

Written Homework 02 Solutions

Assigned: Thu 15 Oct 2009

Due: Thu 22 Oct 2009

Instructions:

- The assignment is due at the *beginning* of class on the due date specified. Late assignments will be penalized 50%, as stated in the course information sheet. Late assignments *will not be accepted* after the solutions have been distributed.
- We expect that you will study with friends and often work out problem solutions together; however, you must write up you own solutions, in your own words. Cheating will not be tolerated.
- We expect your homework to be neat, organized, and legible. If your handwriting is unreadable, please type your solutions. Use 8.5in by 11in loose-leaf or printer paper, and please do not hand in sheets that have been ripped from spiral bound notebooks.

Problem 1 [30 pts; (2,3,5,5,10,2,3)]: **Linear Ciphers**

A spy has been captured, but all attempts to interrogate him have failed; he seems to speak a strange language, unintelligible to any translator. However, this spy was caught with a number of documents. Linguists who have studied these documents believe that they were written in the spy’s language, but that they have been encrypted. Decrypting these documents to obtain valid text in the spy’s language would be incredibly helpful; your job is to decrypt the spy’s documents and hopefully determine where he’s from and what language he speaks.

Linguists analyzing the spy’s documents have determined that the spy’s language uses the familiar 26 English letters, which are encoded and decoded using the numbers $\{0, \dots, 25\}$ in the usual way.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

You suspect that the spy has used a linear encryption scheme with $m = 17$ and $k = 11$ since symbols representing these values were found tattooed on the spy’s scalp. Finally, the linguists and interrogators are particularly interested in the following phrase, which they believe is the *pass phrase* that the spy uses to authenticate himself to his contacts:

srlw infwrwrl onlw tlbqnh

- i. Encode each letter in the above phrase in the usual way, i.e., $s \rightarrow 18$, $r \rightarrow 17$, and so on.
- ii. Since you suspect that these values were encrypted using the function

$$num \rightarrow (17 \cdot num + 11) \pmod{26}$$

you must subtract 11 (mod 26) and then multiply by the multiplicative inverse of 17 (mod 26) in order to decrypt these values. Start by subtracting 11 (mod 26).

To compute the multiplicative inverse of an integer a , mod n , we must find an integer b , $0 < b < n$, such that $a \cdot b \equiv 1 \pmod{n}$. One could try all possibilities for b ; however, one can *solve* for b in a number of ways. One method is to use the Extended Euclidean Algorithm, as discussed in class and described in the text. In what follows, we describe another method based on modular exponentiation.

For any positive integer n , the Euler totient function $\varphi(n)$ is defined to be the number of positive integers less than n that are *relatively prime* to n ; in other words, it is the number of integers less than n that share no common factors with n . For example, $\varphi(10) = 4$ since the integers 1, 3, 7, and 9 are relatively prime to 10. The Euler totient function can be computed in a number of ways without having to list all possible integers less than n and check whether they are relatively prime to n ; perhaps the simplest formula is the following

$$\begin{aligned}\varphi(n) &= n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)\end{aligned}$$

where p_i are the *prime factors* of n . For example, the prime factors of 10 are 2 and 5; thus, we have

$$\begin{aligned}\varphi(10) &= 10 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \\ &= 10 \cdot (1/2) \cdot (4/5) \\ &= 4\end{aligned}$$

which is correct, as we saw above. This formula works in a manner similar to the Sieve of Eratosthenes: Since 2 is a factor of 10, every even number (i.e., *multiples of 2*) will share a factor with 10; thus, we can eliminate half the integers less than 10, resulting in the $(1 - 1/2)$ factor in the formula above; furthermore, since 5 is a factor of 10, we can eliminate every fifth integer (i.e., the *multiples of 5*), resulting in the $(1 - 1/5)$ factor; and so on.

iii. Compute $\varphi(26)$ using the method described above.

The Euler totient function is useful in computing the multiplicative inverses of integers $a \pmod{n}$ due to the following mathematical fact, known as *Euler's Theorem*.

