Introduction to Cryptology

by _____

Math 175
University of Michigan
Fall 2016

CHAPTER 1

Codes

Problem 1.1. YMWTZLMTZY YMNX BTWPXMJJY DTZ BNQQ GJ YMJ “GQZJ” LWTZU.

Problem 1.2. IK AHYXSDHO IDH FHZI YKAH CKQ MXEE FHHA IK NFKM MDPI NHCMKOA MPW QWHA. PWN IDH OHA VOKQS. XG PFCKFH PWNW CKQ GKO P NHCMKOA, IHEE IDHL “LXYDXVPF”.

Problem 1.3. SCFGH PWH LWJP WIVV NFHS EJ HVKBHA HSDW DMFWWUP DJ PWH HERY’O OEWJ XDS VZCNWEH?

CHAPTER 1

Codes

Problem 1.1. KYIFLXYFLK KYZJ NFIBJYVVK PFL NZCC SV KYV “XIVVE” XIFLG.

Problem 1.2. LY JNSXQENI LEN HNOL SYJN ZYC GXTT HNNJ LY RHYG GEML RNZGYIJ GMK CKNJ. MKR LEN ZNTTYG BIYCQ. XV MHZYHN MKRK ZYC VYI M RNZGYIJ, LNTT LENF “FMLENFMLXSK”.

Problem 1.3. YFSAW MUL HPCC DVCC TPRV TD KCEFBT MVOJ MTZQCXC XY MUL DXKL’V BLDP HNV KTFUQIB?

CHAPTER 1

Codes

Problem 1.1. HVFCIUVCIH HVWG KCFYGVSSH MCI KWZZ PS HVS “FSR” UFCID.

Problem 1.2. NK HYJPCGYD NGY IYLN JKHY UKM ZPOO IYYH NK SIKZ ZGEN SYUZKDH ZEQ MQYH. EQS NGY FOMY BDKMC. PT EIUKIY EQSQ UKM TKD E SYUZKDH, NYOO NGYR “ZKOAYDPIY”.

Problem 1.3. IWWSL EOH TIXL JKEA MJNL BU DROWFL BNIF YMUZIME VR GQB LODA’F SPVE ZHR WMADWXD?

CHAPTER 1

Codes

Problem 1.1. CQAXDPQXDC CQRB FXATBQNNC HXD FRUU KN CQN “HNUUXF” PAXDY.

Problem 1.2. UA ORXKEZRD UZR JRBU XAOR TAL SKVV JRRO UA FJAS SZGU FRTSADO SGI LIRO. GIF UZR YDRRJ YDALE. KN GJTAJR GIFI TAL NAD G FRTSADO, URVV UZRP “XDTEUAYDGEZT”.

Problem 1.3. IONSH KON PCNQ BXLR MBEM VG PEVVHQ TAQU EQSLHKQ IY GQM PIWU’X WNHE VZQ KXFAARW?

CHAPTER 1

Codes

Problem 1.1. XLVSYKLSYX XLMW ASVOWLIIX CSY AMPP FI XLI “TYVTPI” KVSYT.

Problem 1.2. DU XTHYMITB DIT ATWD HUXT SUR LYJJ ATTX DU FAUL LIPD LUBX LPE RETX. PEF DIT UBPAKT KBURM. YN PASUAT PEFE SUR NUB P FTSLUBX, DTJJ DITQ “GRJYRE”.

Problem 1.3. YOYDD PQU LSVV DEIF ASNE XG DVEOHW TYKS QWSJCGI AF PQU HADE’V KRGW KJE OWYNQRH?

CHAPTER 1

Codes

Problem 1.1. BPZWCOPWCB BPQA EWZSAPMMB GWC EQTT JM BPM "WZIVOM" OZWCX.

Problem 1.2. OY LSNZBESR OES FSIO NYLS XYD GZQQ FSSL OY AFYG GEUO GYRL GUT DTSL. UTA OES BDRBQS VRYDB. ZJ UFXYFS UTAT XYD JYR U ASXGYRL, OSQQ OESP "NUSTUR".

