e^{-x} \ge 1 - x \quad \text{for all values of } x.$$

(*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

$$e^{-ax} \le (1-x)^a + \frac{1}{2}ax^2 \quad \text{is valid for all } 0 \le x \le 1.$$

(This is a challenging problem.)

(c) We used the inequality in (a) during the proof of the lower bound (5.29) in the collision theorem (Theorem 5.38). Use (b) to prove that

$$\Pr(\text{at least one red}) \le 1 - e^{-mn/N} + \frac{mn^2}{2N^2}.$$

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 5.38.

(a) Let $f(x) = e^{-x} - 1 + x$. Then $f(0) = f'(0) = 0$. Then generalized mean value theorem says that

$$f(x) = f(0) + f'(0)x + \frac{1}{2}f''(z)x^2 \quad \text{for some } 0 \le z \le x,$$

so we find that $f(x) = \frac{1}{2}e^{-z}x^2 \ge 0$. 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^{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 $f(x) \ge 0$ provided that $a > 0.8526055\ldots$, where $c = 0.8526055\ldots$ is the unique real solution to $ce^c = 2$.

(c) We have

$$\begin{aligned} \Pr\begin{pmatrix}\text{at least}\\ \text{one red}\end{pmatrix} &= 1 - \left(1 - \frac{n}{N}\right)^m && \text{from the Collision Theorem} \\ &\le 1 - \left(e^{-mn/N} - \frac{mn^2}{2N^2}\right) && \text{use (b) with } a = m \text{ and } x = \frac{n}{N}. \end{aligned}$$

5.39. 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 5.17.

Solution to Exercise 5.39.

From Table 5.17 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	g^i	$h \cdot g^i$	i	g^i	$h \cdot g^i$	i	g^i	$h \cdot g^i$	i	g^i	$h \cdot g^i$
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 5.12: Data for Exercise 5.39, $g = 10$, $h = 106$, $p = 811$

Section. Pollard's ρ method

5.40. Table 5.18 gives some of the computations for the solution of the discrete logarithm problem

$$11^t = 41387 \quad \text{in } \mathbb{F}_{81799} \tag{5.6}$$

using Pollard's ρ method. (It is similar to Table 5.11 in Example 5.52.) Use the data in Table 5.18 to solve (5.62).

<u>*Solution to Exercise* 5.40</u>.

$$x_{308} = x_{154} = 15386 \quad \text{in } \mathbb{F}_{81799}.$$

$$\alpha_{154} = 81756, \qquad \beta_{154} = 9527, \qquad \gamma_{154} = 67782, \qquad \delta_{154} = 28637.$$

$$11^{81756} \cdot 41387^{9527} = 11^{67782} \cdot 41387^{28637} \quad \text{in } \mathbb{F}_{81799}.$$

$$11^{13974} = 41387^{19110} \quad \text{in } \mathbb{F}_{81799}.$$

$$\gcd(19110, 81798) = 6.$$

$$81340 \cdot 19110 \equiv 6 \pmod{81798}.$$

$$11^{13974 \cdot 81340} = 11^{1136645160} = 11^{61950} = 41387^6 \quad \text{in } \mathbb{F}_{81799}.$$

$$\frac{61950}{6} = 10325, \qquad \frac{81798}{6} = 13633.$$

$$\log_{11}(41387) \in \{10325 + 13633 \cdot k : 0 \le k < 6\}$$
$$= \{10325, 23958, 37591, 51224, 64857, 78490\}.$$

$$11^{10325} = 73192, \quad 11^{23958} = 40412, \quad 11^{37591} = 49019, \quad 11^{51224} = 8607,$$
$$\boxed{11^{64857} = 41387}, \quad 11^{78490} = 32780.$$

5.41. Table 5.19 gives some of the computations for the solution of the discrete logarithm problem

$$7^t = 3018 \quad \text{in } \mathbb{F}_{7963} \tag{5.7}$$

i	x_i	y_i	α_i	β_i	γ_i	δ_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
			⋮			
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 5.13: Computations to solve $11^t = 41387$ in $\mathbb{F}_{81799}$ for Exercise 5.40

using Pollard's ρ method. (It is similar to Table 5.11 in Example 5.52.) Extend Table 5.19 until you find a collision (we promise that it won't take too long) and then solve (5.63).

Solution to Exercise 5.41.

Extending the table:

i	x_i	y_i	α_i	β_i	γ_i	δ_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

$$x_{186} = x_{93} = 1217 \quad \text{in } \mathbb{F}_{7963}.$$

$$\alpha_{93} = 6741, \qquad \beta_{93} = 7648, \qquad \gamma_{93} = 4647, \qquad \delta_{93} = 7656.$$

$$7^{6741} \cdot 3018^{7648} = 7^{4647} \cdot 3018^{7656} \quad \text{in } \mathbb{F}_{7963}.$$

$$7^{2094} = 3018^{8} \quad \text{in } \mathbb{F}_{7963}.$$

$$7^{2094} = 3018^{8} \quad \text{in } \mathbb{F}_{7963}.$$

$$\gcd(8, 7962) = 2.$$

$$6967 \cdot 8 \equiv 2 \pmod{7962}.$$

$$7^{2094 \cdot 6967} = 7^{14588898} = 7^{2514} = 3018^{2} \quad \text{in } \mathbb{F}_{7963}.$$

$$\frac{2514}{2} = 1257, \qquad \frac{7962}{2} = 3981.$$

$$\log_7(3018) \in \{1257 + 3981 \cdot k : 0 \le k < 2\} = \{1257, 5238\}.$$

$$7^{1257} = 4945, \quad 7^{5238} = 3018.$$

i	x_i	y_i	α_i	β_i	γ_i	δ_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
			⋮			
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 5.14: Computations to solve $7^t = 3018$ in $\mathbb{F}_{7963}$ for Exercise 5.41

5.42. Write a computer program implementing Pollard's ρ 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 5.42.

(a) $\boxed{2^{3351} = 2495}$.
(b) $\boxed{17^{14557} = 14226}$.
(c) $\boxed{29^{2528453} = 5953042}$.

5.43. Evaluate the integral $I = \int_0^\infty t^2 e^{-t^2/2}\,dt$ appearing in the proof of Theorem 5.48. (*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 5.43.

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

$$\int_0^{\pi/2} \sin^2\theta\cos^2\theta\,d\theta = \int_0^{\pi/2} \frac{1-\cos(4\theta)}{8}\,d\theta = \frac{\theta}{8} - \frac{\sin(4\theta)}{32}\bigg|_0^{\pi/2} = \frac{\pi}{16}.$$

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 $I = \sqrt{\pi/2}$.

5.44. This exercise describes Pollard's ρ factorization algorithm. It is particularly good at factoring numbers N that have a prime factor p with the property that p is considerably smaller than N/p. Later we will study an even faster, albeit more complicated, factorization algorithm with this property that is based on the theory of elliptic curves; see Section 6.6.

Let N be an integer that is not prime, and let

$$f : \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}$$

be a mixing function, for example $f(x) = x^2 + 1 \bmod N$. As in the abstract verion of Pollard's ρ method (Theorem 5.48), let $x_0 = y_0$ be an initial value, and generate sequences by setting $x_{i+1} = f(x_i)$ and $y_{i+1} = f(f(y_i))$. At each step, also compute the greatest common divisor

$$g_i = \gcd\bigl(|x_i - y_i|, N\bigr).$$

(a) Let p be the smallest prime divisor of N. If the function f is sufficiently random, show that with high probability we have

$$g_k = p \quad \text{for some } k = \mathcal{O}(\sqrt{p}).$$

Hence the algorithm factors N in $\mathcal{O}(\sqrt{p})$ steps.

(b) Program Pollard's ρ algorithm with $f(x) = x^2 + 1$ and $x_0 = y_0 = 0$, and use it to factor the following numbers. In each case, give the smallest value of k such that g_k is a nontrivial factor of N and print the ratio $k/\sqrt{N}$.

(i) $N = 2201$. (ii) $N = 9409613$. (iii) $N = 1782886219$.

(c) Repeat your computations in (b) using the function $f(x) = x^2 + 2$. Do the running times change?

(d) Explain what happens if you run Pollard's ρ algorithm and N is prime.

(e) Explain what happens if you run Pollard's ρ algorithm with $f(x) = x^2$ and any initial values for x_0.

(f) Try running Pollard's ρ algorithm with the function $f(x) = x^2 - 2$. Explain what is happening. (*Hint.* This part is more challenging. It may help to use the identity $f^n(u + u^{-1}) = u^{2^n} + u^{-2^n}$, which you can prove by induction.)

Solution to Exercise 5.44.

(a) We consider the sequences x_i and $y_i = x_{2i}$ modulo p. (Note that this is modulo p, not modulo N.) Then the values are in $\mathbb{Z}/p\mathbb{Z}$. We apply the abstract version of Pollard's ρ method with $S = \mathbb{Z}/p\mathbb{Z}$, so our set has p elements. The theorem says that with high probability, we get

$$y_k \equiv x_k \pmod{p} \quad \text{for some } k = \mathcal{O}(\sqrt{p}).$$

Since it is unlikely that there is some other prime divisor $q \mid N$ such that $y_k \equiv x_k \pmod{q}$ for the same k, we see that $g_k = \gcd(y_k - x_k, N) = p$.

(b)

N	$p = g_k$	N/g_k	k	$k/\sqrt{p}$
2201	31	71	4	0.718
9409613	541	17393	34	1.462
1782886219	7933	224743	126	1.415

(c)

N	$p = g_k$	N/g_k	k	$k/\sqrt{p}$
2201	71	31	7	1.257
9409613	541	17393	6	0.258
1782886219	7933	224743	68	0.763

(d) At some point we will get $g_k = N$, but that won't tell us that N is prime. So before running Pollard's algorithm, one should check that N is composite using some primality test such as Miller–Rabin.

(e) Unless we are extremely lucky, we will have $\gcd(x_0, N) = 1$. Since $x_k = x_0^{2^k}$, we find that

$$\begin{aligned} g_k &= \gcd(x_0^{2^k} - x_0^{2^(2k)}, N) \\ &= \gcd(x_0^{2^k} - x_0^{4^k}, N) \\ &= \gcd(x_0^{2^k}(1 - x_0^{4^k - 2^k}), N) \\ &= \gcd(1 - x_0^{4^k - 2^k}, N). \end{aligned}$$

So we will get $g_k = p$ if

$$x_0^{4^k - 2^k} \equiv 1 \pmod{p}.$$

The number x_0 has some order modulo p, say it has order r, where r is a divisor of $p - 1$. In general, it will be true that $r = \mathcal{O}(p)$. So we get $g_k = p$ when

$$4^k \equiv 2^k \pmod{r},$$

or equivalently (for simplicity we'll assume that r is odd) when

$$2^k \equiv 1 \pmod{r}.$$

So we need k to be the order of 2 modulo r, which again in general will be $\mathcal{O}(r)$. Tracing through our computations, we see that the first k such that $g_k = p$ will satsify $k = \mathcal{O}(p)$. Thus even if it works, the running time of Pollard's algorithm with $f(x) = x^2$ is $\mathcal{O}(p)$, not $\mathcal{O}(\sqrt{p})$. The reason is that the function $f(x) = x^2$ is in fact a very poor mixing functions.

(e) The polynomial $f(x) = x^2 - 2$ also has poor mixing properties, due to the identity described in the hint.

Section. Information theory

5.45. 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 5.12 used in Example 5.54 on page 265).

	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:

$$f(m_1) = f(m_2) = \frac{2}{5}, \qquad f(m_3) = \frac{1}{5}, \qquad f(k_1) = f(k_2) = f(k_3) = \frac{1}{3}.$$

(a) Compute $f(c_1)$, $f(c_2)$, $f(c_3)$, and $f(c_4)$.

(b) Compute $f(c_1 \mid m_1)$, $f(c_1 \mid m_2)$, and $f(c_1 \mid m_3)$. Does this cryptosystem have perfect secrecy?

(c) Compute $f(c_2 \mid m_1)$ and $f(c_3 \mid m_1)$.

(d) Compute $f(k_1 \mid c_3)$ and $f(k_2 \mid c_3)$.

Solution to Exercise 5.45.

(a)

$$\begin{aligned}
f(c_1) &= f(k_1)f_M(d_{k_1}(c_1)) + f(k_2)f_M(d_{k_2}(c_1)) + f(k_3)f_M(d_{k_3}(c_1)) \\
&= f(k_1)f(m_3) + f(k_2)f(m_1) + f(k_3)f(m_2) \\
&= \frac{1}{3}\cdot\frac{1}{5} + \frac{1}{3}\cdot\frac{2}{5} + \frac{1}{3}\cdot\frac{2}{5} \\
&= \frac{1}{3}. \\
f(c_2) &= f(k_1)f_M(d_{k_1}(c_2)) + f(k_2)f_M(d_{k_2}(c_2)) + f(k_3)f_M(d_{k_3}(c_2)) \\
&= f(k_1)f(m_1) + f(k_2)f(m_3) + f(k_3)f(m_3) \\
&= \frac{1}{3}\cdot\frac{2}{5} + \frac{1}{3}\cdot\frac{1}{5} + \frac{1}{3}\cdot\frac{1}{5} \\
&= \frac{4}{15}. \\
f(c_3) &= f(k_1)f_M(d_{k_1}(c_3)) + f(k_2)f_M(d_{k_2}(c_3)) + f(k_3)f_M(d_{k_3}(c_3)) \\
&= f(k_1)\cdot 0 + f(k_2)f(m_2) + f(k_3)f(m_1) \\
&= 0 + \frac{1}{3}\cdot\frac{2}{5} + \frac{2}{3}\cdot\frac{1}{5} \\
&= \frac{4}{15}. \\
f(c_4) &= f(k_1)f_M(d_{k_1}(c_4)) + f(k_2)f_M(d_{k_2}(c_4)) + f(k_3)f_M(d_{k_3}(c_4)) \\
&= f(k_1)f(m_2) + f(k_2)\cdot 0 + f(k_3)\cdot 0 \\
&= \frac{1}{3}\cdot\frac{2}{5} + 0 + 0 \\
&= \frac{2}{15}.
\end{aligned}$$

(b)

$$\begin{aligned}
f(c_1 \mid m_1) &= f(k_2) = \frac{1}{3}. \\
f(c_1 \mid m_2) &= 0. \\
f(c_1 \mid m_3) &= f(k_1) = \frac{1}{3}.
\end{aligned}$$

This cryptosystem does not have prefect secrecy, since for example $f(c_1) = \frac{1}{3}$ is not equal to $f(c_1 \mid m_2) = 0$.

(c)

$$\begin{aligned}
f(c_2 \mid m_1) &= f(k_1) = \frac{1}{3}. \\
f(c_3 \mid m_1) &= f(k_3) = \frac{1}{3}.
\end{aligned}$$

(d)

$$f(k_1 \mid c_3) = 0.$$

$$f(k_2 \mid c_3) = \frac{f(c_3 \mid k_2) f(k_2)}{f(c_3)} = \frac{f(m_2) f(k_2)}{f(c_3)} = \frac{(2/5)(1/3)}{4/15} = \frac{1}{2}.$$

(For the last computation, we used the value $f(c_3) = 4/15$ from (a).)

5.46. 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.

(a) Show that $\sum_{k \in \mathcal{K}} f_M(d_k(c)) = 1$ for every ciphertext $c \in \mathcal{C}$.

(b) Compute the ciphertext density function f_C using (5.47), which in this case says that

$$f_C(c) = \sum_{k \in \mathcal{K}} f_K(k) f_M(d_k(c)).$$

(c) Compare $f_C(c)$ to $f_{C|M}(c \mid m)$.

Solution to Exercise 5.46.

(a) For a given ciphertext c, as k ranges over all possible keys, i.e., k ranges over all possible shift amounts, the possible decryptions $d_k(c)$ of c range over all of the possible plaintexts. Hence

$$\sum_{k \in \mathcal{K}} f_M(d_k(c)) = \sum_{m \in \mathcal{M}} f_M(m) = 1.$$

(b) Since we are assuming that each key is used with equal probability and there are 26 keys, we have $f_K(k) = \frac{1}{26}$ for every key k. Hence

$$f_C(c) = \sum_{k \in \mathcal{K}} f_K(k) f_M(d_k(c)) = \sum_{k \in \mathcal{K}} \frac{1}{26} f_M(d_k(c)) = \frac{1}{26},$$

where for the last equality we used (a).

(c) For a given ciphertext c and given plaintext m, there is exactly one key k such that $c = e_k(m)$. (If we think of the ciphertexts, plaintexts, and keys as numbers modulo 26, then $e_k(m) \equiv m + k \pmod{26}$, so we have $c = e_k(m)$ if and only if $k \equiv c - m \pmod{26}$.) Hence $f_{C|M}(c \mid m)$ is the probability that the key k is the particular key that encrypts m to c, so $f_{C|M}(c \mid m) = f_K(k) = \frac{1}{26}$, where the last equality comes from the assumption that every key is used with equal probability. Comparing this with (b), we see that $f_C(c) = f_{C|M}(c \mid m)$ for every ciphertext c and plaintext m, hence the system has perfect security.

5.47. Give the details of the proof of (5.47), which says that

$$f_C(c) = \sum_{\substack{k \in \mathcal{K} \text{ such} \\ \text{that } c \in e_k(\mathcal{M})}} f_K(k) f_M\big(d_k(c)\big).$$

(*Hint.* Use the decomposition formula from Exercise 5.23(d)).

Solution to Exercise 5.47.

We compute

$$\begin{aligned} f(c) &= \sum_{k\in\mathcal{K}} f(k) f(c \mid k) && \text{using the decomposition formula, Exer} \\ &= \sum_{k\in\mathcal{K}} f(k) \sum_{m\in\mathcal{M}} f(m) f(c \mid k \text{ and } m) && \text{using the decomposition for} \\ &= \sum_{k\in\mathcal{K}} f(k) \sum_{\substack{m\in\mathcal{M} \\ e_k(m)=c}} f(m). \end{aligned}$$

The last equality follows from the fact that

$$f(c \mid k \text{ and } m) = \begin{cases} 1 & \text{if } c = e_k(m), \\ 0 & \text{if } c \ne e_k(m). \end{cases}$$

Now consider the set

$$S = \bigl\{ m \in \mathcal{M} : e_k(m) = c \bigr\}.$$

If $c \notin e_k(\mathcal{M})$, then it is clear that $S = \emptyset$. On the other hand, if $c \in e_k(\mathcal{M})$, say $c = e_k(m')$, then

$$e_k(d_k(c)) = e_k(d_k(e_k(m'))) = e_k(m') = c,$$

so $d_k(c) \in S$. Conversely, if $m \in S$, then $d_k(c) = d_k(e_k(m)) = m$. This proves that

$$S = \begin{cases} \bigl\{ d_k(c) \bigr\} & \text{if } c \in e_k(\mathcal{M}), \\ \emptyset & \text{if } c \notin e_k(\mathcal{M}). \end{cases}$$

Hence the inner sum in our formula for $f(c)$ equals $f(d_k(c))$ if $c \in e_k(\mathcal{M})$, and it equals 0 otherwise, which gives the desired result.

5.48. 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 5.56. 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 5.48.

Fix $k \in \mathcal{K}$. The encryption map $e_k : \mathcal{M} \to \mathcal{C}$ 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.

5.49. Let $\mathcal{S}_{m,c} = \bigl\{k \in \mathcal{K} : e_k(m) = c\bigr\}$ be the set used during the proof of Theorem 5.56. 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 5.49.

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 $c = c'$.

5.50. 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 5.56. The proof of the other is similar.)

Solution to Exercise 5.50.

A solution for this exercise is not currently available.

5.51. Prove the "only if" part of Theorem 5.56, i.e., prove that if a cryptosystem with an equal number of keys, plaintexts, and ciphertexts satisfies conditions (a) and (b) of Theorem 5.56, then it has perfect secrecy.

Solution to Exercise 5.51.

A solution for this exercise is not currently available.

5.52. Let X_n be a uniformly distributed random variable on n objects, and let $r \geq 1$. Prove directly from Property $\mathbf{H}_3$ of entropy that

$$H(X_{n^r}) = rH(X_n).$$

This generalizes Example 5.58.

Solution to Exercise 5.52.

We view X_{n^r} as choosing an element from $\{x_{i_1 i_2 \cdots i_r} : 1 \leq i_k \leq n\}$. We can do this in two steps, first choosing the initial $r-1$ indices $i_1, \ldots, i_{r-1}$, followed by choosing the last index i_r. Then Property $\mathbf{H}_3$ of entropy gives

$$H(X_{n^r}) = H(X_{n^{r-1}}) + \sum_{i=1}^{n} \frac{1}{n} H(X_n) = H(X_{n^{r-1}}) + H(X_n).$$

Now use induction on r. Notice that this is consistant with the formula $H(X_n) = \log_2(n)$.

5.53. Let X, Y, and $Z_1, \ldots, Z_m$ be random variables as described in Property $\mathbf{H}_3$ on page 270. Let

$$p_i = \Pr(Y = Z_i) \quad \text{and} \quad q_{ij} = \Pr(Z_i = x_{ij}), \quad \text{so} \quad \Pr(X = x_{ij}) = p_i q_{ij}.$$

With this notation, Property $\mathbf{H}_3$ says that

$$H\left((p_i q_{ij})_{\substack{1\le i\le n\\1\le j\le m_i}}\right) = H\Bigl((p_i)_{1\le i\le n}\Bigr) + \sum_{i=1}^{n} p_i H\Bigl((q_{ij})_{1\le j\le m_i}\Bigr).$$

(See Example 5.59.) Then the formula (5.51) for entropy given in Theorem 5.60 implies that

$$\sum_{i=1}^{n}\sum_{j=1}^{m_i} p_i q_{ij}\log_2(p_i q_{ij}) = \sum_{i=1}^{n} p_i \log_2(p_i) + \sum_{i=1}^{n} p_i \sum_{j=1}^{m_i} q_{ij}\log_2(q_{ij}). \qquad (5.8)$$

Prove directly that (5.64) is true. (*Hint.* Remember that the probabilities satisfy $\sum_i p_i = 1$ and $\sum_j q_{ij} = 1$.)

Solution to *Exercise* 5.53.