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

How is this result useful? Since $a^{\varphi(n)} = a \cdot a^{\varphi(n)-1}$, we have

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

and thus, $a^{\varphi(n)-1} \pmod{n}$ is the multiplicative inverse of $a \pmod{n}$. Note that to compute $a^{\varphi(n)-1} \pmod{n}$ efficiently, one would use the method for modular exponentiation described in class and in the text.

iv. Compute the multiplicative inverse of 17 (mod 26) using the method described above. Verify that your answer is correct; i.e., letting b be the multiplicative inverse you compute, verify that $17 \cdot b \equiv 1 \pmod{26}$.

- v. Given the multiplicative inverse of 17, you can now complete the decryption you started in part ii above. Decrypt each encoded character by inverting the linear encryption.
- vi. Decode these values in the usual way to obtain a phrase in the spy's language. (It will *not* be intelligible to most people.)
- vii. Conduct some research on the web to see if you can determine what this phrase means. (Try typing the decrypted words or the entire phrase into Google.) What is the English translation of this phrase? What language does the spy speak?

Solution:

- i. Using the table given in the problem, the encoding of the phrase is

s	r	l	w		i	n	f	w	r	w	r	l
18	17	11	22		8	13	5	22	17	22	17	11

o	n	l	w		t	l	b	q	n	h
14	13	11	22		19	11	1	16	13	7

- ii. Subtracting 11 mod 26 gives

s	r	l	w		i	n	f	w	r	w	r	l
18	17	11	22		8	13	5	22	17	22	17	11
7	6	0	11		23	2	20	11	6	11	6	0

o	n	l	w		t	l	b	q	n	h
14	13	11	22		19	11	1	16	13	7
3	2	0	11		8	0	16	5	2	22

- iii. To compute $\varphi(26)$, first you need the prime factorization $26 = 2 \times 13$

$$\begin{aligned}
 \varphi(26) &= 26 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{13}\right) \\
 &= 26 \times \left(\frac{1}{2}\right) \times \left(\frac{12}{13}\right) \\
 &= 12
 \end{aligned}$$

- iv. We need to determine the multiplicative inverse of 17 mod 26 using the Euler Totient function: The multiplicative inverse is $a^{\varphi(n)-1} \bmod n$

$$\begin{aligned}
 17^{\varphi(26)-1} \bmod 26 &= 17^{11} \bmod 26 \\
 &= 17 \times 17^2 \times 17^8 \bmod 26 \\
 &= 17 \times 3 \times 3 \bmod 26 \\
 &= 23
 \end{aligned}$$

23 is the multiplicative inverse of 17 mod 26.

v. To finish the decryption, we multiply by 23.

Cyphertext	s	r	l	w		i	n	f	w	r	w	r	l
Cyphersymbol	18	17	11	22		8	13	5	22	17	22	17	11
Subtract 11	7	6	0	11		23	2	20	11	6	11	6	0
Multiply by 23	5	8	0	19		9	20	18	19	8	19	8	0

Cyphertext	o	n	l	w		t	l	b	q	n	h
Cyphersymbol	14	13	11	22		19	11	1	16	13	7
Subtract 11	3	2	0	11		8	0	16	5	2	22
Multiply by 23	17	20	0	19		2	0	4	11	20	12

vi. Using the table given in the problem, we can convert the symbols to plaintext.

Cyphertext	s	r	l	w		i	n	f	w	r	w	r	l
Cyphersymbol	18	17	11	22		8	13	5	22	17	22	17	11
Subtract 11	7	6	0	11		23	2	20	11	6	11	6	0
Multiply by 23	5	8	0	19		9	20	18	19	8	19	8	0
Plaintext	f	i	a	t		j	u	s	t	i	t	i	a

Cyphertext	o	n	l	w		t	l	b	q	n	h
Cyphersymbol	14	13	11	22		19	11	1	16	13	7
Subtract 11	3	2	0	11		8	0	16	5	2	22
Multiply by 23	17	20	0	19		2	0	4	11	20	12
Plaintext	r	u	a	t		c	a	e	l	u	m

vii. The phrase “fiat justitia caelum” is in the language Latin, and it translates to “Do justice, let the sky fall”.