Problem 1.3. FIFTX QXO SIPW KYPV UTUY EW XWLIOM NZRM XMMKJAP QZ QXO OQXF'C EYWQ LQY VMSOXLO?

CHAPTER 2

Numbers

EXPERIMENT 2.1. Convert to text:

14130419221419071704 04

EXPERIMENT 2.2. Using the same approach as in Experiment 2.1, convert the following to numbers:

michiganmath

PROBLEM 2.3. How we can send messages made of letters by sending a number? What would we need to do to include punctuation?

Modern cryptography works by encoding numerical messages. Our goal now is to very carefully develop a theory of whole numbers (integers), so that we are 100% sure our encryption methods work as expected.

Experiment 2.4. Write down the first 5 whole numbers:

(1) In English.

(2) In your favorite language.

(3) So that each number is in its own language.

(4) In Roman numerals.

(5) In binary.

(6) In a way no other group will use.

PROBLEM 2.5. We think of all the things in Experiment 2.4 as "numbers". What are some things that they have in common?

PROBLEM 2.6. What assumptions should we make about integers for the rest of the course? List as few assumptions as possible, but make sure that they are enough to describe the integers.

PROBLEM 2.7. Use your axioms to prove or disprove:

(a) There is no biggest number.

(b) $5 = 3$

EXPERIMENT 2.8. What does $3 + 2$ mean? Use your fingers to explain, and then write down the idea.

PROBLEM 2.9 (Addition algorithm). Suppose you have two numbers x and y. Provide a list of instructions that computes $x + y$.

EXPERIMENT 2.10. Use your algorithm to compute $1 + 3$. How is it different from $3 + 1$?

PROBLEM 2.11 (Negation algorithm). Provide an algorithm that computes $-x$ for any integer x.

Supplementary Exercises

EXPERIMENT 2.12. What does $7 * 3$ mean?

PROBLEM 2.13 (Multiplication algorithm). Suppose you have two numbers x and y. Provide a list of instructions that computes $x * y$.

EXPERIMENT 2.14. Use your algorithms to compute $4 * 1$ and $1 * 4$. How are the two different?

CHAPTER 3

Modular Addition

DEFINITION 3.1. Let m and d be integers. We say "d *divides* m", which is abbreviated $d \mid m$, if there exists some integer k such that $m = dk$. We can also say that "d is a *divisor* of m" or that "m is a *multiple* of d".

EXPERIMENT 3.2. List some values of x such that $x \mid 6$. Do the same for values of x such that $6 \mid x$. What numbers are on both lists?

DEFINITION 3.3. Let a, b be arbitrary integers and let m be a positive integer. We say that "a and b are *congruent modulo* m", which is abbreviated $a \equiv b \pmod{m}$, when the difference $a - b$ is a multiple of m, i.e., when $m \mid (a - b)$.

EXPERIMENT 3.4. List several values of x such that $x \equiv 2 \pmod{6}$. Do the same for values of x such that $x \equiv 3 \pmod{5}$. Do your lists overlap?

PROBLEM 3.5. Write a formula, in terms of a variable integer k, for all the numbers in the set

$$\{x \in \mathbb{Z} \ : \ x \equiv 3 \pmod 7\}.$$

PROBLEM 3.6. What does it actually mean to write a formula for the set in Problem 3.5?

EXPERIMENT 3.7. Compare the sets of integers

$$S = \{x \in \mathbb{Z} \ : \ x \equiv 3 \pmod 7\}$$

and

$$T = \{x \in \mathbb{Z} \ : \ x \equiv 5 \pmod 7\}.$$

Can you find a number that is both in the set S and in the set T? Can you find a number in S which is 1 away from a number in T? How about numbers that are 2 away? What can you say about the relationship between S and T?

PROBLEM 3.8. Now let m be a positive integer and let b be any integer. Similarly to Problem 3.5, write a formula for all the numbers in the set

$$\{x \in \mathbb{Z} \ : \ x \equiv b \pmod{m}\}.$$

PROBLEM 3.9. Let a, b, c be arbitrary integers and let m be a positive integer. Explain why the following is true: if $a \equiv b \pmod{m}$ then

$$a + c \equiv b + c \pmod{m}.$$

THEOREM 3.10 (Modular Addition Theorem). Let m be a positive integer. If a, b, c, d are integers such that

$$a \equiv b \pmod{m} \quad \text{and} \quad c \equiv d \pmod{m},$$

then

$$a + c \equiv b + d \pmod{m}.$$

PROOF.