We compute

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{m_i} p_i q_{ij}\log_2(p_i q_{ij}) &= \sum_{i=1}^{n}\sum_{j=1}^{m_i} p_i q_{ij}\Bigl(\log_2(p_i) + \log_2(q_{ij})\Bigr)\\ &= \sum_{i=1}^{n} p_i\log_2(p_i)\sum_{j=1}^{m_i} q_{ij} + \sum_{i=1}^{n}\sum_{j=1}^{m_i} p_i q_{ij}\log_2(q_{ij})\\ &= \sum_{i=1}^{n} p_i\log_2(p_i) + \sum_{i=1}^{n}\sum_{j=1}^{m_i} p_i q_{ij}\log_2(q_{ij}),\end{aligned}$$

where the last equality follows from the fact that $\sum_j q_{ij} = 1$.

5.54. Let $F(x)$ be a twice differentiable function with the property that $F''(x) < 0$ for all x in its domain. Prove that F is concave in the sense of (5.52). Conclude in particular that the function $F(x) = \log x$ is concave for all $x > 0$.

Solution to *Exercise* 5.54.

We take s and t to be fixed and consider the function

$$G(\alpha) = F\bigl((1-\alpha)s + \alpha t\bigr) - \alpha F(t) - (1-\alpha)F(s).$$

We need to show that $G(\alpha) > 0$ for all $0 \le \alpha \le 1$. We give a proof by contradiction, so we assume that there is some $0 < \beta < 1$ such that $G(\beta) < 0$ and we derive a contradiction.

We first observe that

$$G(0) = G(1) = 0.$$

The assumption that $G(\beta) < 0$ means that the infimum of G on the interval $[0,1]$ is negative, and since $[0,1]$ is compact, we can find a $0 < \gamma < 1$ where G attains its minimum. (The point γ will be in the interior of the interval because, as already noted, we have $G(0) = G(1) = 0$.) In particular, since G has a minimum at γ, we have $G'(\gamma) = 0$.

The extended mean value theorem says that for any (small) $h > 0$ we can write

$$G(\gamma + h) = G(\gamma) + G'(\gamma)h + \frac{1}{2}G''(\delta)h^2 \quad \text{for some } \gamma < \delta < \gamma + h.$$

But since $G(\gamma)$ is the minimum value of G, we have $G(\gamma) \le G(\gamma + h)$, and further $G'(\gamma) = 0$. This leads to the inequality

$$G(\gamma) \le G(\gamma + h) = G(\gamma) + G'(\gamma)h + \frac{1}{2}G''(\delta)h^2. = G(\gamma) + \frac{1}{2}G''(\delta)h^2,$$

which in turn implies that

$$G''(\delta) \ge 0.$$

However, directly from the definition of G we have

$$G''(\delta) = F''\big((1-\delta)s + \delta t\big)(t-s)^2,$$

and the statement of the exercise says that $F''(x) < 0$ for all x, hence $G''(\delta) < 0$. This contradiction completes the proof.

5.55. Use induction to prove Jensen's inequality (Theorem 5.61).

Solution to Exercise 5.55.

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 β_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

$$f(\alpha_1 t_1 + \cdots + \alpha_{n-1} t_{n-1} + \beta_n y_n) \le \alpha_1 f(t_1) + \cdots + \alpha_{n-1} f(t_{n-1}) + \beta_n f(y_n).$$

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 γ and δ satisfy $\gamma + \delta = 1$. Hence the induction hypothesis tells us that

$$f(y_n) = f(\gamma t_n + \delta t_{n+1}) \le \gamma f(t_n) + \delta f(t_{n+1}).$$

Now multiplying both sides by β_n and substituting in the values γ, δ, and β_n yields

$$\beta_n f(y_n) \le \beta_n \gamma f(t_n) + \beta_n \delta f(t_{n+1}) = \alpha_n f(t_n) + \alpha_{n+1} f(t_{n+1}).$$

Finally, substituting this in above gives the desired inequality

$$f(\alpha_1 t_1 + \cdots + \alpha_n t_n + \alpha_{n+1} t_{n+1}) \le \alpha_1 f(t_1) + \cdots + \alpha_n f(t_n) + \alpha_{n+1} f(t_{n+1}).$$

The induction proof that there is equality if and only if all of the t_i's are equal is similar.

5.56. Let X and Y be independent random variables.
(a) Prove that the equivocation $H(X \mid Y)$ is equal to the entropy $H(X)$.
(b) If $H(X \mid Y) = H(X)$, is it necessarily true that X and Y are independent?

Solution to Exercise 5.56.
Independence means that $f(x \mid y) = f(x)$, so

$$\begin{aligned} H(X \mid Y) &= -\sum_{x,y} f(y) f(x \mid y) \log f(x \mid y) \\ &= -\sum_{x,y} f(y) f(x) \log f(x) \\ &= -\sum_{y} f(y) \sum_{x} f(x) \log f(x) \\ &= 1 \cdot H(X). \end{aligned}$$

For the converse, notice that

$$\begin{aligned} H(X) &= -\sum_{x} f(x) \log f(x) \\ &= -\sum_{x} \Bigl(\sum_{y} f(x,y) \Bigr) \log f(x) \\ &= -\sum_{x,y} f(y) f(x \mid y) \log f(x), \end{aligned}$$

so

$$\begin{aligned} H(X) - H(X \mid Y) &= -\sum_{x,y} f(y) f(x \mid y) \log \frac{f(x)}{f(x \mid y)} \\ &= -\sum_{x,y} f(x,y) \log \frac{f(x) f(y)}{f(x,y)}. \end{aligned}$$

It is likely that one could come up with dependent random variables X and Y making this quantity vanish.

5.57. Prove that key equivocation satisfies the formula

$$H(K \mid C) = H(K) + H(M) - H(C)$$

as described in Proposition 5.64.

Solution to Exercise 5.57.

By definition we have

$$H(K \mid C) = -\sum_{k\in\mathcal{K}}\sum_{c\in\mathcal{C}} f_C(c) f_{K|C}(k \mid c) \log_2 f_{K|C}(k \mid c).$$

The conditional probability $f_{K|C}(k \mid c)$ is equal to

$$f_{K|C}(k \mid c) = \frac{f_{K,C}(k,c)}{f_C(c)} = \frac{f_{K,M}\bigl(k, d_k(c)\bigr)}{f_C(c)} = \frac{f_K(k) f_M\bigl(d_k(c)\bigr)}{f_C(c)},$$

where the last equality follows from the fact that K and M are independent. Substituting into the definition of $H(K \mid C)$, we compute

$$\begin{aligned}
H(K \mid C) &= -\sum_{k\in\mathcal{K}}\sum_{c\in\mathcal{C}} f_C(c) f_{K|C}(k \mid c) \log_2 f_{K|C}(k \mid c) \\
&= -\sum_{k\in\mathcal{K}}\sum_{c\in\mathcal{C}} f_K(k) f_M\bigl(d_k(c)\bigr) \log_2 \left(\frac{f_K(k) f_M\bigl(d_k(c)\bigr)}{f_C(c)} \right) \\
&= -\sum_{k\in\mathcal{K}}\sum_{c\in\mathcal{C}} f_K(k) f_M\bigl(d_k(c)\bigr) \log_2 f_K(k) \\
&\qquad - \sum_{k\in\mathcal{K}}\sum_{c\in\mathcal{C}} f_K(k) f_M\bigl(d_k(c)\bigr) \log_2 f_M\bigl(d_k(c)\bigr) \\
&\qquad + \sum_{k\in\mathcal{K}}\sum_{c\in\mathcal{C}} f_K(k) f_M\bigl(d_k(c)\bigr) \log_2 f_C(c) \\
&= -\sum_{k\in\mathcal{K}}\sum_{m\in\mathcal{M}} f_K(k) f_M(m) \log_2 f_K(k) \\
&\qquad - \sum_{k\in\mathcal{K}}\sum_{m\in\mathcal{M}} f_K(k) f_M(m) \log_2 f_M(m) \\
&\qquad + \sum_{k\in\mathcal{K}}\sum_{c\in\mathcal{C}} f_{K,C}(k,c) \log_2 f_C(c) \\
&= -\sum_{k\in\mathcal{K}} f_K(k) \log_2 f_K(k) \sum_{m\in\mathcal{M}} f_M(m) \\
&\qquad - \sum_{m\in\mathcal{M}} f_M(m) \log_2 f_M(m) \sum_{k\in\mathcal{K}} f_K(k) \\
&\qquad + \sum_{c\in\mathcal{C}} \log_2 f_C(c) \sum_{k\in\mathcal{K}} f_{K,C}(k,c)
\end{aligned}$$

$$
\begin{aligned}
&= -\sum_{k\in\mathcal{K}} f_K(k)\log_2 f_K(k)\cdot 1 \\
&\qquad - \sum_{m\in\mathcal{M}} f_M(m)\log_2 f_M(m)\cdot 1 \\
&\qquad + \sum_{c\in\mathcal{C}} \bigl(\log_2 f_C(c)\bigr) f_C(c) \\
&= H(K) + H(M) - H(C).
\end{aligned}
$$

5.58. We continue with the cipher described in Exercise 5.45.

(a) Compute the entropies $H(K)$, $H(M)$, and $H(C)$.

(b) Compute the key equivocation $H(K \mid C)$.

Solution to Exercise 5.58.

(a) We are given that

$$f(k_1) = f(k_2) = f(k_3) = \frac{1}{3},$$

so

$$H(K) = -\frac{1}{3}\log\frac{1}{3} - \frac{1}{3}\log\frac{1}{3} - \frac{1}{3}\log\frac{1}{3} = \log 3 \approx 1.585.$$

We are also given that

$$f(m_1) = f(m_2) = \frac{2}{5}, \qquad f(m_3) = \frac{1}{5},$$

so

$$H(M) = -\frac{2}{5}\log\frac{2}{5} - \frac{2}{5}\log\frac{2}{5} - \frac{1}{5}\log\frac{1}{5} = \log 5 - \frac{4}{5}\log 2 \approx 1.522.$$

Finally, to compute $H(C)$, we use the results of the earlier exercise, which were

$$f(c_1) = \frac{1}{3}, \quad f(c_2) = \frac{4}{15}, \quad f(c_3) = \frac{4}{15}, \quad f(c_4) = \frac{2}{15}.$$

Hence

$$H(C) = -\frac{1}{3}\log\frac{1}{3} - \frac{4}{15}\log\frac{4}{15} - \frac{4}{15}\log\frac{4}{15} - \frac{2}{15}\log\frac{2}{15} \approx 1.088.$$

(b)

$$H(K \mid C) = H(K) + H(M) - H(C) \approx 1.585 + 1.522 - 1.088 = 2.019.$$

5.59. Suppose that the key equivocation of a certain cryptosystem vanishes, i.e., suppose that $H(K \mid C) = 0$. Prove that even a single observed ciphertext uniquely determines which key was used.

Solution to Exercise 5.59.

By definition of equivocation, we have

$$0 = H(K \mid C) = -\sum_{k\in\mathcal{K},\, c\in\mathcal{C}} f(c)f(k \mid c)\log_2 f(k \mid c).$$

The values of the density functions are all between 0 and 1, so every term $f(c)f(k \mid c)\log_2 f(k \mid c)$ in the sum is non-positive (because the two factors in front are non-negative, and the value of the logarithm is non-positive). The only way that a sum of non-positive quantities can equal 0 is for every term in the sum to equal 0. Hence

$$f(c)f(k \mid c)\log_2 f(k \mid c) = 0 \quad \text{for every } k \in \mathcal{K} \text{ and every } c \in \mathcal{C}.$$

Suppose now that we observe some ciphertext c'. This means that $f(c') > 0$, i.e., the ciphertext c' appears with non-zero probability. It follows that for every key k, either

$$f(k \mid c') = 0 \quad \text{or} \quad f(k \mid c') = 1,$$

since the quantity $f(k \mid c')\log_2 f(k \mid c')$ has to vanish. But we also know that

$$\sum_{k\in\mathcal{K}} f(k \mid c') = 1,$$

since some key must have been used. It follows that there is a unique key k' satisfying $f(k' \mid c') = 1$, and for every other key $k \neq k'$ we have $f(k \mid c') = 0$. Hence the single observed ciphertext c' uniquely determines the key.

5.60. 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 5.6.3 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 5.6.3, 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.org/`. 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.org/etext/11`

(b) *Relativity: the Special and General Theory* by Albert Einstein, `http://www.gutenberg.org/etext/5001`

(c) The Old Testament (translated from the original Hebrew, of course!), `http://www.gutenberg.org/etext/1609`

(d) *20000 Lieues Sous Les Mers* (20000 Leagues Under the Sea) by Jules Verne, `http://www.gutenberg.org/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 6

Elliptic Curves and Cryptography

Exercises for Chapter 6

Section. Elliptic curves

6.1. 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 6.1.
(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 $Q \oplus Q \oplus Q = (-237/121, -845/1331)$.

6.2. 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 6.2.
(a) $P + Q = \left(-\frac{8}{9}, -\frac{109}{27}\right)$ and $P - Q = (8, 23)$.
(b) $2P = \left(\frac{137}{64}, -\frac{2651}{512}\right)$ and $2Q = \left(-\frac{64}{25}, \frac{59}{125}\right)$

Bonus. This curve has 16 points with integer coordinates, including one that is quite large. This is somewhat surpising 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.

6.3. 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 6.3.

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

$$e_1 + 2e_2 = 0, \qquad 2e_1e_2 + e_2^2 = A, \qquad e_1e_2^2 = B.$$

So $e_1 = -2e_2$, and substituting this into the second and third equations gives

$$-3e_2^2 = A \qquad \text{and} \qquad -2e_2^3 = B.$$

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

$$\begin{aligned} 4A^3 + 27B^2 = (4e_2^3 + 12e_3e_2^2 + 12e_3^2e_2 + 4e_3^3)e_1^3 &+ (12e_3e_2^3 + 51e_3^2e_2^2 + 12e_3^3e_2)e_1^2 \\ &+ (12e_3^2e_2^3 + 12e_3^3e_2^2)e_1 \\ &+ 4e_3^3e_2^3. \end{aligned}$$

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

$$4A^3 + 27B^2 \quad \text{if and only if} \quad (e_2 - e_3)^2(e_1 - e_3)^2(e_1 - e_2)^2 = 0,$$

6.4. Sketch each of the following curves, as was done in Figure 6.1 on page 302.
(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

6.5. 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 6.5.
(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) $\#E(\mathbb{F}_{13}) = 9$

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (4,1), (4,12), (8,2), (8,11), (9,3), (9,10), (10,4), (10,9)\}$$

6.6. Make an addition table for E over $\mathbb{F}_p$, as we did in Table 6.1.
(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 6.6.
(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) $E(\mathbb{F}_{11}) = \{\mathcal{O}, (0,4), (0,7), (3,4), (3,7), (4,0), (8,4), (8,7), (9,2), (9,9)\}$.

	$\mathcal{O}$	$(0,4)$	$(0,7)$	$(3,4)$	$(3,7)$	$(4,0)$	$(8,4)$	$(8,7)$	$(9,2)$	$(9,9)$
$\mathcal{O}$	$\mathcal{O}$	$(0,4)$	$(0,7)$	$(3,4)$	$(3,7)$	$(4,0)$	$(8,4)$	$(8,7)$	$(9,2)$	$(9,9)$
$(0,4)$	$(0,4)$	$(9,2)$	$\mathcal{O}$	$(8,7)$	$(9,9)$	$(8,4)$	$(3,7)$	$(4,0)$	$(3,4)$	$(0,7)$
$(0,7)$	$(0,7)$	$\mathcal{O}$	$(9,9)$	$(9,2)$	$(8,4)$	$(8,7)$	$(4,0)$	$(3,4)$	$(0,4)$	$(3,7)$
$(3,4)$	$(3,4)$	$(8,7)$	$(9,2)$	$(8,4)$	$\mathcal{O}$	$(9,9)$	$(0,7)$	$(3,7)$	$(4,0)$	$(0,4)$
$(3,7)$	$(3,7)$	$(9,9)$	$(8,4)$	$\mathcal{O}$	$(8,7)$	$(9,2)$	$(3,4)$	$(0,4)$	$(0,7)$	$(4,0)$
$(4,0)$	$(4,0)$	$(8,4)$	$(8,7)$	$(9,9)$	$(9,2)$	$\mathcal{O}$	$(0,4)$	$(0,7)$	$(3,7)$	$(3,4)$
$(8,4)$	$(8,4)$	$(3,7)$	$(4,0)$	$(0,7)$	$(3,4)$	$(0,4)$	$(9,2)$	$\mathcal{O}$	$(9,9)$	$(8,7)$
$(8,7)$	$(8,7)$	$(4,0)$	$(3,4)$	$(3,7)$	$(0,4)$	$(0,7)$	$\mathcal{O}$	$(9,9)$	$(8,4)$	$(9,2)$
$(9,2)$	$(9,2)$	$(3,4)$	$(0,4)$	$(4,0)$	$(0,7)$	$(3,7)$	$(9,9)$	$(8,4)$	$(8,7)$	$\mathcal{O}$
$(9,9)$	$(9,9)$	$(0,7)$	$(3,7)$	$(0,4)$	$(4,0)$	$(3,4)$	$(8,7)$	$(9,2)$	$\mathcal{O}$	$(8,4)$

6.7. 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 6.7.

p	$\#E(F_p)$	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

6.8. 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 6.8.

We compute the multiples of P:

$$P = (4,2), \quad 2P = (3,4), \quad 3P = (2,4), \quad 4P = (0,4), \quad \boxed{5P = (0,1)}$$
$$6P = (2,1), \quad 7P = (3,1), \quad 8P = (4,3), \quad 9P = \mathcal{O}.$$

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.

6.9. 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 $0 \le r < s$ and determine the value of r.)

Solution to Exercise 6.9.

Following the hint, we write n as $n = is + r$ for some $0 \le r < s$. 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 $r \ge n_0$. 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 $n = is + n_0$.

6.10. Let $\{P_1, P_2\}$ be a basis for $E[m]$. The *Basis Problem* for $\{P_1, P_2\}$ is to express an arbitrary point $P \in E[m]$ as a linear combination of the basis vectors, i.e., to find n_1 and n_2 so that $P = n_1P_1 + n_2P_2$. Prove that an algorithm that solves the basis problem for $\{P_1, P_2\}$ can be used to solve the ECDLP for points in $E[m]$.

Solution to *Exercise* 6.10.

Suppose that $P, Q \in E[m]$ are given, and suppose further that $Q = kP$. We may assume that P has order m, since if not, then we can replace m with the order of P. (In any case, the value of k is only well-defined modulo the order of P.) We need to find k. Since we can solve the basis problem, we can find n_1, n_2, s_1, s_2 such that

$$P = n_1P_1 + n_2P_2 \quad \text{and} \quad Q = s_1Q_1 + s_2Q_2.$$

From $Q = kP$ we see that

$$(s_1 - kn_1)P_1 + (s_2 - kn_2)P_2 = 0.$$

But $\{P_1, P_2\}$ is a basis for $E[m]$, which means that $a_1P_1 + a_2P_2 = 0$ if and only if $a_1 \equiv a_2 \equiv 0 \pmod{m}$. Therefore

$$kn_1 \equiv s_1 \pmod{m} \quad \text{and} \quad kn_2 \equiv s_2 \pmod{m}.$$

Notice that if $\gcd(n_1, m) = 1$ or $\gcd(n_2, m) = 1$, we can immediately solve for k.

In general, we need to do a bit more work. We first prove that $\gcd(n_1, n_2, m) = 1$. To see this, let $d = \gcd(n_1, n_2, m)$. Then

$$\frac{m}{d}P = \frac{m}{d}(n_1P_1 + n_2P_2) = \frac{n_1}{d} \cdot mP_1 + \frac{n_2}{d} \cdot mP_2 = \mathcal{O}.$$

(Note that n_1/d and n_2/d are integers, and P_1 and P_2 have order m.) But we are assuming that P has order m, hence $d = 1$.

The fact that $\gcd(n_1, n_2, m) = 1$ means that we can find integers u, v, w such that

$$un_1 + vn_2 + wm = 1.$$

Note that since we know n_1 and n_2, we can actually compute u, v, w using the extending Euclidean algorithm. We have $un_1 + vn_2 \equiv 1 \pmod{m}$. Multipying by k, we find from above that

$$k \equiv ukn_1 + vkn_2 \equiv us_1 + vs_2 \pmod{m}.$$

But we also know s_1 and s_2, so we have computed k.

6.11. Use the double-and-add algorithm (Table 6.3) to compute nP in $E(\mathbb{F}_p)$ for each of the following curves and points, as we did in Figure 6.4.

(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 6.11.

(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

6.12. Convert the proof of Proposition 6.18 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 $\frac{1}{2}\lfloor \log n \rfloor + 1$ 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 6.12.

(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.

$$\begin{aligned} 8379483273489 &= +2^1 + 2^5 + 2^9 + 2^{12} + 2^{13} + 2^{14} + 2^{16} + 2^{17} + 2^{18} + 2^{19} \\ &\quad + 2^{20} + 2^{21} + 2^{33} + 2^{34} + 2^{35} + 2^{36} + 2^{37} + 2^{40} + 2^{41} \\ &\quad + 2^{42} + 2^{43} \\ &= +2^1 + 2^5 + 2^9 - 2^{12} - 2^{15} + 2^{22} - 2^{33} + 2^{38} - 2^{40} + 2^{44} \end{aligned}$$

6.13. In Section 5.5 we gave an abstract description of Pollard's ρ method, and in Section 5.5.2 we gave an explicit version to solve the discrete logarithm problem in $\mathbb{F}_p$. Adapt this material to create a Pollard ρ algorithm to solve the ECDLP.

Solution to Exercise 6.13.

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 $f : E(\mathbb{F}_p) \to E(\mathbb{F}_p)$ that mixes up the points reasonably well. Following the ideas from Section 5.5.2, we define

$$f : E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_p), \qquad f(T) = \begin{cases} P + T & \text{if } 0 \le x_T < p/3, \\ 2T & \text{if } p/3 \le x_T < 2p/3, \\ Q + T & \text{if } 2p/3 \le x_T < p. \end{cases}$$

Then after i steps, we have

$$f^i(\mathcal{O}) = \alpha_i P + \beta_i Q \qquad \text{and} \qquad f^{2i}(\mathcal{O}) = \gamma_i P + \delta_i Q$$

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 5.5.2. 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

$$(\alpha_i - \gamma_i)P = (\delta_i - \beta_i)Q \qquad \text{in } E(\mathbb{F}_p).$$

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 5.5.2 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

6.14. Alice and Bob agree to use elliptic Diffie–Hellman key exchange with the prime, elliptic curve, and point

$$p = 2671, \qquad E : Y^2 = X^3 + 171X + 853, \qquad P = (1980, 431) \in E(\mathbb{F}_{2671}).$$

(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* 6.14.