□

Supplementary Exercises

EXERCISE 3.1. Which of the following are true? Explain why or why not.

(a) $6 \mid 6$

(b) $-1 \mid 6$

(c) $7 \mid 1$

(d) $-1 \equiv 9 \pmod{10}$

(e) $0 \mid 4$

(f) $4 \mid 0$

(g) The number 2 is in the set

$$F = \{x \in \mathbb{Z} \ : \ x \equiv 0 \pmod{4}\}$$

(h) The number 4 is in the set

$$T = \{x \in \mathbb{Z} \ : \ x \equiv 0 \pmod{2}\}$$

CHAPTER 4

Shift Ciphers

PROBLEM 4.1. The following table provides the encoding rule for the Caesar cipher.

Plain Text	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
Cipher Text	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

If we replace the letters `A,B,...,Z` with the numbers 0,1,...,25, then the table provides a rule for converting numbers to other numbers. Rewrite the table using numbers.

PROBLEM 4.2. Using the table of Problem 4.1, find a function $f(x)$ which returns the encoded number corresponding to x when $x \in \{0, 1, 2, \ldots, 25\}$. Find a similar function $g(y)$ to decode the encoded number y.

PROBLEM 4.3. You discover a mysterious note which reads

`RJJY TS YMJ INFL FY KNAJ.`

Holding the note up to the light, you see a watermark:

Nuntius est occultus per aequatio $y = x +$ V *modulo* XXVI

What is the message?

PROBLEM 4.4. Julius Caesar sent the following message to one of his generals:

BKTO BOJO BOIO

For added security, Caesar encrypted the message twice with the Caesar shift. How would you decode this message? Can you determine the first and second shifts Caesar used?

PROBLEM 4.5. The following message was encrypted using a shift cipher:

K MKOCKB CRSPD SC OKCI DY MBKMU,

OCZOMSKVVI GROX DROBO SC K YXO VODDOB GYBN, VSUO K.

GRKD MYEVN GO NY DY WKUO K WYBO COMEBO MYNO?

Find the encoding and decoding functions as in Problem 4.2 and decrypt the message.

Supplementary Exercises

EXERCISE 4.1. The following table provides the encoding rule for the Caesar cipher.

Plain Text	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
Cipher Text	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

(a) Use Caesar's cipher to encode "But, for my own part, it was Greek to me".

(b) Decipher the following ciphertext created with Caesar's cipher: "`EHZDUH WKH LGHV RI PDUFK!`"

(c) Who wrote (a) and (b)? From where do the quotes come?

EXERCISE 4.2. Suppose that the ciphertext

```
WL LM, TJMLW! LZWF XSDD, USWKSJ.
```

was created by first using a shift cipher of some number of letters, then another shift was applied to the encoded text (possibly by a different amount). How will cracking this cipher compare to cracking the code if the sender only used one shift? Decipher the message.

EXERCISE 4.3. Find the functions that encode and decode the messages in Problems 4.1 and 4.2.

CHAPTER 5

Remainders

PROBLEM 5.1. Let a be an integer and m be a positive integer. Explain why there must be integers q and r such that $a = mq + r$. Is there more than one such pair q, r? How would you find another pair that works?

EXPERIMENT 5.2. For each of the following, find the smallest nonnegative integer r that satisfies the given congruence.

(a) $r \equiv 14 \pmod 3$

(b) $r \equiv 130 \pmod{26}$

(c) $r \equiv -1 \pmod 5$

(d) $r \equiv -258 \pmod{16}$

(e) $r \equiv -6553891137 \pmod{100}$

What are your observations?

THEOREM 5.3 (Division Algorithm). Let a be an integer and m be a positive integer. Then there is a *unique* pair of integers q and r such that $0 \leq r < m$ and $a = mq + r$.

PROOF.

□

DEFINITION 5.4. Let a be an integer and let m be a positive integer. We call the numbers q and r that satisfy

$$a = mq + r \quad \text{and} \quad 0 \leq r < m$$

the *quotient* and *remainder* of a divided by m, respectively. We will use

$$\text{QUO}\ (a, m)$$

to represent the quotient q of a divided by m and

$$\text{REM}\ (a, m)$$

to represent the remainder r of a divided by m.

That is, $\text{QUO}\ (a, m)$ and $\text{REM}\ (a, m)$ are the unique integers from the Division Algorithm such that

$$a = \text{QUO}\ (a, m)\, m + \text{REM}\ (a, m).$$

EXPERIMENT 5.5. Find $\text{QUO}\ (a, m)$ and $\text{REM}\ (a, m)$ for a and m as in Experiment 5.2.

EXPERIMENT 5.6. Let m be a positive integer and let a, b be integers. Which of the following statements are true? Are any sometimes true and other times false? Formulate a conjecture for each with supporting examples.

(a) For all integers a, b, c, $\text{QUO}\,(ab, bc) = \text{QUO}\,(a, c)$.

(b) If $a = \text{REM}\,(b, m)$ then $a \equiv b \pmod{m}$.

(c) If $a \equiv b \pmod{m}$ then $a = \text{REM}\,(b, m)$.

(d) If $\text{REM}\ (a, m) = \text{REM}\ (b, m)$ then $a \equiv b \pmod{m}$.

(e) If $a \equiv \text{REM}\ (b, m) \pmod{m}$ then $\text{REM}\ (a, m) \equiv b \pmod{m}$.

Supplementary Exercises

EXERCISE 5.1. Evaluate the following.

(a) $\text{REM}\,(22, 9) + 1$

(b) $\text{REM}\,(273, 10) - \text{REM}\,(10, 273)$

(c) $\text{QUO}\,(\text{QUO}\,(100, 13), 2)$

(d) $\text{REM}\,(\text{REM}\,(100, 13), 2)$

(e) $\text{QUO}\,(26, 8) + \text{REM}\,(26, 6)$

EXERCISE 5.2. Let a, b, and m be integers such that $a \equiv b \pmod{m}$. Explain why this implies that

$$a \equiv_{\text{REM}} (b, m) \pmod{m},$$
$$b \equiv_{\text{REM}} (a, m) \pmod{m},$$
$$\text{REM}\,(a, m) = \text{REM}\,(b, m).$$

EXERCISE 5.3. When is $\text{QUO}\,(a, m)$ equal to the usual fraction $\frac{a}{m}$?

CHAPTER 6

Modular Multiplication

EXPERIMENT 6.1. Given that $13 \equiv 2 \pmod{11}$ and $15 \equiv 4 \pmod{11}$, can you think of a way compute $\text{REM}\,(195, 11)$ without doing any division?

PROBLEM 6.2. Let m be a positive integer, and let a and c be integers. Suppose $a \equiv 3 \pmod{m}$ and $c \equiv 2 \pmod{m}$. Is $ac \equiv 6 \pmod{m}$? Why?

THEOREM 6.3 (Modular Multiplication). Let m be a positive integer. If a, b, c, d are integers such that

$$a \equiv b \pmod{m} \quad \text{and} \quad c \equiv d \pmod{m},$$

then

$$ac \equiv bd \pmod{m}.$$

PROOF.

□

PROBLEM 6.4. Let a, c, m, r, and s be integers such that $\text{REM}\ (a, m) = r$ and $\text{REM}\ (c, m) = s$. Is it always true that $\text{REM}\ (ac, m) = rs$? Why or why not?

EXPERIMENT 6.5. Define the functions

$$f(x) = \text{REM}\ (3x, 12) \quad \text{and} \quad g(x) = \text{REM}\ (5x, 12).$$

Complete the following table and note any differences you see between the values of f and g.

x	0	1	2	3	4	5	6	7	8	9	10	11
$f(x)$												
$g(x)$												

What might be the cause of the discrepancy?

PROBLEM 6.6. Let $f(x) = \text{REM}\ (5x, 26)$ and complete a table for $f(x)$ like the one in the previous problem. Convert letters to numbers by replacing `A` with 0, `B` with 1, `C` with 2, and so on. Then $f(x)$ defines a cipher for encoding plain text. Encode a short message with this cipher and trade messages with a neighboring group.