(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 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 $\boxed{x = 1708}$.

6.15. Exercise 2.10 on page 109 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* 6.15.

A solution for this exercise is not currently available.

6.16. 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 6.4.2, 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

$$\beta_R = \begin{cases} 0 & \text{if } 0 \le y_R < \frac{1}{2}p, \\ 1 & \text{if } \frac{1}{2}p < y_R < p. \end{cases}$$

(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 2.26.)

(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 6.16.

(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 β_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 β is chosen, we have

$$\boxed{\beta = 0 \Longrightarrow R = (278, 487)} \quad \text{and} \quad \boxed{\beta = 1 \Longrightarrow R = (278, 636)}$$

6.17. 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 6.13 on page 367.

(a) The last line of Table 6.13 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

$$p = 1201, \qquad E : Y^2 = X^3 + 19X + 17, \qquad P = (278, 285) \in E(\mathbb{F}_p),$$

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 6.17.

(a) Suppose that Bob has encrypted the plaintext (m_1, m_2) using the random number k as described in Table 6.13 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 $\boxed{\text{2-to-1}}$. 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 $\boxed{\text{3-to-2}}$.

(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 $\boxed{(509, 767)}$.

6.18. This exercise continues the discussion of the MV-Elgamal cryptosystem described in Table 6.13 on page 367.

(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 6.17(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.

<u>Solution to Exercise 6.18</u>.

(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

$$\begin{aligned} x_S &\equiv m_1^{-1} c_1 \pmod{p}, \\ y_S &\equiv m_2^{-1} c_2 \pmod{p}, \end{aligned}$$

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 $m_1^3 m_2^2$, so

$$c_2^2 m_1^3 \equiv c_1^3 m_2^2 + A c_1 m_1^2 m_2^2 + B m_1^3 m_2^2 \pmod{p}.$$

Thus (m_1, m_2) is a solution to the congruence

$$c_2^2 u^3 \equiv c_1^3 v^2 + A c_1 u^2 v^2 + B u^3 v^2 \pmod{p},$$

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.*

6.19. Section 6.4.3 describes ECDSA, an elliptic analogue of DSA. Formulate an elliptic analogue of the simpler Elgamal digital signature algorithm described in Table 4.2 in Section 4.3.

Solution to Exercise 6.19.
A solution for this exercise is not currently available.

6.20. This exercise asks you to compute some numerical instances of the elliptic curve digital signature algorithm described in Table 6.7 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 $E(\mathbb{F}_p)$.
(a) 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 random element $e = 847$?
(b) Tabitha's public verification key is $V = (11017, 14637)$. Is $(s_1, s_2) = (907, 296)$ a valid signature on the document $d = 993$?
(c) 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 random element $e = 365$.

Solution to Exercise 6.20.
(a) Samantha's public verification key is

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 6.1: Menezes–Vanstone variant of Elgamal (Exercises 6.17, 6.18)

$$V = 542(11259, 11278) = (8689, 1726) \in E(\mathbb{F}_p).$$

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

$$v_1 \equiv ds_2^{-1} \equiv 106 \pmod q \quad \text{and} \quad v_2 \equiv s_1 s_2^{-1} \equiv 311 \pmod q.$$

Then $v_1 G + v_2 V = (8833, 4526) \in E(\mathbb{F}_p)$, and

$$x(v_1 G + v_2 V) \bmod q = 8833 \bmod 1321 = 907$$

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 random element $e = 365$ 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. Lenstra's elliptic curve factorization algorithm

6.21. 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 6.21.
(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	$6! \cdot P = (7881, 16198)$

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 $\mathbb{F}_{2^k}$

6.22. 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 λ and ν as follows:

$$[\text{If } x_1 \neq x_2] \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1},$$

$$[\text{If } x_1 = x_2] \quad \lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

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* 6.22.

This is proven in any basic text on elliptic curves. See for example Group Law Algorithm 2.3 in [137, §2.2].

6.23. Let $\mathbb{F}_8 = \mathbb{F}_2[T]/(T^3 + T + 1)$ be as in Example 6.28, 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* 6.23.

(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 $\#E(\mathbb{F}_8)$.

6.24. Let $\tau(\alpha) = \alpha^p$ be the Frobenius map on $\mathbb{F}_{p^k}$.

(a) Prove that

$$\tau(\alpha{+}\beta) = \tau(\alpha){+}\tau(\beta) \qquad \text{and} \qquad \tau(\alpha{\cdot}\beta) = \tau(\alpha){\cdot}\tau(\beta) \qquad \text{for all } \alpha, \beta \in \mathbb{F}_{p^k}.$$

(*Hint.* For the addition formula, use the binomial theorem (Theorem 5.10).)

(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

$$\tau(P+Q) = \tau(P) + \tau(Q) \quad \text{for all } P \in E(\mathbb{F}_{p^k}).$$

6.25. 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

$$t_k = t_1 t_{k-1} - 2t_{k-2} \qquad \text{for all } k \geq 3.$$

(You may use the formula (6.12) that we stated, but did not prove, on page 336.)

(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 $\#E(\mathbb{F}_{2^{101}})$.

<u>*Solution to Exercise* 6.25</u>.

(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) $\#E(\mathbb{F}_{2^{11}}) = 2116$.

$\#E(\mathbb{F}_{2^{31}}) = 2147574356$.

$\#E(\mathbb{F}_{2^{101}}) = 2535301200456455833701195805484$.

6.26. Let E be an elliptic curve over $\mathbb{F}_p$, and for $k \geq 1$, let

$$t_k = p^k + 1 - \#E(\mathbb{F}_{p^k}).$$

(a) Prove that

$$t_k = t_1 t_{k-1} - p t_{k-2} \qquad \text{for all } k \geq 2,$$

where by convention we set $t_0 = 2$.

(b) Use (a) to express t_2, t_3, and t_4 in terms of p and t_1.

(*Hint.* Use Theroem 6.29(a). This generalizes Exercise 6.25.)

<u>*Solution to Exercise* 6.26</u>.

(a) The theorem says that $t_k = \alpha^k + \beta^k$, where α and β are the roots of $Z^2 - t_1 Z + p$. So in particular, we have $\alpha + \beta = t_1$ and $\alpha\beta = p$. (Note that this formula is also true for $k = 0$ according to our convention that $t_0 = 2$.) Using these formulas we compute

$$\begin{aligned} t_1 t_{k-1} - p t_{k-2} &= (\alpha+\beta)(\alpha^{k-1} + \beta^{k-1}) - \alpha\beta(\alpha^{k-2} + \beta^{k-2}) \\ &= \alpha^k + \beta^k \\ &= t_k. \end{aligned}$$

(b) Using the recursion, we find that

$$t_2 = t_1^2 - pt_0 = t_1^2 - 2p.$$
$$t_3 = t_1t_2 - pt_1 = t_1^3 - 3pt_1.$$
$$t_4 = t_1t_3 - pt_2 = (t_1^4 - 3pt_1^2) - p(t_1^2 - 2p) = t_1^4 - 4pt_1^2 + 2p.$$

6.27. Let τ 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

$$n = v_0 + v_1\tau + v_2\tau^2 + \cdots + v_\ell\tau^\ell. \tag{6.1}$$

Further prove that $\ell \le 2\lceil\log(n)\rceil + 1$.

```
Set $n_0 = n$ and $n_1 = 0$ and $i = 0$
Loop while $n_0 \ne 0$ or $n_1 \ne 0$
    If $n_0$ is odd
        Set $v_i = 2 - \big((n_0 - 2n_1) \bmod 4\big)$
        Set $n_0 = n_0 - v_i$
    Else
        Set $v_i = 0$
    End If
    Set $i = i + 1$
    Set $(n_0, n_1) = \big(n_1 - \frac{1}{2}n_0, -\frac{1}{2}n_0\big)$
End Loop
```

Solution to Exercise 6.27.

A solution for this exercise is not currently available.

6.28. Implement the algorithm in Exercise 6.27 and use it to compute the τ-expansion (6.19) of the following integers. What is the highest power of τ that appears and how many nonzero terms are there?

(a) $n = 931$ (b) $n = 32755$ (c) $n = 82793729188$

Solution to Exercise 6.28.

(a)

$$931 = -1 + \tau^2 + \tau^{10} + \tau^{14} - \tau^{17} - \tau^{19} - \tau^{21}.$$

The highest power of τ is τ^{21} and the τ-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 τ is τ^{31} and the τ-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 τ is τ^{73} and the τ-expansion has 24 nonzero terms.

Section. Bilinear pairings on elliptic curves

6.29. Let $R(x)$ and $S(x)$ be rational functions. Prove that the divisor of a product is the sum of the divisors, i.e.,

$$\operatorname{div}\bigl(R(x)S(x)\bigr) = \operatorname{div}\bigl(R(x)\bigr) + \operatorname{div}\bigl(S(x)\bigr).$$

6.30. This exercise sketches a proof that if $P = (\alpha, 0) \in E$, then $\operatorname{div}(X-\alpha) = 2[P] - 2[\mathcal{O}]$.

(a) Prove that

$$\operatorname{div}(X-\alpha) = m[P] - m[O]$$

for some integer $m \geq 1$.

(b) Prove that the Weierstrass equation of E can be written in the form

$$E : Y^2 = (X-\alpha)(X^2 + aX + b),$$

and that the polynomials of $X - \alpha$ and $X^2 + aX + b$ have no common roots.

(c) Prove that

$$\operatorname{div}(X-\alpha) = 2n[P] - 2n[O]$$

for some integer $n \geq 1$. (*Hint.* Take the divisor of both sides of $Y^2 = (X-\alpha)(X^2 + aX + b)$ and use (b).)

(d) Prove that

$$\operatorname{div}(X-\alpha) = 2[P] - 2[O].$$

(*Warning.* This part requires some knowledge of discrete valuation rings that is not developed in this book.)

<u>*Solution to Exercise* 6.30</u>.

(a) The only zero of $X - \alpha$ is P, and the only possible pole is $\mathcal{O}$. Hence $\operatorname{div}(X-\alpha) = m_1[P] + m_2[\mathcal{O}]$, and since $\operatorname{div}(X-\alpha)$ has degree 0 (this is true for any divisor of a rational function), we have $m_2 = -m_1$. Hence $\operatorname{div}(X-\alpha) = m[P] - m[\mathcal{O}]$.

(b) The fact that $(\alpha, 0) \in E$ means that α is a root of $X^3 + AX + B$, so $X^3 + AX + B$ factors as $(X-\alpha)(X^2 + aX + b)$. The nonsingularity of E says that the roots of $X^3 + AX + B$ are distinct, so $X - \alpha$ and $X^2 + aX + b$ have no common roots.

(c) We have

$$\begin{aligned} 2\operatorname{div}(Y) &= \operatorname{div}(X-\alpha) + \operatorname{div}(X^2+aX+b) \\ &= m[P] - m[\mathcal{O}] + \operatorname{div}(X^2+aX+b). \end{aligned}$$

It follows from (b) that $[P]$ does not appear in $\operatorname{div}(X^2+aX+b)$, so m must be even.

(d) We first prove that Y is a local uniformizer at P, i.e., it vanishes to order 1 at P. To do that, we consider the local ring at P, which is the ring

$$R = \left\{ \frac{f(X,Y)}{g(X,Y)} : Y^2 = X^3+AX+B \text{ and } g(\alpha,0) \neq 0 \right\}.$$

In other words, we take all rational functions whose denominator does not vanish at P. This is a discrete valuation ring whose maximal ideal is generated by $X-\alpha$ and Y. But since

$$X-\alpha = \frac{Y^2}{X^2+aX+b} \quad \text{and} \quad X^2+aX+b \text{ does not vanish at } P,$$

we see that $X-\alpha$ is already in the ideal of R generated by Y, so Y is a uniformizer. This means that $\operatorname{ord}_P(Y) = 1$. Further, the formula $X-\alpha = \frac{Y^2}{X^2+aX+b}$ shows that $X-\alpha$ generates the same ideal as Y^2, so

$$\operatorname{ord}_P(X-\alpha) = 2\operatorname{ord}_P(Y) = 2.$$

Hence $\operatorname{div}(X-\alpha)$ contains the term $2[P]$, and using (a), we conclude that $\operatorname{div}(X-\alpha) = 2[P] - 2[\mathcal{O}]$.

6.31. Prove that the Weil pairing satisfies

$$e_m(P,Q) = e_m(Q,P)^{-1} \qquad \text{for all } P,Q, \in E[m].$$

(*Hint.* Use the fact that $e_m(P+Q,P+Q) = 1$ and expand using bilinearity.)

Solution to Exercise 6.31.

A solution for this exercise is not currently available.

6.32. 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.

6.33. 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 6.39.) Use the basic properties of the Weil pairing described in Theorem 6.38 to prove that

$$e_m(P,Q) = e_m(P_1,P_2)^{\det\left(\begin{smallmatrix} a_P & a_Q \\ b_P & b_Q \end{smallmatrix}\right)} = e_m(P_1,P_2)^{a_P b_Q - a_Q b_P}.$$

6.34. Complete the proof of Proposition 6.52 by proving that $\phi(2P) = 2\phi(P)$.

6.35. 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 6.43.)

	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 6.35.

(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 $Q' = 3Q$.

6.36. Let E over $\mathbb{F}_q$ and ℓ be as described in Theorem 6.44. Prove that the modified Tate pairing is symmetric, in the sense that

$$\hat{\tau}(P,Q) = \hat{\tau}(Q,P) \qquad \text{for all } P,Q \in E(\mathbb{F}_q)[\ell].$$

Solution to Exercise 6.36.

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

$$\hat{\tau}(P,Q) = \hat{\tau}(uT,vT) = \hat{\tau}(T,T)^{uv},$$
$$\hat{\tau}(Q,P) = \hat{\tau}(vT,uT) = \hat{\tau}(T,T)^{vu},$$

which are clearly the same value.

6.37. 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 consistantly. 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

6.38. Prove Proposition 6.52(b) in the case $P_1 = P_2$.

6.39. Let E be an elliptic curve over $\mathbb{F}_p$ and let ℓ be a prime. Suppose that $E(\mathbb{F}_p)$ contains a point of order ℓ and that $\ell > \sqrt{p} + 1$. Prove that $E(\mathbb{F}_p)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$.

Solution to Exercise 6.39.

Hasse's theorem says that

$$\#E(\mathbb{F}_p) \le p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2.$$

The assumption on ℓ 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 ℓ^2 elements, contradicting $\#E(\mathbb{F}_p) < \ell^2$.

6.40. Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and let ℓ 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 ϕ 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 6.40.

Compute

$$\hat{e}_\ell(aP, bP) = \hat{e}_\ell(P, P)^{ab} \qquad \text{and} \qquad \hat{e}_\ell(P, cP) = \hat{e}_\ell(P, P)^{c}.$$

If they agree, then $cP = abP$, otherwise $cP \ne abP$.

6.41. 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 6.52. Prove that $\phi(\phi(P)) = -P$ for all $P \in E$. (Intuitively, ϕ behaves like multiplication by $\sqrt{-1}$ when it is applied to points of E.)

Solution to Exercise 6.41.

Let $P = (x, y)$. We compute

$$\phi(\phi(P)) = \phi(-x, \alpha y) = \bigl(-(-x), \alpha \cdot \alpha y\bigr) = (x, \alpha^2 y) = (x, -y) = -P.$$

6.42. 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 ℓ-distortion map for P described in Proposition 6.53. Suppose further that $\ell \equiv 3 \pmod 4$. Prove that ϕ is an ℓ-distortion map for every point in $E[\ell]$. In other words, if $Q \in E$ is any point of order ℓ, prove that $e_\ell(Q, \phi(Q))$ is a primitive ℓ^{th} root of unity.

Solution to Exercise 6.42.

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 ℓ^{th}-root of unity, so either $e_\ell(Q, \phi(Q))$ is a primitive ℓ^{th}-root of unity, or else $a^2 + b^2$ is a multiple of ℓ. (Note that we can assume that take $0 \le a, b < \ell$ and that a and b are not both 0.) But if ℓ 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 ℓ. From an easy piece of quadratic reciprocity, this implies that $\ell \equiv 1 \pmod 4$, contradicting our assumption that $\ell \equiv 3 \pmod 4$.

6.43. Let E be the elliptic curve

$$E : y^2 = x^3 + 1$$

over a field K, and suppose that K contains an element $\beta \ne 1$ satisfying $\beta^3 = 1$. (We say that β is a *primitive cube root of unity.*) Define a map ϕ 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 ϕ respects the addition law on E, i.e., $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$ for all $P_1, P_2 \in E(K)$.

6.44. Let $E : y^2 = x^3 + 1$ be the elliptic curve in Exercise 6.43.

(a) Let $p \ge 3$ 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 6.43. Suppose that $E(\mathbb{F}_p)$ contains a point P of prime order $\ell \ge 5$. Prove that ϕ is an ℓ-distortion map for P.

Solution to Exercise 6.44.

(b) This is the same as the proof of Proposition 6.53. The multiples of P are in $E(\mathbb{F}_p)$, but $\phi(P)$ is not unless its x-coordinate is 0. Then on 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 6.50 tells us that $e_\ell(P, \phi(P))$ is a primitive ℓ^{th}-root of unity.

6.45. 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 Exercise 6.42 to compute $\hat{e}_{173}(P, P)$ (cf. Example 6.55). Verify that the value is a primitive 173^{rd} root of unity.

Solution to Exercise 6.45.

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 $(242 + 92i)^{173} = 1$.

6.46. Continuing with the curve E, prime $p = 691$, and point $P = (301, 14)$ from Exercise 6.45, 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^{th} power of $\hat{e}_{173}(P, P)$. Check your answer by verifying that nP is equal to Q.

Solution to Exercise 6.46.

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

6.47. 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 6.47.
(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, $\hat{e}_{431}(Q_A, Q_B)^{145} = (977 + 1163i)^{145} = 68 + 428i$.

6.48. Show that Eve can break tripartite Diffie–Hellman key exchange as described in Table 6.10.1 if she knows how to solve the Diffie–Hellman problem (page 69) for the field $\mathbb{F}_q$.

Solution to Exercise 6.48.
Eve can compute

$$\hat{e}_\ell(P, P) \qquad \text{and} \qquad \hat{e}_\ell(Q_A, P) = \hat{e}_\ell(n_A P, P) = \hat{e}_\ell(P, P)^{n_A}.$$

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

$$g^{n_A} \qquad \text{and} \qquad g^{n_B n_C}$$

for a certain primitive ℓ^{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 $g^{n_A n_B n_C}$.

6.49. In this exercise we consider what is required to break the identity-based encryption scheme described in Table 6.12 on page 362.

(a) Show that if Eve can solve the discrete logarithm problem in either $E(\mathbb{F}_q)$ or in $\mathbb{F}_q^*$, then she can recover Tom's secret key s, which means that she can do anything that Tom can do, including decrypting everyone's ciphtertexts.

(b) Suppose that Eve only knows how to solve the elliptic curve Diffie–Hellman problem in $E(\mathbb{F}_q)$, as described on page 320. Show that she can decrypt all ciphertexts.

(c) What if Eve only knows how to solve the Diffie–Hellman problem in $\mathbb{F}_q^*$. Can she still decrypt all ciphertexts?

Solution to Exercise 6.49.

(a) Eve knows P and $P^{\mathsf{Tom}} = sP$, so if she can solve the ECDLP, she can recover s. On the other hand, if she can only solve the DLP, she simply computes $a = \hat{e}_\ell(P,P)$ and $b = \hat{e}_\ell(P,P^{\mathsf{Tom}}) = \hat{e}_\ell(P,P)^s$ and solve the DLP $a^x = b$ in $\mathbb{F}_q^*$ to recover s.

(b, c)These is a little trickier, because as far as we know, Eve can't actually determine Tom's secret key s or the random element r. However, we note that in order to decrypt Bob's message, it's enough for Eve to compute $\hat{e}_\ell(P^{\mathsf{Alice}},P^{\mathsf{Tom}})^r$, since then she can recover M by computing

$$M = C_2 \;\mathsf{xor}\; H_2\bigl(\hat{e}_\ell(P^{\mathsf{Alice}},P^{\mathsf{Tom}})^r\bigr).$$

The difficulty is that $\hat{e}_\ell(P^{\mathsf{Alice}},P^{\mathsf{Tom}})^r$ involves the random element r, which Eve does not know. But we will show that if Eve can solve eithter the ECDHP or the DHP, then she can compute $\hat{e}_\ell(P^{\mathsf{Alice}},P^{\mathsf{Tom}})^r$ without knowing r.

Suppose first that Eve can solve the ECDHP. She knows $C_1 = rP$ and $P^{\mathsf{Tom}} = sP$, so solving the ECDHP allows her to compute rsP. Then she can compute

$$\hat{e}_\ell(P^{\mathsf{Alice}},rsP) = \hat{e}_\ell(P^{\mathsf{Alice}},sP)^r = \hat{e}_\ell(P^{\mathsf{Alice}},P^{\mathsf{Tom}})^r.$$

This solves (b).

Next suppose that Eve only knows how to solve the DLP in $\mathbb{F}_q^*$. Eve knows that values of

$$\begin{aligned} e(P^{\mathsf{Alice}},C_1) &= e(P^{\mathsf{Alice}},rP) = e(P^{\mathsf{Alice}},P)^r,\\ e(P^{\mathsf{Alice}},P^{\mathsf{Tom}}) &= e(P^{\mathsf{Alice}},sP) = e(P^{\mathsf{Alice}},P)^s, \end{aligned}$$

so solving the Diffie–Hellman problem for $e(P^{\mathsf{Alice}},P)^r$ and $e(P^{\mathsf{Alice}},P)^s$ allows Eve to compute

$$e(P^{\mathsf{Alice}},P)^{rs} = e(P^{\mathsf{Alice}},sP)^r = e(P^{\mathsf{Alice}},P^{\mathsf{Tom}})^r.$$

This solves (c).