PROBLEM 6.7. How do we decode a message created with the cipher in the previous problem? Write a formula for a function $g(x)$ that will decode messages encoded by $f(x)$, i.e., a function such that $g(f(x)) = x$ for any number x. Make a table for $g(x)$ and decrypt the message you received from your neighbors.

PROBLEM 6.8. Why is the function $f(x) = \text{REM}\ (6x, 26)$ a bad function for encoding messages? For which numbers a is $f(x) = \text{REM}\ (ax, 26)$ good for encoding messages?

Supplementary Exercises

EXERCISE 6.1. Construct a multiplication table modulo 5, 6, 7, and 9. To write the table modulo m, label the rows and columns of a square $m \times m$ table with the numbers 0 to $m-1$. The entry in the row a and column b is REM (ab, m).)

What patterns do you see? Explain why some nonzero numbers multiply to give zero in the tables for 6 and 9. Why doesn't this happen in the tables for 5 and 7?

EXERCISE 6.2. For each of the following, find the smallest nonnegative integer x that satisfies the given congruence, or show that there is no such x.

(a) $3x \equiv 1 \pmod{26}$

(b) $4x \equiv 1 \pmod{12}$

(c) $5x \equiv 11 \pmod{13}$

(d) $2x \equiv -1 \pmod{17}$

(e) $79x \equiv 1 \pmod{80}$

CHAPTER 7

Multiplicative Inverses

DEFINITION 7.1. Let m be a positive integer and let a be any integer. The integer x is called a *multiplicative inverse* of a modulo m if $ax \equiv 1 \pmod{m}$.

EXPERIMENT 7.2. For each of the following choices of a and m, decide whether a has a multiplicative inverse modulo m. If it does, find at least two.

(a) $a = 0$, $m = 6$

(b) $a = 5$, $m = 9$

(c) $a = 9$, $m = 5$

(d) $a = 4$, $m = 15$

(e) $a = -4$, $m = 15$

(f) $a = 7$, $m = 21$

(g) $a = -2$, $m = 1$

THEOREM 7.3 (Uniqueness of Inverses). Let a be any integer and m be a positive integer. If x and y are both inverses of a modulo m, then $x \equiv y \pmod{m}$.

PROOF.

□

DEFINITION 7.4. Two integers a and b are *relatively prime* if they have no common divisors other than 1 and -1. In other words, a and b are relatively prime when $d \mid a$ and $d \mid b$ implies that $d = \pm 1$.

EXPERIMENT 7.5. For each of the following choices of a and b, decide whether a and b are relatively prime.

(a) $a = 0$, $b = 6$

(b) $a = 5$, $b = 9$

(c) $a = 9$, $b = 5$

(d) $a = 4$, $b = 15$

(e) $a = -4$, $b = 15$

(f) $a = 7$, $b = 21$

(g) $a = -2$, $b = 1$

How does this relate to your answers in Experiment 7.2?

PROBLEM 7.6. Let $a, m > 0$. Prove or disprove: there is a value of x such that $0 < x < m$ and $ax \equiv 0 \pmod{m}$.

THEOREM 7.7. If a has an inverse modulo m then a is relatively prime with m.

PROOF.

□

Supplementary Exercises

EXERCISE 7.1. For the following pairs of integers, find an inverse b of a modulo m such that $0 < b < m$.

(a) $a = -1$, $m = 63$

(b) $a = 5$, $m = 24$

(c) $a = -5$, $m = 24$

(d) $a = 6$, $m = 37$

(e) $a = 9999$, $m = 10000$

EXERCISE 7.2. Let n be a positive integer. Explain why $n-1$ is its own inverse modulo n for every integer $n \geq 2$. Why did we exclude $n = 1$?

EXERCISE 7.3. In Kid Krypto (see lab), we had an encoding function

$$\text{enc}(x) = \text{REM } (ex, n)$$

and decoding function

$$\text{dec}(x) = \text{REM } (fx, n).$$

For our decoding function to work, we want to know that

$$\text{dec}(\text{enc}(x)) = x$$

for every $0 \leq x < n$. Explain why this is true. That is, prove that Kid Krypto always works. (*Hint.* Expand the above composition using the definition of REM (a, m) and prove that e is an inverse of f modulo n.)

CHAPTER 8

Affine ciphers

DEFINITION 8.1. An *affine cipher* is defined by the encoding formula

$$f(x) = \text{REM } (ax + b, 26)$$

where a and b are integers. (We use the standard correspondence between numbers and letters: `A` is 0, `B` is 1, `C` is 2, and so on.)

PROBLEM 8.2. The message

`ETTCRQ KCXZQDG EDQ QEGY,`

`URKQ YUM IRUS CRPQDGQG OUNMLU O.`

was encoded using the affine cipher

$$f(x) = \text{REM } (3x + 4, 26).$$

Decode the message and come up with a formula for the decoding cipher. In other words, find c and d such that the decoding cipher is $g(x) = \text{REM } (cx + d, 26)$.

PROBLEM 8.3. Why is $f(x) = \text{REM } (13x+1, 26)$ not a good affine cipher?

PROBLEM 8.4. Come up with a necessary and sufficient condition for

$$f(x) = \text{REM } (ax + b, 26)$$

to be a good affine cipher. If f is a good affine cipher, describe a way to find the decoding function.

PROBLEM 8.5. The Roman alphabet in Caesar's time only had 23 letters. Can you find a function $f(x) = \text{REM } (ax + b, 23)$, $1 \leq a \leq 22$ that would be a bad affine cipher? Why or why not?

Supplementary Exercises

EXERCISE 8.1. Look up how a *rail fence transposition cipher* works. Decode the following message, which was created with a two-level rail fence cipher:

```
IIAEE NUTEI IBSAD NOTEH UDROG ATFHV SEFRH RTSYT NIGNH SOLES FINS
```

Who said this?

EXERCISE 8.2. Look up *keyword columnar transposition ciphers*. Decipher the following message that was created in this way.

```
FNNARBESTGHRIEERESSTSNSEVEAHIUNEIYDXASFTTAARDMLXHTSOICIENNUXIOASSEGWAOOS
```

(*Hint.* The keyword has six letters and is related to the previous problem.)

EXERCISE 8.3. For the following questions refer to the *Vigenère cipher*.

(a) Encode the following message using the Vigenère cipher with keyword given by the (four letter) author of the quotation:

```
My purpose is to tell of bodies which have been transformed into
shapes of a different kind.
```

(b) Decode the following message created with the keyword `HOUSE`:

```
VJYJH PRSGY ZOSGZ LFHGX OWHYM ZCPWV BBNAP DSXWG PRYAX PGQSW PHINI
YKBWR AVYYI YAUFW ICGTI KDYSV SVUJF VFBWP SBIXZ
```

(c) A long message has been encoded using the Vigenère cipher with a key of length m. An enemy has intercepted the cipher text and wants to decode it.

The enemy guesses that it is encoded by the Vigenère method, and guesses that the key has length ℓ. Then he extracts from the cipher text a subsequence consisting of every ℓ-th letter. If his guess about the length is right (i.e., $\ell = m$), then all the extracted letters were encoded using the same letter of the key. If his guess is wrong ($\ell \neq m$), then how many letters of the key were used in coding the letters he extracted? Your answer should be in terms of ℓ and m.

In particular, under what circumstances (i.e., under what conditions on ℓ and m) would all the letters of the key be used in producing the extracted subsequence of the cipher text? You may assume that the text is long compared to ℓ and m and even compared to ℓm. You may also assume that the key doesn't contain any repeated letters.

CHAPTER 9

The Euclidean algorithm

DEFINITION 9.1. Let a and b be integers, and assume at least one is not 0. The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is the largest integer d such that $d \mid a$ and $d \mid b$. By convention, we define $\gcd(0, 0) = 0$.

EXPERIMENT 9.2. For each of the following examples, find $\gcd(a, b)$.