Chapter 7

Lattices and Cryptography

Exercises for Chapter 7

Section. A congruential public key cryptosystem

7.1. 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 random element $r = 19564$. What is the ciphertext that Bob sends to Alice?

Solution to Exercise 7.1.
(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 random element was 19564.)
(c)

$$e \equiv rh + m \equiv 619167208 \pmod{q}.$$

Section. Subset-sum problems and knapsack cryptosystems

7.2. Use the algorithm described in Proposition 7.5 to solve each of the following subset-sum problems. If the "solution" that you get is not correct, explain what went wrong.
(a) $\boldsymbol{M} = (3, 7, 19, 43, 89, 195), \quad S = 260.$

(b) $\boldsymbol{M} = (5, 11, 25, 61, 125, 261), \quad S = 408.$
(c) $\boldsymbol{M} = (2, 5, 12, 28, 60, 131, 257), \quad S = 334.$
(d) $\boldsymbol{M} = (4, 12, 15, 36, 75, 162), \quad S = 214.$

Solution to Exercise 7.2.

(a) Output from algorithm is $\boldsymbol{x} = (1, 0, 1, 1, 0, 1)$. Sum is correct.
(b) Output from algorithm is $\boldsymbol{x} = (1, 1, 0, 0, 1, 1)$. Sum is 402 instead of 408. Incorrect. Superincreasing, but this S has no solution.
(c) Output from algorithm is $\boldsymbol{x} = (0, 1, 1, 0, 1, 0, 1)$. Sum is correct.
(d) Output from algorithm is $\boldsymbol{x} = (0, 0, 1, 1, 0, 1)$. Sum is 213 instead of 214. Incorrect. $\boldsymbol{M}$ is not superincreasing, this problem has a solution $(1, 1, 0, 1, 0, 1)$, but it is not found by the algorithm.

7.3. Alice's public key for a knapsack cryptosystem is

$$\boldsymbol{M} = (5186, 2779, 5955, 2307, 6599, 6771, 6296, 7306, 4115, 637).$$

Eve intercepts the encrypted message $S = 4398$. 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 $\boldsymbol{r}$ and then decrypt the message.

Solution to Exercise 7.3.

First we compute $A^{-1} \equiv 2683 \pmod{B}$. Then

$$A^{-1} \cdot \boldsymbol{M} \equiv (5, 14, 30, 75, 160, 351, 750, 1579, 3253, 6510) \pmod{B}.$$

Finally, we to write $S = 4398$ as a sum of elements from this set,

$$S = 4398 = 3253 + 750 + 351 + 30 + 14.$$

7.4. Proposition 7.3 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 ρ algorithm (Section 5.5), that takes $\mathcal{O}(2^{n/2})$ steps, but requires only $\mathcal{O}(1)$ storage.

Solution to Exercise 7.4.

A solution for this exercise is not currently available.

Section. A brief review of vector spaces

7.5. (a) Let

$$\mathcal{B} = \{(1, 3, 2), (2, -1, 3), (1, 0, 2)\}, \qquad \mathcal{B}' = \{(-1, 0, 2), (3, 1, -1), (1, 0, 1)\}.$$

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 $\boldsymbol{v} = (2, 3, 1)$ and $\boldsymbol{w} = (-1, 4, -2)$. Compute the lengths $\|\boldsymbol{v}\|$ and $\|\boldsymbol{w}\|$ and the dot product $\boldsymbol{v} \cdot \boldsymbol{w}$. Compute the angle between $\boldsymbol{v}$ and $\boldsymbol{w}$.

Solution to Exercise 7.5.

(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) $\|\boldsymbol{v}\| = \sqrt{14} \approx 3.7417$. $\|\boldsymbol{w}\| = \sqrt{21} \approx 4.5826$. $\boldsymbol{v} \cdot \boldsymbol{w} = 8$.

$$\cos(\theta) = 8/\sqrt{14} \cdot \sqrt{21} \approx 0.4666, \text{ so}$$
$$\theta \approx \cos^{-1}(0.4666) \approx 1.0854 \text{ radians} \approx 62.188 \text{ degrees.}$$

7.6. Use the Gram–Schmidt algorithm (Theorem 7.13) to find an orthogonal basis from the given basis.

(a) $\boldsymbol{v}_1 = (1, 3, 2)$, $\boldsymbol{v}_2 = (4, 1, -2)$, $\boldsymbol{v}_3 = (-2, 1, 3)$.

(b) $\boldsymbol{v}_1 = (4, 1, 3, -1)$, $\boldsymbol{v}_2 = (2, 1, -3, 4)$, $\boldsymbol{v}_3 = (1, 0, -2, 7)$.

Solution to Exercise 7.6.

(a)

$$\boldsymbol{v}_1^* = (1, 3, 2), \quad \boldsymbol{v}_2^* = (53/14, 5/14, -17/7), \quad \boldsymbol{v}_3^* = (56/285, -14/57, 77/285).$$

(b)

$$\boldsymbol{v}_1^* = (4, 1, 3, -1), \quad \boldsymbol{v}_2^* = (70/27, 31/27, -23/9, 104/27),$$
$$\boldsymbol{v}_3^* = (-287/397, -405/397, 799/397, 844/397).$$

Section. Lattices: Basic definitions and properties

7.7. 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 7.7.

The volume is

$$\left| \det \begin{pmatrix} 1 & 3 & -2 \\ 2 & 1 & 0 \\ -1 & 2 & 5 \end{pmatrix} \right| = 35.$$

7.8. Let $L \subset \mathbb{R}^m$ be an additive subgroup with the property that there is a positive constant $\epsilon > 0$ such that

$$L \cap \{\boldsymbol{w} \in \mathbb{R}^m : \|\boldsymbol{w}\| < \epsilon\} = \{\boldsymbol{0}\}.$$

Prove that L is discrete, and hence is a lattice. (In other words, show that in the defintion of discrete subgroup, it suffices to check that (7.8) is true for the single vector $\boldsymbol{v} = \boldsymbol{0}$.)

Solution to Exercise 7.8.

A solution for this exercise is not currently available.

7.9. Prove that a subset of $\mathbb{R}^m$ is a lattice if and only if it is a discrete additive subgroup.

Solution to Exercise 7.9.

A solution for this exercise is not currently available.

7.10. 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^{th} row of A and the j^{th} column of A. Define a new matrix B whose ij^{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 7.10.

A solution for this exercise is not currently available.

7.11. Recall from Remark 7.16 that the general linear group $\mathrm{GL}_n(\mathbb{Z})$ is the group of n-by-n matrices with integer coefficients and determinant ± 1. Let A and B be matrices in $\mathrm{GL}_n(\mathbb{Z})$.

(a) Prove that $AB \in \mathrm{GL}_n(\mathbb{Z})$.
(b) Prove that $A^{-1} \in \mathrm{GL}_n(\mathbb{Z})$.
(c) Prove that the n-by-n identity matrix is in $\mathrm{GL}_n(\mathbb{Z})$.
(d) Prove that $\mathrm{GL}_n(\mathbb{Z})$ 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 $\mathrm{GL}_n(\mathbb{Z})$ a commutative group?

Solution to Exercise 7.11.

(a) By assumption, A^{-1} and B^{-1} have integer entries. Hence $(AB)^{-1} = B^{-1}A^{-1}$ also has integer entries, so $AB \in \mathrm{GL}_n(\mathbb{Z})$.
(b) $(A^{-1})^{-1}$ is equal to A, so it has integer entries. Hence $A^{-1} \in \mathrm{GL}_n(\mathbb{Z})$.
(c) Let I be the identity matrix. Then I has integer entries, and $I^{-1} = I$ also has integer entries, so $I \in \mathrm{GL}_n(\mathbb{Z})$.
(d) As the hint says, (a), (b) and (c) show that the product and inverse of matrices in $\mathrm{GL}_n(\mathbb{Z})$ are again in $\mathrm{GL}_n(\mathbb{Z})$ and the identity matrix is in $\mathrm{GL}_n(\mathbb{Z})$, 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, $\mathrm{GL}_n(\mathbb{Z})$ is not commutative for $n \ge 2$. For example, $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ do not commute, and similar examples exist for any $n \ge 2$. Of course, for $n = 1$, $\mathrm{GL}_1(\mathbb{Z}) = \{\pm 1\}$ is commutative.

7.12. Which of the following matrices are in $\mathrm{GL}_n(\mathbb{Z})$? Find the inverses of those matrices that are in $\mathrm{GL}_n(\mathbb{Z})$.

$$\text{(a)}\quad A_1 = \begin{pmatrix}3&1\\2&2\end{pmatrix} \qquad \text{(b)}\quad A_2 = \begin{pmatrix}3&-2\\2&-1\end{pmatrix}$$

$$\text{(c)}\quad A_3 = \begin{pmatrix}3&2&2\\2&1&2\\-1&3&1\end{pmatrix} \qquad \text{(d)}\quad A_4 = \begin{pmatrix}-3&-1&2\\1&-3&-1\\3&0&-2\end{pmatrix}$$

Solution to Exercise 7.12.

(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 $= 1$. $A_4^{-2} = \begin{pmatrix}6&-2&7\\-1&0&-1\\9&-3&10\end{pmatrix}$.

7.13. Let L be the lattice given by the basis

$$\mathcal{B} = \bigl\{(3,1,-2),\ (1,-3,5),\ (4,2,1)\bigr\}.$$

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 7.13.

(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 $\det(\mathcal{B}_2) = 96$.

7.14. Let $L \subset \mathbb{R}^m$ be a lattice of dimension n and let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ be a basis for L. Note that we are allowing n to be smaller than m. The *Gram matrix of* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ is the matrix

$$\operatorname{Gram}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = \big(\boldsymbol{v}_i \cdot \boldsymbol{v}_j\big)_{1 \le i,j \le n}.$$

(a) Let $F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ be the matrix (7.11) described in Proposition (7.20), except that now $F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ is an n-by-m matrix, so it need not be square. Prove that

$$\operatorname{Gram}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)^t,$$

where $F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)^t$ is the transpose matrix, i.e., the matrix with rows and columns interchanged.

(b) Prove that

$$\det\big(\operatorname{Gram}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)\big) = \det(L)^2, \tag{7.1}$$

where note that $\det(L)$ is the volume of the parallelopiped spanned by any basis for L. (You may find it easier to to first do the case $n = m$.)

(c) Let $L \subset \mathbb{R}^4$ be the 3-dimensional lattice with basis

$$\boldsymbol{v}_1 = (1, 0, 1, -1), \quad \boldsymbol{v}_2 = (1, 2, 0, 4), \quad \boldsymbol{v}_3 = (1, -1, 2, 1).$$

Compute the Gram matrix of this basis and use it to compute $\det(L)$.

(d) Let $\boldsymbol{v}_1^*, \dots, \boldsymbol{v}_n^*$ be the Gram–Schmidt orthogonalized vectors (Theorem 7.13) associated to $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$. Prove that

$$\det\bigl(\mathrm{Gram}(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)\bigr) = \|\boldsymbol{v}_1^*\|^2 \|\boldsymbol{v}_2^*\|^2 \cdots \|\boldsymbol{v}_n^*\|^2.$$

Solution to Exercise 7.14.

(a,b,d) *A solution for this exercise is not currently available.*

(c)

$$\mathrm{Gram}(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) = \begin{pmatrix} 1 & 0 & 1 & -1 \\ 1 & 2 & 0 & 4 \\ 1 & -1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & -1 \\ 1 & 0 & 2 \\ -1 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 3 & -3 & 2 \\ -3 & 21 & 3 \\ 2 & 3 & 7 \end{pmatrix}$$

Then

$$\det(L) = \sqrt{\det \mathrm{Gram}(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)} = \sqrt{231}.$$

Section. The shortest and closest vector problems

7.15. Let L be a lattice and let $\mathcal{F}$ be a fundamental domain for L. This exercise sketches a proof that

$$\lim_{R \to \infty} \frac{\#\bigl(\mathbb{B}_R(\mathbf{0}) \cap L\bigr)}{\mathrm{Vol}\bigl(\mathbb{B}_R(\mathbf{0})\bigr)} = \frac{1}{\mathrm{Vol}(\mathcal{F})}. \tag{7.2}$$

(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

$$\bigcup_{\substack{\boldsymbol{v} \in L \\ \mathcal{F}+\boldsymbol{v} \subset \mathbb{B}_R(\mathbf{0})}} (\mathcal{F} + \boldsymbol{v}) \subset \mathbb{B}_R(\mathbf{0}) \subset \bigcup_{\substack{\boldsymbol{v} \in L \\ (\mathcal{F}+\boldsymbol{v}) \cap \mathbb{B}_R(\mathbf{0}) \neq \emptyset}} (\mathcal{F} + \boldsymbol{v}).$$

(b) Take volumes in (a) and prove that

$$\begin{aligned} &\#\bigl\{\boldsymbol{v} \in L : \mathcal{F} + \boldsymbol{v} \subset \mathbb{B}_R(\mathbf{0})\bigr\} \cdot \mathrm{Vol}(\mathcal{F}) \\ &\qquad \le \mathrm{Vol}\bigl(\mathbb{B}_R(\mathbf{0})\bigr) \le \#\bigl\{\boldsymbol{v} \in L : (\mathcal{F} + \boldsymbol{v}) \cap \mathbb{B}_R(\mathbf{0}) \neq \emptyset\bigr\} \cdot \mathrm{Vol}(\mathcal{F}). \end{aligned}$$

(*Hint.* Proposition 7.18 says that the different translates of $\mathcal{F}$ are disjoint.)

(c) Prove that the number of translates $\mathcal{F} + \boldsymbol{v}$ 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 $\mathcal{F}_{\boldsymbol{v}}$ 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

$$\mathrm{Vol}\bigl(\mathbb{B}_R(\mathbf{0})\bigr) = \#\bigl(\mathbb{B}_R(\mathbf{0}) \cap L\bigr) \cdot \mathrm{Vol}(\mathcal{F}) + (\text{smaller term}).$$

Divide by $\mathrm{Vol}\bigl(\mathbb{B}_R(\mathbf{0})\bigr)$ and let $R \to \infty$ to complete the proof of (7.63).

Solution to Exercise 7.15.

A solution for this exercise is not currently available.

7.16. 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 7.16.

The Gaussian heuristic (7.21) 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

7.17. Let $L \subset \mathbb{R}^2$ be the lattice given by the basis $\boldsymbol{v}_1 = (213, -437)$ and $\boldsymbol{v}_2 = (312, 105)$, and let $\boldsymbol{w} = (43127, 11349)$.

(a) Use Babai's algorithm to find a vector $\boldsymbol{v} \in L$ that is close to $\boldsymbol{w}$. Compute the distance $\|\boldsymbol{v} - \boldsymbol{w}\|$.

(b) What is the value of the Hadamard ratio $\big(\det(L)/\|\boldsymbol{v}_1\|\|\boldsymbol{v}_2\|\big)^{1/2}$? Is the basis $\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ a "good" basis?

(c) Show that the vectors $\boldsymbol{v}_1' = (2937, -1555)$ and $\boldsymbol{v}_2' = (11223, -5888)$ are also a basis for L by expressing them as linear combinations of $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ and checking that the change-of-basis matrix has integer coefficients and determinant ± 1.

(d) Use Babai's algorithm with the basis $\{\boldsymbol{v}_1', \boldsymbol{v}_2'\}$ to find a vector $\boldsymbol{v}' \in L$. Compute the distance $\|\boldsymbol{v}' - \boldsymbol{w}\|$ and compare it to your answer from (a).

(e) Compute the Hadamard ratio using $\boldsymbol{v}_1'$ and $\boldsymbol{v}_2'$. Is $\{\boldsymbol{v}_1', \boldsymbol{v}_2'\}$ a good basis?

Solution to Exercise 7.17.

(a) $(t_1, t_2) = (6.22, 133.98)$, so $\boldsymbol{v} = 6\boldsymbol{v}_1 + 134\boldsymbol{v}_2 = (43086, 11448)$. Then $\|\boldsymbol{v} - \boldsymbol{w}\| = 107.15$.

(b) $\det(L)/\|\boldsymbol{v}_1\|\|\boldsymbol{v}_2\| = 158709/(486.15)(329.19) = 0.9917$. The ratio is close to 1, so $\{\boldsymbol{v}_1', \boldsymbol{v}_2'\}$ a good basis.

(c) $\boldsymbol{v}_1' = 5\boldsymbol{v}_1 + 6\boldsymbol{v}_2$ and $\boldsymbol{v}_2' = 19\boldsymbol{v}_1 + 23\boldsymbol{v}_2$. We have $\det\left(\begin{smallmatrix} 5 & 6 \\ 19 & 23 \end{smallmatrix}\right) = 1$.

(d) $(t_1, t_2) = (-2402.52, 632.57)$, so $\boldsymbol{v}' = -2403\boldsymbol{v}_1' + 633\boldsymbol{v}_2' = (46548, 9561)$. Then $\|\boldsymbol{v} - \boldsymbol{w}\| = 3860.08$.

(e) $\det(L)/\|\boldsymbol{v}_1'\|\|\boldsymbol{v}_2'\| = 158709/(3323.25)(12673.76) = 0.00377$. The ratio is very small, so $\{\boldsymbol{v}_1', \boldsymbol{v}_2'\}$ a bad basis.

Section. The GGH public key cryptosystem

7.18. Alice uses the GGH cryptosystem with private basis

$$\boldsymbol{v}_1 = (4, 13), \quad \boldsymbol{v}_2 = (-57, -45),$$

and public basis

$$\boldsymbol{w}_1 = (25453, 9091), \quad \boldsymbol{w}_2 = (-16096, -5749).$$

(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 $\boldsymbol{e} = (155340, 55483)$. Use Alice's private basis to decrypt the message and recover the plaintext. Also determine Bob's random perturbation $\boldsymbol{r}$.

(c) Try to decrypt Bob's message using Babai's algorithm with the public basis $\{\boldsymbol{w}_1, \boldsymbol{w}_2\}$. Is the output equal to the plaintext?

Solution to Exercise 7.18.

(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)

$$\begin{aligned}\boldsymbol{e} &\approx -6823.12\boldsymbol{v}_1 - 3204.08\boldsymbol{v}_2.\\ \boldsymbol{v} &= -6823\boldsymbol{v}_1 - 3204\boldsymbol{v}_2\\ &= (155336, 55481)\\ &= 8\boldsymbol{w}_1 + 3\boldsymbol{w}_2.\end{aligned}$$

So the plaintext is $\boldsymbol{m} = (8, 3)$. Also $\boldsymbol{r} = \boldsymbol{w} - \boldsymbol{v} = (4, 2)$.

(c)

$$\boldsymbol{e} \approx -8.39\boldsymbol{w}_1 - 22.92\boldsymbol{w}_2.$$

This yields the incorrect plaintext $(-8, -23)$.

7.19. Alice uses the GGH cryptosystem with private basis

$$\boldsymbol{v}_1 = (58, 53, -68), \quad \boldsymbol{v}_2 = (-110, -112, 35), \quad \boldsymbol{v}_3 = (-10, -119, 123)$$

and public basis

$$\begin{aligned}\boldsymbol{w}_1 &= (324850, -1625176, 2734951),\\ \boldsymbol{w}_2 &= (165782, -829409, 1395775),\\ \boldsymbol{w}_3 &= (485054, -2426708, 4083804).\end{aligned}$$

(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 $\boldsymbol{e} = (8930810, -44681748, 75192665)$. Use Alice's private basis to decrypt the message and recover the plaintext. Also determine Bob's random perturbation $\boldsymbol{r}$.

(c) Try to decrypt Bob's message using Babai's algorithm with the public basis $\{\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3\}$. Is the output equal to the plaintext?

Solution to Exercise 7.19.

(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)

$$\begin{aligned}
\boldsymbol{e} &\approx -334865.23\boldsymbol{v}_1 - 304373.02\boldsymbol{v}_2 + 512803.95\boldsymbol{v}_3.\\
\boldsymbol{v} &= -334865\boldsymbol{v}_1 - 304373\boldsymbol{v}_2 + 512804\boldsymbol{v}_3\\
&= (8930820, -44681745, 75192657)\\
&= -50\boldsymbol{w}_1 - 91\boldsymbol{w}_2 + 83\boldsymbol{w}_3.
\end{aligned}$$

So the plaintext is $\boldsymbol{m} = (-50, -91, 83)$. Also $\boldsymbol{r} = \boldsymbol{w} - \boldsymbol{v} = (-10, -3, 8)$.
(c)

$$\boldsymbol{e} \approx 51.59\boldsymbol{w}_1 + 416.67\boldsymbol{w}_2 - 158.55\boldsymbol{w}_3.$$

This yields the incorrect plaintext $(52, 417, -159)$.

7.20. Bob uses the GGH cryptosystem to send some messages to Alice.
(a) Suppose that Bob sends the same message $\boldsymbol{m}$ twice, using different random elements $\boldsymbol{r}$ and $\boldsymbol{r}'$. Explain what sort of information Eve can deduce from the ciphertexts $\boldsymbol{e} = \boldsymbol{m}W + \boldsymbol{r}$ and $\boldsymbol{e}' = \boldsymbol{m}W + \boldsymbol{r}'$.
(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 $\boldsymbol{r}$. Suppose further that Eve intercepts two ciphertexts

$$\boldsymbol{e} = (-9, -29, -48, 18, 48) \quad \text{and} \quad \boldsymbol{e}' = (-6, -26, -51, 20, 47)$$

having the same plaintext. With this information, how many possibilities are there for $\boldsymbol{r}$?
(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 $\boldsymbol{e} = \boldsymbol{m}W + \boldsymbol{r}$ and $\boldsymbol{e}' = \boldsymbol{m}'W + \boldsymbol{r}$.

Solution to Exercise 7.20.