(a) $a = 75, b = 90$

(b) $a = 189, b = 343$

(c) $a = 54435, b = 285$

(d) $a = 37$, $b = 0$

EXPERIMENT 9.3. For each of the following, find $r = \text{REM}\ (a, b)$, $q = \text{QUO}\ (a, b)$ as well as $\gcd(a, b)$.

(a) $a = 168, b = 84$

(b) $a = -252, b = 168$

(c) $a = 420, b = 252$

(d) $a = 1092, b = 420$

(e) $a = 1512, b = 1092$

PROBLEM 9.4. Let a and b be two positive integers with $a \geq b$, and write $a = qb + r$, where $r = \text{REM}\ (a, b)$ and $q = \text{QUO}\ (a, b)$.

(a) Assume that $r = 0$. What can you say about $\gcd(a, b)$?

(b) Now, assume that $r \neq 0$. What can you say about the relationship between $\gcd(a, b)$ and $\gcd(b, r)$?

THEOREM 9.5. Let a and b be two positive integers with $a \geq b$, and use the division algorithm to write $a = qb + r$ for $r = \text{REM}\ (a, b)$ and $q = \text{QUO}\ (a, b)$. Then ...

PROOF.

□

PROBLEM 9.6. Explain how Theorem 9.5 allows you to do Experiment 9.3 without computing all the divisors of every number.

PROBLEM 9.7. Use your solutions to the last few problems to help you find $\gcd(1850, 1221)$. The method you just used is called the *Euclidean Algorithm*.

Supplementary Exercises

EXERCISE 9.1. Use the Euclidean Algorithm to find the greatest common divisor of the following pairs of integers.

(a) $a = 14$ and $b = 21$.

(b) $a = 29$ and $b = 101$.

(c) $a = -169$ and $b = 91$.

(d) $a = 2604$ and $b = 2046$.

(e) $a = 1187$ and $b = 827$.

(f) $a = n$ and $b = n - 1$, where n is any positive integer.

CHAPTER 10

The extended Euclidean algorithm

EXPERIMENT 10.1. Consider the following equations:

$$360 = 1 \cdot 294 + 66$$
$$294 = 4 \cdot 66 + 30$$
$$66 = 2 \cdot 30 + 6$$

What is $\gcd(360, 294)$? How about $\gcd(294, 30)$ and $\gcd(30, 6)$? We can rearrange these equations as:

$$360 - 1 \cdot 294 = 66 \quad (1)$$
$$294 - 4 \cdot 66 = 30 \quad (2)$$
$$66 - 2 \cdot 30 = 6 \quad (3)$$

(a) Substitute the left side of equation (2) for the 30 in equation (3). We see that some multiple of 66 plus some multiple of 294 equals 6. Call this equation (4).

(b) Do a similar substitution of equation (1) into equation (4).

(c) Find two integers s, t such that $360s + 294t = 6$.

PROBLEM 10.2. The method you used in Experiment 10.1 is called the *extended Euclidean algorithm*.

(a) Find integers s and t such that $57s + 81t = \gcd(57, 81)$.

(b) Find integers s and t such that $234s + 24t = \gcd(234, 24)$.

(c) Are there integers s and t such that $52s + 18t = 1$? Why or why not?

THEOREM 10.3 (Bézout's Lemma). For any two integers a, b there exist integers s and t such that

$$as + bt = \gcd(a, b).$$

PROOF.

□

EXPERIMENT 10.4. Use the extended Euclidean algorithm to do the following.

(a) Compute an inverse of 63 modulo 95 and an inverse of 95 modulo 63.

(b) Find an inverse of 73 modulo 191 and an inverse of 191 modulo 73.

THEOREM 10.5 (Existence of Inverses). Let m be a positive integer. An integer a has an inverse modulo m if and only if a is relatively prime to m.

PROOF.

□

Supplementary Exercises

EXERCISE 10.1. Use the Euclidean algorithm to find the greatest common divisor of the following pairs of integers and integers s and t such that $as + bt = \gcd(a, b)$.

(a) $a = 2604$, $b = 2046$

(b) $a = 1187$, $b = 827$

EXERCISE 10.2. Solve the following using your answer to Problem 10.1(b).

(a) Find the smallest nonnegative integer x such that

$$x \equiv 0 \pmod{1187} \qquad \text{and} \qquad x \equiv 1 \pmod{827}.$$

(b) Find the smallest nonnegative integer x such that

$$x \equiv 1 \pmod{1187} \qquad \text{and} \qquad x \equiv 0 \pmod{827}.$$

(c) Find the smallest nonnegative integer x such that

$$x \equiv 3 \pmod{1187} \qquad \text{and} \qquad x \equiv 2 \pmod{827}.$$

EXERCISE 10.3. Find an inverse of 37 modulo 191, if such a thing exists.

CHAPTER 11

RSA encryption

EXPERIMENT 11.1. Compute 2^8 by hand in two ways:

(a) By multiplying 2 by itself 8 times.

(b) Using only 3 multiplications.

EXPERIMENT 11.2. (a) Compute $\text{REM}\,(584^2, 10)$ in your head.

(b) Compute $\text{REM}\,(73^{13}, 10)$ by hand.

RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman, who first published the algorithm in 1978. We will see that RSA is much more difficult to break than Kid Krypto because factoring integers is surprisingly difficult compared to computing inverses modulo m.

DEFINITION 11.3 (RSA Key Generation). To generate a *RSA public and private keys* choose two prime numbers p and q and calculate

$$n = pq$$
$$m = (p-1)(q-1).$$

Next, choose a positive integer e that is relatively prime to m and compute an inverse d of e modulo m. At this point, securely discard the numbers p, q, and m. The *RSA public key* consists of the numbers e and n. The *RSA private key* consists of the numbers d and n.

EXPERIMENT 11.4. Generate RSA keys using the primes $p = 7$, $q = 11$.

(a) Compute n and m.

(b) Verify that $e = 13$ is relatively prime to m and compute an inverse d of 13 modulo m.

DEFINITION 11.5 (RSA Encryption & Decryption). RSA messages are represented using numbers in the range $0, 1, \ldots, n-1$.

- To encrypt and send a message x using the public key e, n, compute the number $y = \text{REM}\ (x^e, n)$ and send y.
- To decrypt a message y, encrypted as above, use the private key d to compute $\text{REM}\ (y^d, n)$ to recover the original message x.

EXPERIMENT 11.6. Use the RSA keys you generated in Experiment 11.4.

(a) Encrypt the message $x = 42$ by computing $y = \text{REM}\ (x^e, n)$.

(b) Decrypt the message y by computing $\text{REM}\ (y^d, n)$.

PROBLEM 11.7. Nora publishes her RSA public key $e = 5715$ and $n = 30967$. You intercept the following RSA encrypted message from Nick to Nora: 30384. Do you think it is possible to decode Nick's original message? How might you do it?

(a) Find the values of p and q that Nora used.

(b) Find Nora's private key d.

(c) Recover Nick's message.

Supplementary Exercises

To crack the RSA, it's enough to factor the number n into p and q, since we can then compute the private key f. Doing this directly for large n is extremely time-consuming using any known algorithm.

In this homework, we'd like to see that just discovering m allows us to quickly find p and q. It's also true that discovering f makes it possible to quickly find p and q, so cracking the RSA is just as hard as factoring n.

EXERCISE 11.1. Nick wasn't very careful when generating his RSA keys. Digging through his computer's trash bin, you found the number $m = 5\,331\,408$ that he used. Knowing his public key $e = 17$ and $n = 5\,336\,063$, find the numbers p and q that Nick used to generate his RSA keys.

EXERCISE 11.2. Come up with a general way to find p and q given m and n? (*Hint*: Find an expression of the form $ap^2 + bp + c = 0$, where a, b, c depend only on m and n and use the quadratic formula.)

EXERCISE 11.3. **Start this problem as soon as possible.**

(a) Pick two large primes, at least 10 digits each. (Hint: about a tenth of 10-digit numbers are prime.)

(b) Use your primes to create an RSA public key and post it along with your name on Piazza **at the latest two days before this homework is due**.

(c) I will encode a message and post it publicly as a response on Piazza. What message did I send you?

(d) (Optional) Decode at least one message that I sent to another person. The top 3 hackers get stickers.