(a) Eve can compute $\boldsymbol{e}' - \boldsymbol{e} = \boldsymbol{r}' - \boldsymbol{r}$ and use this information to narrow down the possibilities for $\boldsymbol{r}$ and $\boldsymbol{r}'$.
(b) Eve computes

$$\boldsymbol{e} - \boldsymbol{e}' = \boldsymbol{r} - \boldsymbol{r}' = (-3, -3, 3, -2, 1).$$

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 $\boldsymbol{r}$. For example

$$r_1 = r_1' - 3 \le 2 - 3 = -1, \quad \text{so} \quad r_1 \in \{-2, -1\},$$

and similarly

$$\begin{aligned} r_2 &= r_2' - 3 \le -2 + 3 = 1, &\quad& \text{so} \quad r_2 \in \{-2, -1\}, \\ r_3 &= r_3' + 3 \ge -2 + 3 = 1, && \text{so} \quad r_3 \in \{1, 2\}, \\ r_4 &= r_4' - 2 \le 2 - 2 = 0, && \text{so} \quad r_4 \in \{-2, -1, 0\}, \\ r_5 &= r_5' + 1 \ge -2 + 1 = -1, && \text{so} \quad r_1 \in \{-1, 0, 1, 2\}. \end{aligned}$$

Hence the number of possibilities for $\boldsymbol{r}$ 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 $(\boldsymbol{e} - \boldsymbol{e}')W^{-1} = \boldsymbol{m} - \boldsymbol{m}'$, and then the fact that $\boldsymbol{m}$ and $\boldsymbol{m}'$ are small again allows Eve to narrow down the possibilities.

7.21. The previous exercise shows the danger of using GGH to send a single message $\boldsymbol{m}$ twice using different values of $\boldsymbol{r}$.

(a) In order to guard against this danger, suppose that Bob generates $\boldsymbol{r}$ by applying a publicly available hash function Hash to $\boldsymbol{m}$, i.e., Bob's encrypted message is

$$\boldsymbol{e} = \boldsymbol{m}W + \mathsf{Hash}(\boldsymbol{m}).$$

(See Section 8.1 for a discussion of hash functions.) If Eve guesses that Bob's message might be $\boldsymbol{m}'$, explain why she can check whether her guess is correct.

(b) Explain why the following algorithm eliminates both the problem with repeated messages and the problem described in (a), while still allowing Alice to decrypt Bob's message. Bob chooses an message $\boldsymbol{m}_0$ and a random string $\boldsymbol{r}_0$. He then computes

$$\boldsymbol{m} = (\boldsymbol{m}_0 \mathbin{\mathsf{xor}} \boldsymbol{r}_0) \parallel \boldsymbol{r}_0, \quad \boldsymbol{r} = \mathsf{Hash}(\boldsymbol{m}), \quad \boldsymbol{e} = \boldsymbol{m}W + \boldsymbol{r}.$$

(c) In (b), the advantage of constructing $\boldsymbol{m}$ from $\boldsymbol{m}_0 \mathbin{\mathsf{xor}} \boldsymbol{r}_0$ is that none of the bits of the actual plaintext $\boldsymbol{m}_0$ appear unaltered in $\boldsymbol{m}$. In practice, people replace $(\boldsymbol{m}_0 \mathbin{\mathsf{xor}} \boldsymbol{r}_0) \parallel \boldsymbol{r}_0$ with more complicated mixing functions $M(\boldsymbol{m}_0, \boldsymbol{r}_0)$ having the following two properties: (1) M is easily invertible. (2) If even one bit of either $\boldsymbol{m}_0$ or $\boldsymbol{r}_0$ changes, then the value of every bit of $M(\boldsymbol{m}_0, \boldsymbol{r}_0)$ changes in an unpredictable manner. Try to construct a mixing function M having these properties.

<u>Solution to Exercise 7.21</u>.

(a) This is easy. Eve knows W and the hash function Hash, so she can compute $\boldsymbol{m}'W + \mathsf{Hash}(\boldsymbol{m}')$ and compare it with the intercepted ciphertext $\boldsymbol{e}$.

(b) The introduction of the random $\boldsymbol{r}_0$ means that Even cannot check if a guessed plaintext $\boldsymbol{m}_0'$ is correct. Next, if Bob sends the same message $\boldsymbol{m}_0$ twice using first $\boldsymbol{r}_0$ and second using $\boldsymbol{r}_0'$, then Eve sees

$$\boldsymbol{e} = \big((\boldsymbol{m}_0 \mathbin{\mathsf{xor}} \boldsymbol{r}_0) \parallel \boldsymbol{r}_0\big)W + \mathsf{Hash}\big((\boldsymbol{m}_0 \mathbin{\mathsf{xor}} \boldsymbol{r}_0) \parallel \boldsymbol{r}_0\big)$$

and

$$e' = \big((m_0 \operatorname{\mathsf{xor}} r'_0) \parallel r'_0\big)W + \mathsf{Hash}\big((m_0 \operatorname{\mathsf{xor}} r'_0) \parallel r'_0\big)$$

The vectors

$$(m_0 \operatorname{\mathsf{xor}} r_0) \parallel r_0 \quad \text{and} \quad (m_0 \operatorname{\mathsf{xor}} r'_0) \parallel r'_0$$

are not related in any obvious way, since r_0 and r'_0 are random (and Eve has no idea of their values). In particular, taking a linear combination of e and e' does not allow Eve to eliminate the dependence on W as was done in the attack in the previous problem. (There $e = mW + r$ and $e' = mW + r'$, so Eve could compute $e - e' = r - r'$.)

Finally, it's easy for Alice to decrypt Bob's message. First she uses ordinary GGH decryption (using her private key) to recover $(m_0 \operatorname{\mathsf{xor}} r_0) \parallel r_0$. She breaks this bit string into the two pieces $m_0 \operatorname{\mathsf{xor}} r_0$ and r_0. Finally, the plaintext is recovered by computing

$$(m_0 \operatorname{\mathsf{xor}} r_0) \operatorname{\mathsf{xor}} r_0 = m_0.$$

Section. Convolution polynomial rings

7.22. Compute (by hand!) the polynomial convolution product $c = a \star b$ using the given value of N.

(a) $N = 3$, $a(x) = -1 + 4x + 5x^2$, $b(x) = -1 - 3x - 2x^2$;

(b) $N = 5$, $a(x) = 2 - x + 3x^3 - 3x^4$, $b(x) = 1 - 3x^2 - 3x^3 - x^4$;

(c) $N = 6$, $a(x) = x + x^2 + x^3$, $b(x) = 1 + x + x^5$;

(d) $N = 10$, $a(x) = x + x^2 + x^3 + x^4 + x^6 + x^7 + x^9$,
$b(x) = x^2 + x^3 + x^6 + x^8$.

Solution to Exercise 7.22.
(a) $c = a \star b = -22 - 11x - 15x^2$.
(b) $c = a \star b = -6 - x + 3x^3 - 2x^4$.
(c) $c = a \star b = 1 + 2x + 3x^2 + 2x^3 + x^4$.
(d) $c = a \star b = 3 + 2x + 3x^2 + 2x^3 + 3x^4 + 4x^5 + 2x^6 + 3x^7 + 2x^8 + 4x^9$.

7.23. Compute the polynomial convolution product $c = a \star b$ modulo q using the given values of q and N.

(a) $N = 3$, $q = 7$, $a(x) = 1 + x$, $b(x) = -5 + 4x + 2x^2$;

(b) $N = 5$, $q = 4$, $a(x) = 2 + 2x - 2x^2 + x^3 - 2x^4$,
$b(x) = -1 + 3x - 3x^2 - 3x^3 - 3x^4$;

(c) $N = 7$, $q = 3$, $a(x) = x + x^3$, $b(x) = x + x^2 + x^4 + x^6$;

(d) $N = 10$, $q = 2$, $a(x) = x^2 + x^5 + x^7 + x^8 + x^9$,
$b(x) = 1 + x + x^3 + x^4 + x^5 + x^7 + x^8 + x^9$.

Solution to Exercise 7.23.
(a) $\boldsymbol{c} \equiv \boldsymbol{a} \star \boldsymbol{b} \equiv 4 + 6x + 6x^2 \pmod{7}$.
(b) $\boldsymbol{c} \equiv \boldsymbol{a} \star \boldsymbol{b} \equiv 1 + x + x^2 + 3x^3 + 3x^4 \pmod{4}$.
(c) $\boldsymbol{c} \equiv \boldsymbol{a} \star \boldsymbol{b} \equiv 2 + 2x^2 + x^3 + x^4 + 2x^5 \pmod{3}$.
(d) $\boldsymbol{c} \equiv \boldsymbol{a} \star \boldsymbol{b} \equiv x + x^2 + x^4 + x^6 \pmod{2}$.

7.24. Let $\boldsymbol{a}(x) \in (\mathbb{Z}/q\mathbb{Z})[x]$, where q is a prime.
(a) Prove that

$$\boldsymbol{a}(1) \equiv 0 \pmod{q} \quad \text{if and only if} \quad (x-1) \mid \boldsymbol{a}(x) \quad \text{in } (\mathbb{Z}/q\mathbb{Z})[x].$$

(b) Suppose that $\boldsymbol{a}(1) \equiv 0 \pmod{q}$. Prove that $\boldsymbol{a}(x)$ is not invertible in R_q.

Solution to Exercise 7.24.

(a) Working in $(\mathbb{Z}/q\mathbb{Z})[x]$, we use division with remainder to divide $\boldsymbol{a}(x)$ by $x-1$. The result is

$$\boldsymbol{a}(x) = (x-1)\boldsymbol{b}(x) + \boldsymbol{r}(x) \quad \text{with } \deg \boldsymbol{r} < \deg(x-1) = 1.$$

Thus either $\boldsymbol{r}(x) = 0$ or $\deg \boldsymbol{r}(x) = 0$, so in any case, $\boldsymbol{r}(x)$ is a constant. Thus

$$\boldsymbol{a}(x) = (x-1)\boldsymbol{b}(x) + c \quad \text{for some } c \in \mathbb{Z}/q\mathbb{Z}.$$

We can determine c by substituting $x = 1$, which gives $c = \boldsymbol{a}(1)$. Thus

$$\boldsymbol{a}(x) = (x-1)\boldsymbol{b}(x) + \boldsymbol{a}(1).$$

Now (a) is obvious, since this equation shows that $\boldsymbol{a}(x)$ is a multiple of $x-1$ if and only if $\boldsymbol{a}(1) = 0$.
(b) Suppose that $\boldsymbol{a}(x)$ is invertible in R_q, say $\boldsymbol{a}(x)\boldsymbol{b}(x) = 1$ in R_q. We have a well-defined map $R_q \to \mathbb{Z}/q\mathbb{Z}$ 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 $\boldsymbol{a}(x)\boldsymbol{b}(x) = 1$ in R_q leads to the relation $\boldsymbol{a}(1)\boldsymbol{b}(1) = 1$ in $\mathbb{Z}/q\mathbb{Z}$. In particular, we certainly can't have $\boldsymbol{a}(1) = 0$. This proves

$$\boldsymbol{a}(x) \text{ invertible} \quad \Longrightarrow \quad \boldsymbol{a}(1) \neq 0,$$

which is equivalent to the statement

$$\boldsymbol{a}(1) = 0 \quad \Longrightarrow \quad \boldsymbol{a}(x) \text{ is not invertible.}$$

7.25. Let $N = 5$ and $q = 3$ and consider the two polynomials

$$\boldsymbol{a}(x) = 1 + x^2 + x^3 \in R_3 \quad \text{and} \quad \boldsymbol{b}(x) = 1 + x^2 - x^3 \in R_3.$$

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 7.25.

$\boldsymbol{a}(x)$ does not have an inverse, because $\boldsymbol{a}(1) \equiv 0 \pmod 3$. The previous exercise then implies that $\boldsymbol{a}(x)$ does not have an inverse. Alternatively, using the Euclidean algorithm, one finds that

$$\gcd\bigl(\boldsymbol{a}(x), x^5 - 1\bigr) = 1 - x \quad \text{in } (\mathbb{Z}/3\mathbb{Z})[x],$$

so $\boldsymbol{a}(x)$ does not have an inverse from Proposition 7.45.

Similarly, $\gcd(\boldsymbol{b}(x), x^5 - 1) = 1$ in $(\mathbb{Z}/3\mathbb{Z})[x]$, and using the extended Euclidean algorithm, we find that

$$\boldsymbol{b}(x)^{-1} = 1 - x - x^2 - x^3 \quad \text{in } (\mathbb{Z}/3\mathbb{Z})[x].$$

7.26. For each of the following values of N, q, and $\boldsymbol{a}(x)$, either find $\boldsymbol{a}(x)^{-1}$ in R_q or show that the inverse does not exist.

(a) $N = 5$, $q = 11$, and $\boldsymbol{a}(x) = x^4 + 8x + 3$;

(b) $N = 5$, $q = 13$, and $\boldsymbol{a}(x) = x^3 + 2x - 3$.

(c) $N = 7$, $q = 23$, and $\boldsymbol{a}(x) = 20x^6 + 8x^5 + 4x^4 + 15x^3 + 19x^2 + x + 8$.

Solution to Exercise 7.26.

(a) $\boldsymbol{a}(x)^{-1} = 7x^4 + 8x^3 + 3x^2 + 2x + 3$ in $\mathbb{F}_{11}[x]$.

(b) $\gcd(\boldsymbol{a}(x), x^5 - 1) = x + 12$ in $\mathbb{F}_{13}[x]$, so no inverse.

(c) $\boldsymbol{a}(x)^{-1} = 17x^6 + 4x^5 + 12x^4 + 18x^2 + 12x + 10$ in $\mathbb{F}_{23}[x]$.

7.27. 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

$$G(x) = F(x) \star \bigl(2 - f(x) \star F(x)\bigr)$$

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.

$$\begin{aligned}
&\text{(i)} \quad N = 5, \quad m = 2^4, && f(x) = 7 + 3x + x^2,\\
& && f(x)^{-1} \equiv 1 + x^2 + x^3 \pmod 2.\\
&\text{(ii)} \quad N = 5, \quad m = 2^7, && f(x) = 22 + 11x + 5x^2 + 7x^3,\\
& && f(x)^{-1} \equiv 1 + x^2 + x^3 \pmod 2.\\
&\text{(iii)} \quad N = 7, \quad m = 5^5, && f(x) = 112 + 34x + 239x^2 + 234x^3 + 105x^4\\
& && \qquad + 180x^5 + 137x^6,\\
& && f(x)^{-1} \equiv 1 + 3x^2 + 2x^4 \pmod 5.
\end{aligned}$$

Solution to Exercise 7.27.

(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 $2^k \ge e$, 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) $f(x)^{-1} \bmod 2^4 = 13 + 5X^2 + 7X^3 + 10X^4$.

(ii) $f(x)^{-1} \bmod 2^7 = 101 + 12X + X^2 + 17X^3 + 34X^4$.

(iii) $f(x)^{-1} \bmod 5^5 = 840 + 711X + 710X^2 + 268X^3 + 1710X^4 + 1142X^5 + 2430X^6$.

7.28. Let $\boldsymbol{a} \in \mathbb{R}^N$ be a fixed vector.

(a) Suppose that $\boldsymbol{b}$ is an N-dimensional vector whose coefficients are chosen randomly from the set $\{-1, 0, 1\}$. Prove that the expected values of $\|\boldsymbol{b}\|^2$ and $\|\boldsymbol{a} \star \boldsymbol{b}\|^2$ are given by

$$E\bigl(\|\boldsymbol{b}\|^2\bigr) = \frac{2}{3}N \quad \text{and} \quad E\bigl(\|\boldsymbol{a} \star \boldsymbol{b}\|^2\bigr) = \|\boldsymbol{a}\|^2 E\bigl(\|\boldsymbol{b}\|^2\bigr).$$

(b) More generally, suppose that the coefficients of $\boldsymbol{b}$ are chosen at random from the set of integers $\{-T, -T+1, \ldots, T-1, T\}$. Compute the expected values of $\|\boldsymbol{b}\|^2$ and $\|\boldsymbol{a} \star \boldsymbol{b}\|^2$ as in (a).

(c) Suppose now that the coefficients of $\boldsymbol{b}$ are real numbers that are chosen uniformly and independently in the interval from $-R$ to R. Prove that

$$E\bigl(\|\boldsymbol{b}\|^2\bigr) = \frac{R^2N}{3} \quad\text{and}\quad E\bigl(\|\boldsymbol{a}\star\boldsymbol{b}\|^2\bigr) = \|\boldsymbol{a}\|^2 E\bigl(\|\boldsymbol{b}\|^2\bigr).$$

(*Hint.* The most direct way to do (c) is to use continuous probability theory. As an alternative, let the coefficients of $\boldsymbol{b}$ be chosen uniformly and independently from the set $\{jR/T : -T \le j \le T\}$, redo the computation from (b), and then let $T \to \infty$.)

(d) For each of the scenarios described in (a), (b), and (c), prove that

$$E\bigl(\|\boldsymbol{a}+\boldsymbol{b}\|^2\bigr) = \|\boldsymbol{a}\|^2 + E\bigl(\|\boldsymbol{b}\|^2\bigr).$$

Solution to Exercise 7.28.

Let $\boldsymbol{c} = \boldsymbol{a}\star\boldsymbol{b}$. Then

$$\begin{aligned}
\|\boldsymbol{c}\|^2 &= \sum_{k \bmod N} c_k^2 \\
&= \sum_{k \bmod N} \Biggl(\sum_{i+j\equiv k \pmod N} a_i b_j \Biggr)^2 \\
&= \sum_{k \bmod N} \sum_{i+j\equiv k \pmod N} a_i b_j \sum_{u+v\equiv k \pmod N} a_u b_v \\
&= \sum_{i+j\equiv u+v \pmod N} a_i a_u b_j b_v.
\end{aligned}$$

Note that this last sum is over all 4-tuples (i,j,u,v) mod N satisfying $i+j \equiv u+v \pmod N$. We suppose now that the coefficients of $\boldsymbol{b}$ 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 $\boldsymbol{a}$ are fixed, we can compute

$$\begin{aligned}
E\bigl(\|\boldsymbol{a}\star\boldsymbol{b}\|^2\bigr) &= \sum_{i+j\equiv u+v \pmod N} E(a_i a_u b_j b_v) \\
&= \sum_{i+j\equiv u+v \pmod N} a_i a_u E(b_j b_v) \\
&= \sum_{\substack{i+j\equiv u+v \pmod N \\ j\ne v}} a_i a_u E(b_j)E(b_v) + \sum_{i \bmod N} \sum_{j \bmod N} a_i^2 E(b_j^2) \\
&= \sum_{i \bmod N} a_i^2 \sum_{j \bmod N} E(b_j^2) \\
&= \|\boldsymbol{a}\|^2 E(b_0^2 + \cdots + b_{N-1}^2) \\
&= \|\boldsymbol{a}\|^2 E\bigl(\|\boldsymbol{b}\|^2\bigr).
\end{aligned}$$

Hence in all cases we have

$$E\big(\|\boldsymbol{a} \star \boldsymbol{b}\|^2\big) = \|\boldsymbol{a}\|^2 E\big(\|\boldsymbol{b}\|^2\big).$$

It remains to compute $E\big(\|\boldsymbol{b}\|^2\big)$ under the various scenarios.

(a) The coefficients of $\boldsymbol{b}$ are independent random variables taking values in $\{-1, 0, 1\}$ with equal probabilities, so

$$\begin{aligned} E(b_i) &= \frac{1}{3} \cdot (-1) + \frac{1}{3} \cdot 0 + \frac{1}{3} \cdot 1 = 0, \\ E(b_i^2) &= \frac{1}{3} \cdot (-1)^2 + \frac{1}{3} \cdot 0^2 + \frac{1}{3} \cdot 1^2 = \frac{2}{3}, \\ E\big(\|\boldsymbol{b}\|^2\big) &= E(b_0^2 + \cdots + b_{N-1}^2) = E(b_0^2) + \cdots + E(b_{N-1}^2) = \frac{2}{3}N. \end{aligned}$$

(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

$$E\big(\|\boldsymbol{b}\|^2\big) = \sum_{i=0}^{N-1} E(b_j^2) = \frac{T^2+T}{3} N.$$

(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 $E\big(\|\boldsymbol{b}\|^2\big) = R^2 N/3$.

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 $T \to \infty$ yields $E(b_i^2) = R^2/3$, and then

$$E\big(\|\boldsymbol{b}\|^2\big) = NR^2/3.$$

(d) Let B be the set of $\boldsymbol{b}$ in (a) or (b). Then

$$\begin{aligned}
E\bigl(\|\boldsymbol{a}+\boldsymbol{b}\|^2\bigr) &= \frac{1}{\#B}\sum_{\boldsymbol{b}\in B}\|\boldsymbol{a}+\boldsymbol{b}\|^2 \\
&= \frac{1}{\#B}\sum_{\boldsymbol{b}\in B}\sum_{i=0}^{N}(a_i+b_i)^2 \\
&= \frac{1}{\#B}\sum_{\boldsymbol{b}\in B}\sum_{i=0}^{N}(a_i^2+2a_ib_i+b_i^2) \\
&= \frac{1}{\#B}\sum_{\boldsymbol{b}\in B}\sum_{i=0}^{N}a_i^2 + \frac{1}{\#B}\sum_{\boldsymbol{b}\in B}\sum_{i=0}^{N}2a_ib_i + \frac{1}{\#B}\sum_{\boldsymbol{b}\in B}\sum_{i=0}^{N}b_i^2 \\
&= \frac{1}{\#B}\sum_{\boldsymbol{b}\in B}\|\boldsymbol{a}\|^2 + \sum_{i=0}^{N}2a_i\frac{1}{\#B}\sum_{\boldsymbol{b}\in B}b_i + \frac{1}{\#B}\sum_{\boldsymbol{b}\in B}\|\boldsymbol{b}\|^2 \\
&= \|\boldsymbol{a}\|^2 + 0 + E\bigl(\|\boldsymbol{b}\|^2\bigr).
\end{aligned}$$

Section. The NTRU public key cryptosystem

7.29. Alice and Bob agree to communicate using NTRUEncrypt with

$$(N,p,q)=(7,3,37).$$

Alice's private key is

$$\begin{aligned}
\boldsymbol{f}(x) &= -1+X-X^3+X^4+X^5, \\
\boldsymbol{F}_3(x) &= 1+X-X^2+X^4+X^5+X^6.
\end{aligned}$$

(You can check that $\boldsymbol{f}\star\boldsymbol{F}_3\equiv 1 \pmod 3$.) Alice receives the ciphertext

$$\boldsymbol{e}(x)=2+8X^2-16X^3-9X^4-18X^5-3X^6.$$

from Bob. Decipher the message and find the plaintext.

Solution to Exercise 7.29.

Alice first computes

$$\boldsymbol{a}\equiv\boldsymbol{f}\star\boldsymbol{e}\equiv -4-5X+5X^2+X^3-8X^4+3X^5+9X^6 \pmod{37}.$$

Then she computes

$$\begin{aligned}
\boldsymbol{F}_3\star\boldsymbol{a} &\equiv 3-20X+15X^3-4X^4-6X^5+16X^6 \pmod{37} \\
&\equiv X-X^4+X^6 \pmod{3}.
\end{aligned}$$

The plaintext is $\boldsymbol{m}=X-X^4+X^6$.

7.30. Alice and Bob decide to communicate using NTRUEncrypt with parameters $(N, p, q) = (7, 3, 29)$. Alice's public key is

$$\boldsymbol{h}(x) = 3 + 14X - 4X^2 + 13X^3 - 6X^4 + 2X^5 + 7X^6.$$

Bob sends Alice the plaintext message $\boldsymbol{m}(x) = 1 + X - X^2 - X^3 - X^6$ using the random element $\boldsymbol{r}(x) = -1 + X^2 - X^5 + X^6$.

(a) What ciphertext does Bob send to Alice?

(b) Alice's private key is $\boldsymbol{f}(x) = -1 + X - X^2 + X^4 + X^6$ and $\boldsymbol{F}_3(x) = 1 + X + X^2 + X^4 + X^5 - X^6$. Check your answer in (a) by using $\boldsymbol{f}$ and $\boldsymbol{F}_3$ to decrypt the message.

<u>*Solution to Exercise* 7.30</u>.

(a)

$$\begin{aligned} \boldsymbol{e} &\equiv 3\boldsymbol{r} \star \boldsymbol{h} + \boldsymbol{m} \pmod{29} \\ &\equiv -6 - 13X - 10X^2 + 7X^3 - 9X^4 - 13X^5 + 14X^6 \pmod{29}. \end{aligned}$$

(b) First compute

$$\boldsymbol{a} \equiv \boldsymbol{f} \star \boldsymbol{e} \equiv -2 + 3X - 3X^2 + X^3 + 7X^4 - 2X^5 - 5X^6 \pmod{29}.$$

Then compute

$$\begin{aligned} \boldsymbol{F}_3 \star \boldsymbol{a} &\equiv -14 + 7X + 2X^2 - 13X^3 + 12X^5 + 2X^6 \pmod{29} \\ &\equiv 1 + X - X^2 - X^3 - X^6 \pmod{3}. \end{aligned}$$

This agrees with the plaintext.

7.31. What is the message expansion of NTRUEncrypt in terms of N, p, and q?

<u>*Solution to Exercise* 7.31</u>.

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 NTRUEncrypt is $\log_2(q)/\log_2(p)$.

7.32. The guidelines for choosing NTRUEncrypt 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 $p = q$.)

<u>*Solution to Exercise* 7.32</u>.

We always have

$$\boldsymbol{e}(x) \equiv p\boldsymbol{r}(x)\boldsymbol{h}(x) + \boldsymbol{m}(x) \equiv \boldsymbol{m}(x) \pmod{q}.$$

If $p = q$, then this reduces to $\boldsymbol{e}(x) = \boldsymbol{m}(x)$, so the ciphertext is equal to the plaintext. In general, if $p \mid q$, then reducing $\boldsymbol{e}(x)$ modulo p gives the plaintext $\boldsymbol{m}(x)$.

7.33. The guidelines for choosing NTRUEncrypt public parameters (N, p, q, d) include the assumption that $\gcd(N, q) = 1$. Suppose instead that Alice takes $q = N$, where as always, N is an odd prime.

(a) Make a change of variables $x = y + 1$ in the ring $\mathbb{Z}[x]/(x^N - 1)$, and show that the NTRU lattice takes a simpler form.

(b) Can you find an efficient way to break NTRU in the case that $q = N$ that does involve lattice reduction? (This appears to be an open problem.)

<u>*Solution to Exercise* 7.33</u>.

(a) If $q = N$, then Fermat's little theorem says that

$$(x^N - 1) \equiv (x - 1)^N = y^N \pmod{q},$$

so $\mathbb{Z}[x]/(x^N - 1) = \mathbb{Z}[y]/(y^N)$. Hence polynomial multiplication $a(y) \star b(y)$ now means to discard all terms whose degree is N or larger; there's no "wrapping". This leads to a simpler lattice with more zeros in the matrix.

(b) One idea would be to solve

$$\boldsymbol{f}(y) \star \boldsymbol{h}(y) \equiv \boldsymbol{g}(y) \pmod{y^k}$$

successively for $k = 1, 2, 3, \ldots, N$. Since $\boldsymbol{f}(x)$ and $\boldsymbol{g}(x)$ are ternary, one might be able to limit the size of the search space for each new value of k. But the authors do not know how to make this work in practice.

7.34. Alice uses NTRUEncrypt with $p = 3$ to send messages to Bob.

(a) Suppose that Alice uses the same random element $\boldsymbol{r}(x)$ to encrypt two different plaintexts $\boldsymbol{m}_1(x)$ and $\boldsymbol{m}_2(x)$. Explain how Eve can use the two ciphertexts $\boldsymbol{e}_1(x)$ and $\boldsymbol{e}_2(x)$ to determine approximately $\frac{2}{9}$ of the coefficients of $\boldsymbol{m}_1(x)$. (See Exercise 7.38 for a way to exploit this information.)

(b) For example, suppose that $N = 8$, so there are 3^8 possibilities for $\boldsymbol{m}_1(x)$. Suppose that Eve intercepts two ciphertexts

$$\begin{aligned} \boldsymbol{e}_1(x) &= 32 + 21x - 9x^2 - 20x^3 - 29x^4 - 29x^5 - 19x^6 + 38x^7, \\ \boldsymbol{e}_2(x) &= 33 + 21x - 7x^2 - 19x^3 - 31x^4 - 27x^5 - 19x^6 + 38x^7, \end{aligned}$$

that were encrypted using the same random element $\boldsymbol{r}(x)$. How many coefficients of $\boldsymbol{m}_1(x)$ can she determine exactly? How many possibilities are there for $\boldsymbol{m}_1(x)$?

(c) Formulate a similar attack if Alice uses two different random elements $\boldsymbol{r}_1(x)$ and $\boldsymbol{r}_2(x)$ to encrypt the same plaintext $\boldsymbol{m}(x)$. (*Hint.* Do it first assuming that $\boldsymbol{h}(x)$ has an inverse in R_q. The problem is harder without this assumption.)

<u>*Solution to Exercise* 7.34</u>.

(a) Eve computes

$$\begin{aligned} \boldsymbol{e}_1(x) - \boldsymbol{e}_2(x) &\equiv \bigl(\boldsymbol{r}(x) \star \boldsymbol{h}(x) + \boldsymbol{m}_1(x)\bigr) - \bigl(\boldsymbol{r}(x) \star \boldsymbol{h}(x) + \boldsymbol{m}_2(x)\bigr) \pmod{q} \\ &\equiv \boldsymbol{m}_1(x) - \boldsymbol{m}_2(x) \pmod{q}. \end{aligned}$$

The coefficients of $\boldsymbol{m}_1(x)-\boldsymbol{m}_2(x)$ are in the set $\{-2,-1,0,1,2\}$, so since $q>5$, Eve recovers $\boldsymbol{m}_1(x)-\boldsymbol{m}_2(x)$ exactly. Any coefficient that is nonzero limits the possibilities for that coefficient of $\boldsymbol{m}_1(x)$. (This is the same as the analogous GGH exercise.)

More precisely, Eve can recover the i^{th} coefficient of $\boldsymbol{m}_1(x)$ if the i^{th} coefficient of both $\boldsymbol{m}_1(x)$ and $\boldsymbol{m}_2(x)$ 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 $\boldsymbol{m}_1(x)$.

(b) Eve finds that

$$\boldsymbol{m}_1(x)-\boldsymbol{m}_2(x)=\boldsymbol{e}_1(x)-\boldsymbol{e}_2(x)=-1-2x^2-x^3+2x^4-2x^5$$

The coefficients of x^2, x^4 and x^5 for $\boldsymbol{m}_1$ are determined, they are $-x^2+x^4-x^5$. So Eve knows three of the coefficients of $\boldsymbol{m}_1$.

More generally, $\boldsymbol{m}_1(x)$ 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 $2\cdot3\cdot2\cdot3\cdot3=108$ possibilities for $\boldsymbol{m}_1(x)$, which is much smaller than $3^8=6561$.

(c) If $\boldsymbol{h}(x)$ is invertible in R_q, then Eve can compute

$$\begin{aligned}\boldsymbol{h}(x)^{-1}\big(\boldsymbol{e}_1(x)-\boldsymbol{e}_2(x)\big)&=\boldsymbol{h}(x)^{-1}\big(p\boldsymbol{r}_1(x)\boldsymbol{h}(x)-p\boldsymbol{r}_2(x)\boldsymbol{h}(x)\big)\pmod q\\&=\boldsymbol{r}_1(x)-\boldsymbol{r}_2(x)\pmod q.\end{aligned}$$

Then the analysis is the same as in (a), since $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ have ternary coefficients.

In general, however, $\boldsymbol{h}(x)$ is not invertible, since $\boldsymbol{g}(x)$ is not invertible, since $\boldsymbol{g}(1)=0$. 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 $\mathbb{Z}\times\mathbb{Z}[x]/\big(\Phi(x)\big)$, where $\Phi(x)=x^{N-1}+x^{N-2}+\cdots+x+1$. The image of $g(x)$ in the product ring is $(0,\overline{g(x)})$, so one inverts the second factor.

7.35. This exercise describes a variant of NTRUEncrypt that eliminates a step in the decryption algorithm at the cost of requiring slightly larger parameters. Suppose that the NTRUEncrypt private key polynomials $\boldsymbol{f}(x)$ and $\boldsymbol{g}(x)$ are chosen to satisfy

$$\boldsymbol{f}(x)=1+p\boldsymbol{f}_0(x)\equiv1\pmod p\quad\text{and}\quad\boldsymbol{g}(x)=p\boldsymbol{g}_0(x)\equiv0\pmod p,$$

and that NTRU encryption is changed to

$$\boldsymbol{e}(x)\equiv\boldsymbol{h}(x)\star\boldsymbol{r}(x)+\boldsymbol{m}(x)\pmod q.$$

(The change is the omission of p before $\boldsymbol{h}(x)$.)

(a) Prove that if q is sufficiently large, then the following algorithm correctly decrypts the message:

- Compute $\boldsymbol{a}(x) \equiv \boldsymbol{f}(x) \star \boldsymbol{e}(x) \pmod{q}$ and center-lift to an element of R.
- Compute $\boldsymbol{a}(x) \pmod{p}$. The result is $\boldsymbol{m}(x)$.

  Note that this eliminates the necessity to multiply $\boldsymbol{a}(x)$ by $\boldsymbol{f}(x)^{-1} \pmod{p}$.

(a) Suppose that we choose $\boldsymbol{f}_0, \boldsymbol{g}_0 \in \mathcal{T}(d,d)$, and that we also assume that $\boldsymbol{m}$ is ternary. Prove that decryption works provided $q > 8dp+2$. (*Hint.* Mimic the proof of Proposition 7.48.)

Solution to Exercise 7.35.

(a) We have

$$\begin{aligned} \boldsymbol{a} &\equiv \boldsymbol{f} \star \boldsymbol{e} \pmod{q} \\ &\equiv \boldsymbol{f} \star (\boldsymbol{h} \star \boldsymbol{r} + \boldsymbol{m}) \pmod{q} \\ &\equiv \boldsymbol{g} \star \boldsymbol{r} + \boldsymbol{f} \star \boldsymbol{m} \pmod{q}. \end{aligned}$$

If q is sufficiently large, then the center-lift of $\boldsymbol{a}$ will be exactly

$$\boldsymbol{a} = \boldsymbol{g} \star \boldsymbol{r} + \boldsymbol{f} \star \boldsymbol{m}.$$

Then

$$\boldsymbol{a} = p\boldsymbol{g}_0 \star \boldsymbol{r} + (1 + p\boldsymbol{f}_0) \star \boldsymbol{m} \equiv \boldsymbol{m} \pmod{p}.$$

(b) From (a), we need the largest coefficient of $\boldsymbol{g} \star \boldsymbol{r} + \boldsymbol{f} \star \boldsymbol{m}$ to be smaller than $\frac{1}{2}q$. We have

$$\boldsymbol{g} \star \boldsymbol{r} + \boldsymbol{f} \star \boldsymbol{m} = p(\boldsymbol{g}_0 \star \boldsymbol{r} + \boldsymbol{f}_0 \star \boldsymbol{m}) + \boldsymbol{m}.$$

The largest coefficients of $\boldsymbol{g}_0 \star \boldsymbol{r}$ and $\boldsymbol{f}_0 \star \boldsymbol{m}$ are at most $2d$, so decryption works provided

$$\frac{1}{2}q > p(2d + 2d) + 1 = 4dp + 1$$

Section. NTRU as a lattice cryptosystem

7.36. This exercise explains how to formulate NTRU message recovery as a closest vector problem. Let $\boldsymbol{h}(x)$ be an NTRU public key and let

$$\boldsymbol{e}(x) \equiv p\boldsymbol{r}(x) \star \boldsymbol{h}(x) + \boldsymbol{m}(x) \pmod{q}$$

be a message encrypted using $\boldsymbol{h}(x)$.

(a) Prove that the vector $(p\boldsymbol{r}, \boldsymbol{e} - \boldsymbol{m})$ is in $L_{\boldsymbol{h}}^{\mathrm{NTRU}}$.

(b) Prove that the lattice vector in (a) is almost certainly the closest lattice vector to the known vector $(0, \boldsymbol{e})$. Hence solving CVP reveals the plaintext $\boldsymbol{m}$. (For simplicity, you may assume that $d \approx N/3$ and $q \approx 2N$, as we did in Proposition 7.61.)

(c) Show how one can reduce the lattice-to-target distance, without affecting the determinant, by using instead a modified NTRU lattice of the form

$$\begin{pmatrix} 1 & p\boldsymbol{h} \\ 0 & q \end{pmatrix}.$$

Solution to Exercise 7.36.

(a) By the definition of $\boldsymbol{e}$, we can find a polynomial $\boldsymbol{v}(x)$ satisfying

$$\boldsymbol{e} = p\boldsymbol{r} \star \boldsymbol{h} + \boldsymbol{m} + q\boldsymbol{v}(x).$$

Thus

$$\begin{aligned}(p\boldsymbol{r}, \boldsymbol{v})M_{\boldsymbol{h}}^{\text{NTRU}} &= (p\boldsymbol{r}, \boldsymbol{v}) \begin{pmatrix} 1 & \boldsymbol{h} \\ 0 & q \end{pmatrix} \\ &= (p\boldsymbol{r}, p\boldsymbol{r} \star \boldsymbol{h} + q\boldsymbol{v}) \\ &= (p\boldsymbol{r}, \boldsymbol{e} - \boldsymbol{m}).\end{aligned}$$

This shows that $(p\boldsymbol{r}, \boldsymbol{e} - \boldsymbol{m})$ is in the NTRU lattice $L_{\boldsymbol{h}}^{\text{NTRU}}$ spanned by the rows of $M_{\boldsymbol{h}}^{\text{NTRU}}$. Also notice that

$$(p\boldsymbol{r}, \boldsymbol{e} - \boldsymbol{m}) = \overbrace{(0, \boldsymbol{e})}^{\text{Eve knows this vector}} + \overbrace{(p\boldsymbol{r}, -\boldsymbol{m})}^{\text{a short vector}}.$$

(b) We have

$$\begin{aligned}\big\|(p\boldsymbol{r}, \boldsymbol{e} - \boldsymbol{m}) - (0, \boldsymbol{e})\big\| &= \big\|(p\boldsymbol{r}, -\boldsymbol{m})\big\| \\ &= \sqrt{p^2 \cdot 2d + 2d} \\ &\approx \sqrt{(p^2+1)2N/3}.\end{aligned}$$

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 $\sigma(L_{\boldsymbol{h}}^{\text{NTRU}}) \approx 0.484N$.

(c) Let

$$A_{\boldsymbol{h}}^{\text{NTRU}} = \begin{pmatrix} 1 & p\boldsymbol{h} \\ 0 & q \end{pmatrix}.$$

Then with notation as in (a), we have

$$\begin{aligned}(\boldsymbol{r}, \boldsymbol{v})A_{\boldsymbol{h}}^{\text{NTRU}} &= (\boldsymbol{r}, \boldsymbol{v}) \begin{pmatrix} 1 & p\boldsymbol{h} \\ 0 & q \end{pmatrix} \\ &= (p\boldsymbol{r}, p\boldsymbol{r} \star \boldsymbol{h} + q\boldsymbol{v}) \\ &= (p\boldsymbol{r}, \boldsymbol{e} - \boldsymbol{m}).\end{aligned}$$

This shows that $(\boldsymbol{r}, \boldsymbol{e} - \boldsymbol{m})$ is in the lattice spanned by the rows of $A_{\boldsymbol{h}}^{\text{NTRU}}$. And $\det(A_{\boldsymbol{h}}^{\text{NTRU}}) = q^N$, which is the same as $\det(M_{\boldsymbol{h}}^{\text{NTRU}})$.

Now reworking (b), we see that

$$\begin{aligned}\big\|(\boldsymbol{r}, \boldsymbol{e} - \boldsymbol{m}) - (0, \boldsymbol{e})\big\| &= \big\|(\boldsymbol{r}, -\boldsymbol{m})\big\| \\ &= \sqrt{4d} \approx \sqrt{4N/3} \approx 1.15\sqrt{N}.\end{aligned}$$

So the distance to the closest vector using this new lattice is less than when using the old lattice.

7.37. The guidelines for choosing NTRUEncrypt public parameters (N, p, q, d) include the requirement that N be 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

$$\mathbb{Z}[x]/(x^N - 1) \to \mathbb{Z}[x]/(x^{N/2} - 1).$$

Solution to Exercise 7.37.

This method of breaking NTRUEncrypt 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.

7.38. Suppose that Bob and Alice are using NTRUEncrypt to exchange messages and that Eve intercepts a ciphertext $\boldsymbol{e}(x)$ for which she already knows part of the plaintext $\boldsymbol{m}(x)$. (This is not a ludicrous assumption; see Exercise 7.34, for example.) More precisely, suppose that Eve knows t of the coefficients of $\boldsymbol{m}(x)$. Explain how to set up a CVP to find $\boldsymbol{m}(x)$ using a lattice of dimension $2N - 2t$.

Solution to Exercise 7.38.

A solution for this exercise is not currently available.

Section. Lattice-based digital signature schemes

7.39. Samantha uses the GGH digital signature scheme with private and public bases

$$\begin{aligned} \boldsymbol{v}_1 &= (-20, -8, 1), & \boldsymbol{w}_1 &= (-248100, 220074, 332172),\\ \boldsymbol{v}_2 &= (14, 11, 23), & \boldsymbol{w}_2 &= (-112192, 99518, 150209),\\ \boldsymbol{v}_3 &= (-18, 1, -12), & \boldsymbol{w}_3 &= (-216150, 191737, 289401). \end{aligned}$$

What is her signature on the document

$$\boldsymbol{d} = (834928, 123894, 7812738)?$$

Solution to Exercise 7.39.

Samantha uses Babai's algorithm with the good basis to find the vector

$$\boldsymbol{s} = 283411\boldsymbol{v}_1 + 233700\boldsymbol{v}_2 - 179519\boldsymbol{v}_3 = (834922, 123893, 7812739)$$

that is close to $\boldsymbol{d}$,

$$\|\boldsymbol{s} - \boldsymbol{d}\| \approx 6.16.$$

She then expresses the signature in terms of bad basis,

$$\boldsymbol{s} = 785152901\boldsymbol{w}_1 - 1383699316\boldsymbol{w}_2 - 183004589\boldsymbol{w}_3$$

and publishes the signature $(785152901, -1383699316, -183004589)$.

7.40. Samantha uses the GGH digital signature scheme with public basis

$$\begin{aligned}\boldsymbol{w}_1 &= (3712318934, -14591032252, 11433651072),\\ \boldsymbol{w}_2 &= (-1586446650, 6235427140, -4886131219),\\ \boldsymbol{w}_3 &= (305711854, -1201580900, 941568527).\end{aligned}$$

She publishes the signature

$$(6987814629, 14496863295, -9625064603)$$

on the document

$$\boldsymbol{d} = (5269775, 7294466, 1875937).$$

If the maximum allowed distance from the signature to the document is 60, verify that Samantha's signature is valid.

Solution to Exercise 7.40.

We first compute

$$\begin{aligned}\boldsymbol{s} &= 6987814629\boldsymbol{w}_1 + 14496863295\boldsymbol{w}_2 - 9625064603\boldsymbol{w}_3\\ &= (5269774, 7294492, 1875902) \in L.\end{aligned}$$

Then we compute the distance

$$\|\boldsymbol{s} - \boldsymbol{d}\| \approx 43.61$$

and verify that it is smaller than the cutoff value of 60, so the signature is valid.

7.41. Samantha uses the GGH digital signature scheme with public basis

$$\begin{aligned}\boldsymbol{w}_1 &= (-1612927239, 1853012542, 1451467045),\\ \boldsymbol{w}_2 &= (-2137446623, 2455606985, 1923480029),\\ \boldsymbol{w}_3 &= (2762180674, -3173333120, -2485675809).\end{aligned}$$

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

$$\boldsymbol{d} = (87398273893, 763829184, 118237397273).$$

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 7.41.

Eve's implementation of LLL gives the basis

$$\boldsymbol{v}_1 = (-9, -147, -136), \quad \boldsymbol{v}_2 = (73, 169, -41), \quad \boldsymbol{v}_3 = (109, -132, -110).$$

Using this LLL reduced basis, she computes

$$\begin{aligned}\boldsymbol{s} &= -1542740188\boldsymbol{v}_1 - 532211991\boldsymbol{v}_2 + 1030872363\boldsymbol{v}_3\\ &= (87398273916, 763829241, 118237397269) \in L.\end{aligned}$$

It satisfies

$$\|\boldsymbol{s} - \boldsymbol{d}\| \approx 61.60,$$

so is quite a good solution. To find the signature, Eve expresses $\boldsymbol{s}$ in terms of the original bad basis,

$$\boldsymbol{s} = 203927306009123\boldsymbol{w}_1 + 225365519245447\boldsymbol{w}_2 + 293473443761381\boldsymbol{w}_3.$$

The signature is

$$(203927306009123, 225365519245447, 293473443761381).$$

7.42. This exercise gives further details of the NTRUMLS signature scheme. We fix parameters (N, p, q) and set

$$B = \left\lceil \frac{p^2 N}{4} \right\rceil \quad \text{and} \quad A = \left\lfloor \frac{q}{2p} - \frac{1}{2} \right\rfloor .$$

We choose private key polynomials $\boldsymbol{f}$ and $\boldsymbol{g}$ as follows. For $\boldsymbol{f}$ we first choose a polynomial $\boldsymbol{F}$ whose coefficients are randomly selected from the set $\{-1, 0, 1\}$ and then let $\boldsymbol{f} = p\boldsymbol{F}$. For $\boldsymbol{g}$ we choose a polynomial whose coefficients are randomly selected to lie between $-p/2$ and $p/2$. We further assume that both $\boldsymbol{F}$ and $\boldsymbol{g}$ are invertible modulo p and that $\boldsymbol{f}$ is invertible modulo q, otherwise we discard them and choose new polynomials.

(a) If $\boldsymbol{a}$ and $\boldsymbol{b}$ are polynomials whose coefficients lie between $-p/2$ and $p/2$, prove that $\|\boldsymbol{a} \star \boldsymbol{b}\|_\infty \le B$.

(b) Prove that the following algorithm outputs a pair of polynomials $(\boldsymbol{s}, \boldsymbol{t})$ satisfying

$$\boldsymbol{t} \equiv \boldsymbol{h} \star \boldsymbol{s} \pmod{q} \quad \text{and} \quad \boldsymbol{s} \equiv \boldsymbol{s}_p \pmod{p} \quad \text{and} \quad \boldsymbol{t} \equiv \boldsymbol{t}_p \pmod{p}.$$

```
0: Input polynomials $\boldsymbol{s}_p$ and $\boldsymbol{t}_p$ with coefficients between $-\frac{1}{2}p$ and $\frac{1}{2}p$.
1: Choose a random polynomial $\boldsymbol{r}$ with coefficients between $-A$ and $A$.
2: Set $\boldsymbol{s}_0 = \boldsymbol{s}_p + p\boldsymbol{r}$.
3: Set $\boldsymbol{t}_0 \equiv \boldsymbol{h} \star \boldsymbol{s}_0 \pmod{q}$ with $\|\boldsymbol{t}_0\|_\infty \le \frac{1}{2}q$.
4: Set $\boldsymbol{a} \equiv \boldsymbol{g}^{-1} \star (\boldsymbol{t}_p - \boldsymbol{t}_0) \pmod{p}$ with $\|\boldsymbol{a}\|_\infty \le \frac{1}{2}p$.
5: Set $\boldsymbol{s} = \boldsymbol{s}_0 + a \star \boldsymbol{f}$ and $\boldsymbol{t} = \boldsymbol{t}_0 + a \star \boldsymbol{g}$.
```

(c) Prove that the output from the algorithm in (b) satisfies

$$\|\boldsymbol{s}\|_\infty \le \frac{q}{2} + B \quad \text{and} \quad \|\boldsymbol{t}\|_\infty \le \frac{q}{2} + B.$$

(d) Make the simplifying assumption that the output produces polynomials whose coefficients are uniformly and independently distributed between $-\frac{1}{2}q - B$ and $\frac{1}{2}q + B$. Assume further that $k := q/NB$ is not too large, say $2 \le k \le 50$. Prove that the probability that the algorithm in (b) produces a valid signature is approximately $e^{-8/k}$. (Note that according to (b), the output $(\boldsymbol{s}, \boldsymbol{t})$ will be a valid signature if it satisfies the size criteria $\|\boldsymbol{s}\|_\infty \le \frac{1}{2}q - B$ and $\|\boldsymbol{t}\|_\infty \le \frac{1}{2}q - B$.)

Solution to Exercise 7.42.

A solution for this exercise is not currently available.

(c) There are $2N$ coefficients in $\boldsymbol{s}$ and $\boldsymbol{t}$, each of which has magnitude at most $\frac{1}{2}q + B$, and we want to know the probability that they all have magnitude at most $\frac{1}{2}q - B$. This probability is

$$\begin{aligned}\Pr\left(\|(\boldsymbol{s},\boldsymbol{t})\|_\infty \le \frac{1}{2}q - B\right) &\approx \left(\frac{\frac{1}{2}q - B}{\frac{1}{2}q + B}\right)^{2N} \\ &\approx \left(\frac{1 - \frac{2B}{q}}{1 + \frac{2B}{q}}\right)^{2N} \\ &\approx \left(\frac{1 - \frac{2}{kN}}{1 + \frac{2}{kN}}\right)^{2N} \\ &\approx e^{-8/k},\end{aligned}$$

where for the last equality we use the estimate $(1 + t/n)^n \approx e^t$, valid when t is small and n is large.

Section. Lattice reduction algorithms

7.43. Let $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ be vectors, and set

$$t = \boldsymbol{b}_1 \cdot \boldsymbol{b}_2 / \|\boldsymbol{b}_1\|^2 \qquad \text{and} \qquad \boldsymbol{b}_2^* = \boldsymbol{b}_2 - t\boldsymbol{b}_1.$$

Prove that $\boldsymbol{b}_2^* \cdot \boldsymbol{b}_1 = 0$ and that $\boldsymbol{b}_2^*$ is the projection of $\boldsymbol{b}_2$ onto the orthogonal complement of $\boldsymbol{b}_1$.

Solution to Exercise 7.43.

A solution for this exercise is not currently available.

7.44. Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be nonzero vectors in $\mathbb{R}^n$.

(a) What value of $t \in \mathbb{R}$ minimizes the distance $\|\boldsymbol{a} - t\boldsymbol{b}\|$? (*Hint.* It's easier to minimize the value of $\|\boldsymbol{a} - t\boldsymbol{b}\|^2$.)

(b) What is the minimum distance in (a)?

(c) If t is chosen as in (a), show that $\boldsymbol{a} - t\boldsymbol{b}$ is the projection of $\boldsymbol{a}$ onto the orthogonal complement of $\boldsymbol{b}$.

(d) If the angle between $\boldsymbol{a}$ and $\boldsymbol{b}$ is θ, use your answer in (b) to show that the minimum distance is $\|a\| \sin\theta$. Draw a picture illustrating this result.

Solution to Exercise 7.44.

(a) We have

$$\begin{aligned} F(t) &= \|\boldsymbol{a} - t\boldsymbol{b}\|^2 \\ &= (\boldsymbol{a} - t\boldsymbol{b}) \cdot (\boldsymbol{a} - t\boldsymbol{b}) \\ &= \|\boldsymbol{a}\|^2 - 2t\boldsymbol{a} \cdot \boldsymbol{b} + t^2\|\boldsymbol{b}\|^2. \end{aligned}$$

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 $t = \frac{\boldsymbol{a}\cdot\boldsymbol{b}}{\|\boldsymbol{b}\|^2}$.

(b) Substituting this value of t and simplifying gives the minimum distance

$$\sqrt{\frac{\|\boldsymbol{a}\|^2\|\boldsymbol{b}\|^2 - (\boldsymbol{a}\cdot\boldsymbol{b})^2}{\|\boldsymbol{b}\|^2}}.$$

(c) *A solution for this exercise is not currently available.*

(d) Substitute $\boldsymbol{a}\cdot\boldsymbol{b} = \|\boldsymbol{a}\|\|\boldsymbol{b}\|\cos\theta$ into (b) and use

$$\begin{aligned} \|\boldsymbol{a}\|^2\|\boldsymbol{b}\|^2 - (\boldsymbol{a}\cdot\boldsymbol{b})^2 &= \|\boldsymbol{a}\|^2\|\boldsymbol{b}\|^2 - \bigl(\|\boldsymbol{a}\|\|\boldsymbol{b}\|\cos\theta\bigr)^2 \\ &= \|\boldsymbol{a}\|^2\|\boldsymbol{b}\|^2(1 - \cos^2\theta) \\ &= \|\boldsymbol{a}\|^2\|\boldsymbol{b}\|^2\sin^2\theta. \end{aligned}$$

7.45. Apply Gauss's lattice reduction algorithm (Proposition 7.66) to solve SVP for the following two dimensional lattices having the indicated basis vectors. How many steps does the algorithm take?

(a) $\boldsymbol{v}_1 = (120670, 110521)$ and $\boldsymbol{v}_2 = (323572, 296358)$.

(b) $\boldsymbol{v}_1 = (174748650, 45604569)$ and $\boldsymbol{v}_2 = (35462559, 9254748)$.

(c) $\boldsymbol{v}_1 = (725734520, 613807887)$ and $\boldsymbol{v}_2 = (3433061338, 2903596381)$.

Solution to Exercise 7.45.

(a)

Step	$\boldsymbol{v}_1$	$\boldsymbol{v}_2$	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 $\boldsymbol{v} = (14, -47)$.
(b)

Step	$\boldsymbol{v}_1$	$\boldsymbol{v}_2$	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 $\boldsymbol{v} = (147, 330)$.
(c)

Step	$\boldsymbol{v}_1$	$\boldsymbol{v}_2$	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 $\boldsymbol{v} = (4690, 126)$.

7.46. 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.

(a) Prove that $W^\perp$ is also a vector subspace of V.

(b) Prove that every vector $\boldsymbol{v} \in V$ can be written as a sum $\boldsymbol{v} = \boldsymbol{w} + \boldsymbol{w}'$ for unique vectors $\boldsymbol{w} \in W$ and $\boldsymbol{w}' \in W^\perp$. (One says that V is the *direct sum* of the subspaces W and $W^\perp$.)

(c) Let $\boldsymbol{w} \in W$ and $\boldsymbol{w}' \in W^\perp$ and let $\boldsymbol{v} = a\boldsymbol{w} + b\boldsymbol{w}'$. Prove that

$$\|\boldsymbol{v}\|^2 = a^2\|\boldsymbol{w}\|^2 + b^2\|\boldsymbol{w}'\|^2.$$

Solution to Exercise 7.46.

A solution for this exercise is not currently available.

7.47. Let L be a lattice with basis vectors $\boldsymbol{v}_1 = (161, 120)$ and $\boldsymbol{v}_2 = (104, 77)$.

(a) Is $(0,1)$ in the lattice?
(b) Find an LLL reduced basis.
(c) Use the reduced basis to find the closest lattice vector to $\left(-\frac{9}{2}, 11\right)$.

Solution to Exercise 7.47.

A solution for this exercise is not currently available.

7.48. Use the LLL algorithm to reduce the lattice with basis

$$\boldsymbol{v}_1 = (20,16,3), \quad \boldsymbol{v}_2 = (15,0,10), \quad \boldsymbol{v}_3 = (0,18,9).$$

You should do this exercise by hand, writing out each step.

Solution to Exercise 7.48.

Compute

$$\mu_{2,1} = \frac{300+30}{400+(14)^2+64} = \frac{330}{665} < \frac{1}{2}.$$

Checking the Lovász condition for $\boldsymbol{v}_2$ amounts to checking that $\|\boldsymbol{v}_2\|^2 \geq \frac{3}{4}\|\boldsymbol{v}_1\|^2$ and $\|\boldsymbol{v}_2\|^2 = 225+100 = 325, \|\boldsymbol{v}_1\|^2 = 665$, so swap. Now $\boldsymbol{v}_1 = (15,0,10)$ and $\boldsymbol{v}_2 = (20,16,3)$. Recompute $\mu_{2,1} = \frac{356}{325}$ and subtract one multiple of $\boldsymbol{v}_1$ from $\boldsymbol{v}_2$. New $\boldsymbol{v}_2 = (5,16,-7)$. Note that the (new) $\mu_{2,1}$ is now $(75-70)/325 = -5/325$.

Move on to $\boldsymbol{v}_3$ 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 $\boldsymbol{v}_2$ from $\boldsymbol{v}_3$ obtaining the new $\boldsymbol{v}_3 = (-5,2,16)$.

On to the Lovász condition, computing

$$\|\boldsymbol{v}_3^* + \mu_{3,2}\boldsymbol{v}_2^*\|^2 = \|\boldsymbol{v}_3 - \mu_{3,1}\boldsymbol{v}_1\|^2 = \|(-5,2,16) - \frac{85}{325}(15,0,10)\|^2 = \|\frac{1}{13}(-14,26,174)\|^2.$$

Next compute

$$\|\boldsymbol{v}_2^*\|^2 = \|\frac{1}{13}(62,208,3)\|^2$$

and we find the condition (2) is not satisfied, so we swap. At this point,

$$\boldsymbol{v}_1 = (15,0,10), \quad \boldsymbol{v}_2 = (-5,2,16), \quad \boldsymbol{v}_3 = (5,16,-7).$$

Checking condition (2) for (the new) $\boldsymbol{v}_2$: $\|\boldsymbol{v}_2\|^2 = 285$, which is larger than 3/4 times $\|\boldsymbol{v}_1\|^2 = 325$. (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 $\boldsymbol{v}_2$ is smaller than the length of $\boldsymbol{v}_1$.) Now check the value of

$$\mu_{3,2} = \frac{-105}{285}$$

and the Lovász condition for $\boldsymbol{v}_3$, which is satisfied. So we now have an LLL reduced basis.

7.49. 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 7.8) 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 7.49.

(a) $\det(L) = 21242880806$, $\mathcal{H}(M) = 0.45726$, smallest basis vector is $\|\boldsymbol{v}_6\| = 63.198$,

(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 $\|\boldsymbol{v}_1\| = 28.792$. Gaussian expected shortest is $\sigma(L) = 40.0239$. This suggests that $\boldsymbol{v}_1$ 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 $\|\boldsymbol{v}_1\| = 28.792$.

(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 $\|\boldsymbol{v}_1\| = 28.792$. This is the same basis as in (c), in a different order.

7.50. A more efficient way to implement the LLL algorithm is described in Figure 7.9, with Reduce and Swap subroutines given in Figure 7.10. (This implementation of LLL follows [28, Algorithm 2.6.3]. We thank Henri Cohen for his permission to include it here.)

(a) Prove that the algorithm described in Figures 7.9 and 7.10 returns an LLL reduced basis.

(b) For any given N and q, let $L_{N,q}$ be the N-dimensional lattice with basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_N$ described by the formulas

$$\boldsymbol{v}_i = (r_{i1}, r_{i2}, \ldots, r_{iN}), \qquad r_{ij} \equiv (i+N)^j \pmod{q}, \qquad 0 \le r_{ij} < q.$$

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.

<u>Solution to Exercise 7.50</u>.

(b) We write L for the original basis and L' for the LLL reduced basis, and we write $\boldsymbol{v}$ for the shortest vector in the original basis and $\boldsymbol{v}'$ 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) $\boldsymbol{v}' = (-98, 166, -131, -18, 100, 28, 81, 50, -39, -39)$.

(ii) $\boldsymbol{v}' = (-122, -33, -59, 166, 9, -394, -46, 227, -148, -86, -46, 108, -214,$
$173, -107, 171, 34, -86, -153, -117)$.

(iii) $\boldsymbol{v}' = (98, -148, -263, -370, 76, 53, 258, -128, 221, -435, -119, -59, 142,$
$-336, 311, 290, 89, -538, 16, 437, 108, 361, 322, -374, 56, -117,$
$-208, -131, 645, 42)$.

(iv) $\boldsymbol{v}' = (192, -1426, 552, -292, 52, 482, 1046, -1344, -414, -226, -1413,$
$-1466, -447, 653, -484, -553, -284, 232, 1975, 1944, 27, 1203,$
$-1363, 707, 91, -549, -831, 974, 768, 1074, 57, -966, 1997,$
$2099, 828, -1295, -972, -842, 185, -2271)$.

The lengths, Hadamard ratios, and Gaussian expected shortest lengths are given in the following table:

	$\|\boldsymbol{v}\|$	$\|\boldsymbol{v}'\|$	$\mathcal{H}(L)$	$\mathcal{H}(L')$	$\sigma(L)$
(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

7.51. Let $\frac{1}{4} < \alpha < 1$ and suppose that we replace the Lovász condition with the condition

$$\|\boldsymbol{v}_i^*\|^2 \geq \left(\alpha - \mu_{i,i-1}^2\right) \|\boldsymbol{v}_{i-1}^*\|^2 \quad \text{for all } 1 < i \leq n. \tag{7.3}$$

(a) Prove a version of Theorem 7.69 assuming the alternative Lovász condition (7.64). What quantity, depending on α, replaces the 2 that appears in the estimates (7.54), (7.55), and (7.56)?

(b) Prove a version of Theorem 7.71 assuming the alternative Lovász condition (7.64). In particular, how does the upper bound for the number of swap steps depend on α? What happens as $\alpha \to 1$?

Solution to Exercise 7.51.

A solution for this exercise is not currently available.

7.52. Let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ 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 $y_1, \ldots, y_n \in \mathbb{R}$ we have

$$C_1^n \sum_{i=1}^n y_i^2 \|\boldsymbol{v}_i\|^2 \geq \left\| \sum_{i=1}^n y_i \boldsymbol{v}_i \right\|^2 \geq C_2^n \sum_{i=1}^n y_i^2 \|\boldsymbol{v}_i\|^2. \tag{7.4}$$

(This is a hard exercise.) We observe that the inequality (7.65) is another way of saying that the basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ is quasi-orthogonal, since if it were truly orthogonal, then we would have an equality $\|\sum y_i \boldsymbol{v}_i\|^2 = \sum y_i^2 \|\boldsymbol{v}_i\|^2$.

```
[1]  Input a basis $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ for a lattice $L$
[2]  Set $k = 2$, $k_{\max} = 1$, $\boldsymbol{v}_1^* = \boldsymbol{v}_1$, and $B_1 = \|\boldsymbol{v}_1\|^2$
[3]  If $k \le k_{\max}$ go to Step [9]
[4]  Set $k_{\max} = k$ and $\boldsymbol{v}_k^* = \boldsymbol{v}_k$
[5]  Loop $j = 1, 2, \ldots, k-1$
[6]      Set $\mu_{k,j} = \boldsymbol{v}_k \cdot \boldsymbol{v}_j^* / B_j$ and $\boldsymbol{v}_k^* = \boldsymbol{v}_k^* - \mu_{k,j}\boldsymbol{v}_j^*$
[7]  End $j$ Loop
[8]  Set $B_k = \|\boldsymbol{v}_k^*\|^2$
[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 $\ell = k-2, k-3, \ldots, 2, 1$
[15]         Execute Subroutine RED$(k, \ell)$
[16]     End $\ell$ Loop
[17]     Set $k = k+1$
[18] End If
[19] If $k \le n$ go to Step [3]
[20] Return LLL reduced basis $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$
```

Figure 7.1: The LLL algorithm—Main routine

(b) Prove that there is a constant C such that for any target vector $\boldsymbol{w} \in \mathbb{R}^n$, Babai's algorithm (Theorem 7.34) finds a lattice vector $\boldsymbol{v} \in L$ satisfying

$$\|\boldsymbol{w} - \boldsymbol{v}\| \le C^n \min_{\boldsymbol{u} \in L} \|\boldsymbol{w} - \boldsymbol{u}\|.$$

Thus Babai's algorithm applied with an LLL reduced basis solves apprCVP to within a factor of C^n. This is Theorem 7.76.

(c) Find explicit values for the constants C_1, C_2, and C in (a) and (b).

Solution to Exercise 7.52.

(a) This is a hard exercise. We follow the proof given in [**?**, §5.7].

Fix a basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$, let $\boldsymbol{v}_1^*, \ldots, \boldsymbol{v}_n^*$ be the associated Gram–Schmidt orthogonalized basis, and let

$$\boldsymbol{e}_i = \boldsymbol{v}_i^* / \|\boldsymbol{v}_i^*\|, \quad 1 \le i \le n,$$

be the associated orthonormal basis. Let $\mu_{i,j}$ be as usual (settting $\mu_{i,i} = 1$ and $\mu_{i,j} = 0$ for $i > j$), so the change of basis matrix $M = (\mu_{i,j})$ satisfies

$$V = V^* M.$$

```
—— Subroutine RED($k,\ell$) ——
If $|\mu_{k,\ell}| \le \frac{1}{2}$, return to Main Routine
Set $m = \lfloor \mu_{k,\ell} \rceil$
Set $\boldsymbol{v}_k = \boldsymbol{v}_k - m\boldsymbol{v}_\ell$ and $\mu_{k,\ell} = \mu_{k,\ell} - m$
Loop $i = 1, 2, \ldots, \ell - 1$
    Set $\mu_{k,i} = \mu_{k,i} - m\mu_{\ell,i}$
End $i$ Loop
Return to Main Routine

—— Subroutine SWAP($k$) ——
Exchange $\boldsymbol{v}_{k-1}$ and $\boldsymbol{v}_k$
Loop $j = 1, 2, \ldots, k - 2$
    Exchange $\mu_{k-1,j}$ and $\mu_{k,j}$
End $j$ Loop
Set $\mu = \mu_{k,k-1}$ and $B = B_k + \mu^2 B_{k-1}$
Set $\mu_{k,k-1} = \mu B_{k-1}/B$ and $B_k = B_{k-1}B_k/B$ and $B_{k-1} = B$
Loop $i = k+1, k+2, \ldots, k_{\max}$
    Set $m = \mu_{i,k}$ and $\mu_{i,k} = \mu_{i,k-1} - \mu m$ and $\mu_{i,k-1} = m + \mu_{k,k-1}\mu_{i,k}$
End $i$ Loop
Return to Main Routine
```

Figure 7.2: The LLL algorithm—RED and SWAP subroutines

(The rows of V are $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ and the rows of V^* are $\boldsymbol{v}_1^*, \ldots, \boldsymbol{v}_n^*$.)

In general, for any linear transformation A, we write $A = (a_{i,j})$ as a matrix relative to the orthonormal basis $\boldsymbol{e}_1^*, \ldots, \boldsymbol{e}_n^*$ and define

$$\|A\| = \sup_{\boldsymbol{0} \ne \boldsymbol{v} \in \mathbb{R}^n} \frac{\|\boldsymbol{v}A\|}{\|\boldsymbol{v}\|} \qquad \text{and} \qquad \|A\|_{\boldsymbol{e}} = \sup_{i,j} |a_{i,j}|.$$

We observe that if $\boldsymbol{v} = \sum x_i \boldsymbol{e}_i^*$, then $\|\boldsymbol{v}\|^2 = \sum x_i^2$ and we have

$$\begin{aligned}
\|\boldsymbol{v}A\|^2 &= \left\| \sum_{i=1}^n x_i \sum_{j=1}^n a_{i,j} \boldsymbol{e}_j \right\|^2 \\
&= \sum_{j=1}^n \left(\sum_{i=1}^n x_i a_{i,j} \right)^2 \\
&\le \sum_{j=1}^n \|\boldsymbol{v}\|^2 \|\boldsymbol{a}_{\cdot,j}\|^2 && \text{(Cauchy–Schwartz),} \\
&\le \sum_{j=1}^n \|\boldsymbol{v}\|^2 n \|A|_{\boldsymbol{e}}^2 \\
&= n^2 \|A\|_{\boldsymbol{e}}^2 \|\boldsymbol{v}\|^2.
\end{aligned}$$

Taking square roots, dividing by $\|\boldsymbol{v}\|$, and taking the sup over nonzero $\boldsymbol{v}$ yields

$$\|A\| \le n\|A\|_{\boldsymbol{e}}.$$

To ease notation, we let

$$c_i = \|\boldsymbol{v}_i^*\|, \quad \text{so} \quad \boldsymbol{v}_i^* = c_i\boldsymbol{e}_i.$$

Now we compute

$$\begin{aligned}\boldsymbol{e}_iM = c_i^{-1}\boldsymbol{v}_i^*M = c_i^{-1}\boldsymbol{v}_i = c_i^{-1}\left(\boldsymbol{v}_i^* + \sum_{j=1}^{i-1}\mu_{i,j}\boldsymbol{v}_j^*\right) &= c_i^{-1}\left(c_i\boldsymbol{e}_i + \sum_{j=1}^{i-1}\mu_{i,j}c_j\boldsymbol{e}_j\right)\\ &= \boldsymbol{e}_i + \sum_{j=1}^{i-1}\mu_{i,j}c_i^{-1}c_j\boldsymbol{e}_j.\end{aligned}$$

So relative to the $\boldsymbol{e}$ basis, the linear transformation M has a matrix that is lower triangular with 1's on the diagonal and with ij^{th} entry satisfying

$$|\mu_{i,j}c_i^{-1}c_j| \le \frac{1}{2}\cdot\frac{\|\boldsymbol{v}_j^*\|}{\|\boldsymbol{v}_i^*\|} \le 2^{(i-j)/2-1}, \tag{7.5}$$

where for the last inequality we use (7.58) (N.B. This is where we use the fact that the basis is reduced, since the size condition gives $|\mu_{i,j}| \le \frac{1}{2}$ and the Lovász condition implies the estimate (7.58).) Therefore,

$$\|M\|_{\boldsymbol{e}} \le \max_{1\le j\le i\le n} 2^{(i-j)/2-1} = 2^{(n-3)/2}.$$

(If $n \le 2$, we need to replace this upper bound by 1.)

This allows us to get an upper bound

$$\begin{aligned}\left\|\sum_{i=1}^{n} y_i\boldsymbol{v}_i\right\|^2 = \|\boldsymbol{y}V\|^2 = \|\boldsymbol{y}V^*M\| \le \|\boldsymbol{y}V^*\|\,\|M\| \le \|\boldsymbol{y}V^*\|\cdot n\|M\|_{\boldsymbol{e}}\\ \le \|\boldsymbol{y}V^*\|n2^{(n-3)/2} = n2^{(n-3)/2}\sum_{i=1}^{n} y_i^2\|\boldsymbol{v}_i^*\|^2.\end{aligned} \tag{7.6}$$

To obtain a lower bound, we observe that

$$\begin{aligned}\sum_{i=1}^{n} y_i^2\|\boldsymbol{v}_i^*\|^2 = \|\boldsymbol{y}V^*\|^2 = \left\|\boldsymbol{y}VM^{-1}\right\|^2\\ \le \|\boldsymbol{y}V\|\left\|M^{-1}\right\|^2 = \left\|M^{-1}\right\|^2\left\|\sum_{i=1}^{n} y_i\boldsymbol{v}_i\right\|^2.\end{aligned} \tag{7.7}$$

So we need an upper bound for $\left\|M^{-1}\right\|$.

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 7.1. *Let $B = (b_{i,j})$ be the matrix of a linear transformation relative to an orthonormal basis $\{\boldsymbol{e}_i\}$. Suppose that there are positive constants β and γ so that*

$$b_{i,j} = 0 \text{ for } i \le j \quad \text{and} \quad |b_{i,j}| \le \gamma\delta^{j-i} \text{ for } i > j.$$

Then

$$\left\|B + B^2 + B^3 + \cdots + B^{n-1}\right\|_{\boldsymbol{e}} \le \gamma(\gamma+1)^{n-2}\delta^{n-1}.$$

Note that (**??**) tells us that the coefficients of N satisfy

$$|\text{coef. of } N| \le 2^{(i-j)/2-1} = \frac{1}{2}\cdot\left(\frac{1}{\sqrt{2}}\right)^{j-i}.$$

So we can apply the lemma to N with $\gamma = 1/2$ and $\delta = 1/\sqrt{2}$, which gives

$$\left\|N + N^2 + \cdots + N^{n-1}\right\|_{\boldsymbol{e}} \le \frac{1}{2}\cdot\left(\frac{3}{2}\right)^{n-2}\cdot\left(\frac{1}{\sqrt{2}}\right)^{n-1} = \frac{1}{3}\left(\frac{9}{8}\right)^{(n-1)/2}.$$

Hence

$$\begin{aligned}\left\|M^{-1}\right\| \le n\left\|M^{-1}\right\|_{\boldsymbol{e}} &\le n\left(1 + \left\|N + N^2 + \cdots + N^{n-1}\right\|_{\boldsymbol{e}}\right)\\ &\le n + \frac{n}{3}\left(\frac{9}{8}\right)^{(n-1)/2} \le n\left(\frac{9}{8}\right)^{(n-1)/2}.\end{aligned}$$

(The last inequality is valid for $n \ge 8$. For smaller n, one can put in a small correction factor.)

Substituting into (**??**) gives

$$\sum_{i=1}^{n} y_i^2\|\boldsymbol{v}_i^*\|^2 \le n^2\left(\frac{9}{8}\right)^{n-1}\left\|\sum_{i=1}^{n} y_i\boldsymbol{v}_i\right\|^2. \tag{7.8}$$

We now apply (7.55) from Theorem 7.69, which says that $\|\boldsymbol{v}_i^*\|^2 \ge 2^{-(i-1)}\|\boldsymbol{v}_i\|^2$. This yields

$$\left\|\sum_{i=1}^{n} y_i\boldsymbol{v}_i\right\|^2 \ge n^{-2}\left(\frac{8}{9}\right)^{n-1}\sum_{i=1}^{n} y_i^2\cdot 2^{-(i-1)}\|\boldsymbol{v}_i\|^2 \ge n^{-2}\left(\frac{4}{9}\right)^{n-1}\sum_{i=1}^{n} y_i^2\|\boldsymbol{v}_i\|^2.$$

(b) Let $\boldsymbol{a} = \sum a_i \boldsymbol{v}_i \in L$ be any lattice vector, for example, it could be the lattice vector that is closest to $\boldsymbol{w}$. Write

$$\boldsymbol{w} = \sum \beta_i \boldsymbol{v}_i \quad \text{with } \beta_i \in \mathbb{R},$$

and let

$$\boldsymbol{b} = \sum b_i \boldsymbol{v}_i \quad \text{with} \quad b_i = \lfloor \beta_i \rceil$$

be the vector returned by Babai's algorithm. Also write

$$\beta_i = b_i + \delta_i \quad \text{with} \quad |\delta_i| \le \frac{1}{2}.$$

Then

$$\begin{aligned} \|\boldsymbol{w} - \boldsymbol{a}\|^2 &= \left\| \sum (\beta_i - a_i) \boldsymbol{v}_i \right\|^2 \\ &\ge C_2^n \sum (\beta_i - a_i)^2 \|\boldsymbol{v}_i\|^2 && \text{from (7.65)}, \\ &= C_2^n \sum (b_i - a_i + \delta_i)^2 \|\boldsymbol{v}_i\|^2. \end{aligned}$$

If $a_i \ne b_i$, then $|b_i - a_i| \ge 1$, so

$$(b_i - a_i + \delta_i)^2 \ge \frac{1}{4}(b_i - a_i)^2,$$

and clearly this is also valid if $a_i = b_i$. Hence using the other inequality in (7.65),

$$\begin{aligned} \|\boldsymbol{w} - \boldsymbol{a}\|^2 &\ge C_2^n \sum \frac{1}{4}(b_i - a_i)^2 \|\boldsymbol{v}_i\|^2 \\ &\ge \frac{1}{4} C_2^n C_1^{-n} \left\| \sum (b_i - a_i) \boldsymbol{v}_i \right\|^2 \\ &= \frac{1}{4} C_2^n C_1^{-n} \|\boldsymbol{b} - \boldsymbol{a}\|^2. \end{aligned}$$

Using the triangle inequality, we find that

$$\|\boldsymbol{w} - \boldsymbol{a}\| \ge \frac{1}{2}(C_2/C_1)^{n/2} \|\boldsymbol{b} - \boldsymbol{a}\| \ge \frac{1}{2}(C_2/C_1)^{n/2} \bigl(\|\boldsymbol{b} - \boldsymbol{w}\| - \|\boldsymbol{w} - \boldsymbol{a}\| \bigr),$$

and now a little bit of algebra yields

$$\|\boldsymbol{w} - \boldsymbol{b}\| \le \left(2 \left(\frac{C_1}{C_2} \right)^{n/2} + 1 \right) \|\boldsymbol{w} - \boldsymbol{a}\|.$$

This shows that the Babai vector $\boldsymbol{b}$ is the closest vector to $\boldsymbol{w}$ up to a factor of $2(C_1/C_2)^{n/2} + 1$.

```
Input a basis $v_1, \ldots, v_n$ of a lattice $L$.
Input a target vector $t$.
Compute Gram–Schmidt orthogonalized vectors $v_1^*, \ldots, v_n^*$ (Theorem 7.13).
Set $w = t$.
Loop $i = n, n-1, \ldots, 2, 1$
    Set $w = w - \lfloor w \cdot v_i^* / \|v_i^*\|^2 \rceil v_i$.
End $i$ Loop
Return the lattice vector $t - w$.
```

Figure 7.3: Babai's closest plane algorithm

7.53. Babai's *Closest Plane Algorithm*, which is described in Figure 7.11, 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 7.34 and Figure 7.11) 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 $\boldsymbol{t} = (-178, 117, -407, 419, -4, 252)$. (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 $\boldsymbol{t} = (-126, -377, -196, 455, -200, -234)$. (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 7.53.

(a) The Closest Plane Algorithm gives the vector

$$\boldsymbol{w} = (-185, 105, -414, 419, -8, 277) = (-1, -4, -13, -3, 12, 5)M_L \in L.$$

It satisfies $\|\boldsymbol{t} - \boldsymbol{w}\| = 29.7153$. The Closest Vertex Algorithm gives the vector

$$\boldsymbol{w} = (-159, 102, -425, 433, -3, 251) = (-1, -3, -13, -3, 12, 5)M_L \in L.$$

It satisfies $\|\boldsymbol{t} - \boldsymbol{w}\| = 33.2866$. So the Closest Plane Algorithm gives a slightly better result than the Closest Vertex Algorithm.

(b) The Closest Plane Algorithm gives the vector

$$\boldsymbol{w} = (-166, -394, -203, 460, -196, -204) = (-6, -13, 4, -12, -4, 3)M_L \in L.$$

It satisfies $\|\boldsymbol{t} - \boldsymbol{w}\| = 53.6563$. The Closest Vertex Algorithm gives the vector

$$\boldsymbol{w} = (-156, -385, -158, 470, -202, -207) = (-6, -12, 4, -12, -4, 3)M_L \in L.$$

It satisfies $\|\boldsymbol{t} - \boldsymbol{w}\| = 58.0172$. 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

$$\boldsymbol{w} = (-132, -367, -191, 467, -198, -263) = (-12, 6, 1, -9, 4, -4)M_L \in L.$$

It satisfies $\|\boldsymbol{t} - \boldsymbol{w}\| = 33.9116$. The Closest Vertex Algorithm gives the exact same result. So starting with an LLL reduced basis yields a significantly better solution to apprCVP.

7.54. We proved that the LLL algorithm terminates and has polynomial running time under the assumption that $L \subset \mathbb{Z}^n$; see Theorem 7.71. Show that this assumption is not necessary by proving that LLL terminates in polynomial time for any lattice $L \subset \mathbb{R}^n$. You may assume that your computer can do exact computations in $\mathbb{R}$, although in practice one does need to worry about round-off errors. (*Hint.* Use Hermite's theorem to derive a lower bound, depending on the length of the shortest vector in L, for the quantity D that appears in the proof of Theorem 7.71.)

Solution to Exercise 7.54.

The only place that the proof used the assumption that $L \subset \mathbb{Z}^n$ was in order to show that $d_\ell \geq 1$, which in turn was used to give the lower bound $D \geq 1$. In general, let

$$\tau(L) = \min_{\substack{\boldsymbol{w} \in L \\ \boldsymbol{w} \neq \boldsymbol{0}}} \|\boldsymbol{w}\|$$

be the length of a shortest nonzero vector in L. Then Hermite's theorem (and the fact that $L_\ell \subset L$) implies that

$$\sqrt{\ell}\,\det(L_\ell)^{1/\ell} \geq \tau(L_\ll) \geq \tau(L).$$

Hence

$$d_\ell = \det(L_\ell)^2 \geq \ell^{-\ell}\tau(L)^\ell,$$

from which we obtain

$$\begin{aligned} D &= \prod_{\ell=1}^{n} d_\ell \\ &\geq \prod_{\ell=1}^{n} \ell^{-\ell}\tau(L)^\ell \\ &\geq \prod_{\ell=1}^{n} n^{-n}\min\{1,\tau(L)\}^n \\ &= \left(\frac{\min\{1,\tau(L)\}}{n}\right)^{n^2}. \end{aligned}$$

This lower bound for D depends only on L, so D can be multiplied by $3/4$ only a finite number of times. Hence the LLL algorithm terminates. In order to estimate the running time, we use the estimate

$$\left(\frac{\min\{1,\tau(L)\}}{n}\right)^{n^2} \leq D_{\text{final}} \leq (3/4)^N D_{\text{init}}$$

and take logarithms to get

$$N = \mathcal{O}\left(n^2 \log\left(\frac{n}{\min\{1,\tau(L)\}}\right) + \log D_{\text{init}}\right).$$

Then the estimate $D_{\text{init}} \leq B^{n^2+n}$ that we used in the proof of the theorem gives an upper bound for the running time of

$$N = \mathcal{O}\left(n^2 \log\left(\frac{n}{\min\{1,\tau(L)\}}\right) + n^2 \log B\right).$$

Section. Applications of LLL to cryptanalysis

7.55. 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 7.1. 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 7.55.

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,

$$m = f^{-1}a = 94649 \cdot 94843884201 \equiv 186000 \pmod{g}.$$

7.56. Let

$$\boldsymbol{M} = (81946, 80956, 58407, 51650, 38136, 17032, 39658, 67468, 49203, 9546)$$

and let $S = 168296$. Use the LLL algorithm to solve the subset-sum problem for $\boldsymbol{M}$ and S, i.e., find a subset of the elements of $\boldsymbol{M}$ whose sum is S.

Solution to Exercise 7.56.

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

$$\boldsymbol{r} = (73, 160, 323, 657, 1325, 2660, 5348, 10698, 21396, 42807)$$

and the multiplier and modulus $A = 79809$ and $B = 85733$.

7.57. 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

$$\boldsymbol{e} = (388120266, -22516188, 1708295783, 1491331246, 453299858).$$

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 7.57.

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 $\boldsymbol{e}$. If we let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_5$ be the LLL-reduced basis vectors and $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_5$ be the original basis vectors, then

$$\begin{aligned}(388120256, &- 22516180, 1708295793, 1491331242, 453299848)\\ &= 1622959\boldsymbol{v}_1 + 2403687\boldsymbol{v}_2 - 4093270\boldsymbol{v}_3 - 1942134\boldsymbol{v}_4 - 1269978\boldsymbol{v}_5\\ &= -3\boldsymbol{w}_1 - 9\boldsymbol{w}_2 + 0\boldsymbol{w}_3 + 6\boldsymbol{w}_4 - 4\boldsymbol{w}_5.\end{aligned}$$

So Bob's plaintext is the vector $(-3, -9, 0, 6, -4)$.

7.58. Alice and Bob communicate using NTRUEncrypt with public parameters $(N, p, q, d) = (11, 3, 67, 3)$. Alice's public key is

$$\boldsymbol{h} = 39 + 9x + 33x^2 + 52x^3 + 58x^4 + 11x^5 + 38x^6 + 6x^7 + x^8 + 48x^9 + 41x^{10}.$$

Apply the LLL algorithm to the associated NTRU lattice to find an NTRU private key $(\boldsymbol{f}, \boldsymbol{g})$ for $\boldsymbol{h}$. Check your answer by verifying that $\boldsymbol{g} \equiv \boldsymbol{f} \star \boldsymbol{h} \pmod{q}$. Use the private key to decrypt the ciphertext

$$\boldsymbol{e} = 52 + 50x + 50x^2 + 61x^3 + 61x^4 + 7x^5 + 53x^6 + 46x^7 + 24x^8 + 17x^9 + 50x^{10}.$$

Solution to Exercise 7.58.

We apply LLL to the 22 dimensional NTRU lattice $L_{\boldsymbol{h}}^{\mathrm{NTRU}}$ associated to $\boldsymbol{h}$. 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

$$\begin{aligned}\boldsymbol{f}(x) &= -1 - x - x^2 - x^5 + x^7 + x^9 + x^{10}\\ \boldsymbol{g}(x) &= 1 + x - x^2 - x^5 - x^6 + x^8 - x^{10}.\end{aligned}$$

To decipher the message, we compute

$$\boldsymbol{a} \equiv \boldsymbol{f} \star \boldsymbol{e} \equiv -11-13x-1x^2+3x^3-4x^4+2x^5+16x^6+4x^7+4x^9-2x^{10} \pmod{q}.$$

Then we use

$$\boldsymbol{f}^{-1} \equiv -1 + x - x^3 + x^4 - x^6 + x^7 - x^8 - x^9 + x^{10} \pmod{3}$$

to compute the plaintext

$$\boldsymbol{m} \equiv \boldsymbol{a} \star \boldsymbol{f}^{-1} \equiv 1 - x - x^2 - x^3 - x^4 + x^7 + x^{10} \pmod{3}.$$

In vector form, $\boldsymbol{m} = (1, -1, -1, -1, -1, 0, 0, 1, 0, 0, 1)$.

7.59. (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 1.49 for a cryptosystem associated to this problem.

Solution to Exercise 7.59.

We do (b) first, then illustrate the general idea by doing (a). Let α 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

$$\sqrt{K} \approx J + \beta \qquad \text{for some } J \in \mathbb{Z}.$$

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

$$M = \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & t\beta \\ 0 & 0 & t\beta^2 \end{pmatrix},$$

where we will choose t later. Notice that

$$\begin{pmatrix} B & A & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & t\beta \\ 0 & 0 & t\beta^2 \end{pmatrix} = \begin{pmatrix} B & A & t(B + A\beta + \beta^2) \end{pmatrix}.$$

What we do is to choose t so that A, B, and $t(B+A\beta+\beta^2)$ are all about the same size. Then the vector $(B, A, t(B+A\beta+\beta^2))$ will be a small vector in the lattice generated by the rows of M. So we can hope that LLL applied to this lattice will give this small vector. In fact, our target vector may not be the smallest vector in the lattice, so we may need to try small linear combinations of the LLL basis vectors until we find $(B, A, t(B + A\beta + \beta^2))$.

A more careful analysis, which we leave to the reader, shows that A and B are both approximately equal to $2\sqrt{K}$, while $B + A\beta + \beta^2$ is approximately equal to $10^{-d}\sqrt{K}$, so taking $t \approx 10^d$ should work well.

(a) We are told that K is a 10 digit number, and we are given $d = 15$ digits after the decimal place of $\sqrt{K}$, namely $\beta = 0.418400286617716$. We take $t = 10^{15}$, so $t\beta = 418400286617716$ and $t\beta^2 = 175058799841786.8985151250567$. We can round this off, so we take the lattice generated by the rows of the matrix

$$\begin{pmatrix} 1 & 0 & 10^{15} \\ 0 & 1 & 418400286617716 \\ 0 & 0 & 175058799841787 \end{pmatrix}.$$

Applying LLL gives the matrix

$$\begin{pmatrix} -12420 & 9695 & -27668 \\ -4562 & 50882 & 35875 \\ 80169 & 19398 & -39511 \end{pmatrix}$$

Call the rows of this matrix $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, and $\boldsymbol{v}_3$. We note that $A = 2L$ has to be even, so $\boldsymbol{v}_1$ cannot be $(B, A, *)$. If we try setting $\boldsymbol{v}_2 = (B, A, *)$, then $B = -4562$ and $A = 50882$, then $K = \frac{1}{4}A^2 - B = 647249043$. This K has $\sqrt{K} = 25441.08966\cdots$, which is not what we want.

So we try various small linear combinations of $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, and $\boldsymbol{v}_3$. When we get to

$$2\boldsymbol{v}_1 + \boldsymbol{v}_2 = (-29402, 70272, -19461),$$

we obtain $A = 70272$, $B = -29402$, $K = \frac{1}{4}A^2 - B = 1234567898$, which yields $\sqrt{K} = 35136.41840028661771627694$. Eureka! We have found a 10 digit number K whose first 15 digits after the decimal place are the desired digits.

Chapter 8

Additional Topics in Cryptography

http://www.springer.com/978-1-4939-1710-5

An Introduction to Mathematical Cryptography
Hoffstein, J.; Pipher, J.; Silverman, J.H.
2014, XVII, 538 p. 32 illus., Hardcover
ISBN: 978-1-4939-1710-5