Problem 2 [20 pts; (5,10,5)]: Mod Multiplication Patterns

- i. List all natural numbers less than 15 that are relatively prime to 15 (i.e., those natural numbers that do not share a common factor with 15).
- ii. Construct the multiplication table, mod 15, for only the numbers that you obtained in your solution to part i. That is, the row headers and the column headers of the table should include precisely the numbers you obtained in your solution to part i.
- iii. Discuss any patterns you see in the multiplication table and why they occur.

Solution:

- i. The following numbers are relatively prime to 15:
1,2,4,7,8,11,13,14.
- ii.

	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

iii. The \times table is symmetric along both diagonals. It reflects along the NW–SE diagonal because \times is commutative ($ab = ba$) and it reflects along the SW–NE diagonal because $(-a)(-b) = ab$. Also, every row and column is a permutation of the set $\{1, 2, 4, 7, 8, 11, 13, 14\}$. This indicates that every number in the set has a multiplicative inverse that is also in the set.

Problem 3 [20 pts; (5,5,5,5)]: **Prime Factorization and Euclid’s Algorithm**

Compute the following. Show *all* of your work.

- i. $\gcd(752, 72)$ using prime factorization.
- ii. $\gcd(252, 116)$ using Euclid’s algorithm.
- iii. $\gcd(492, 397)$ using Euclid’s algorithm.
- iv. $\text{lcm}(525, 252)$ by first computing the gcd using Euclid’s algorithm.

Solution:

i.

$$\begin{aligned} \gcd(752, 72) &= \gcd(2^4 \times 47, 2^3 \times 3^2) \\ &= 2^3 \times 3^0 \times 47^0 \\ &= 8 \end{aligned}$$

ii.

$$\begin{aligned} \gcd(252, 116) &= \gcd(116, 252 \bmod 116) \\ &= \gcd(116, 20) \\ &= \gcd(20, 116 \bmod 20) \\ &= \gcd(20, 16) \\ &= \gcd(16, 20 \bmod 16) \\ &= \gcd(16, 4) \\ &= \gcd(4, 16 \bmod 4) \\ &= \gcd(4, 0) \\ &= 4 \end{aligned}$$

iii.

$$\begin{aligned}\gcd(492, 397) &= \gcd(397, 492 \bmod 397) \\ &= \gcd(397, 95) \\ &= \gcd(95, 397 \bmod 95) \\ &= \gcd(95, 17) \\ &= \gcd(17, 95 \bmod 17) \\ &= \gcd(17, 10) \\ &= \gcd(10, 17 \bmod 10) \\ &= \gcd(10, 7) \\ &= \gcd(7, 10 \bmod 7) \\ &= \gcd(7, 3) \\ &= \gcd(3, 7 \bmod 3) \\ &= \gcd(3, 1) \\ &= \gcd(1, 3 \bmod 1) \\ &= \gcd(1, 0) \\ &= 1\end{aligned}$$

iv.

$$\begin{aligned}\gcd(525, 252) &= \gcd(252, 525 \bmod 252) \\ &= \gcd(252, 21) \\ &= \gcd(21, 252 \bmod 21) \\ &= \gcd(21, 0) \\ &= 21\end{aligned}$$

$$525 \times 252 = \gcd(525, 252) \times \text{lcm}(525, 252)$$

$$\frac{525 \times 252}{\gcd(525, 252)} = \text{lcm}(525, 252)$$

$$\frac{525 \times 252}{21} = 6300$$

$$\text{lcm}(525, 252) = 6300$$

Problem 4 [30 pts; (5,5,10,10)]: An Alternative GCD Algorithm

Euclid's algorithm computes the gcd of two positive numbers a and b ($a \geq b$) by reducing the problem to that of computing the gcd of b and $(a \bmod b)$, where $a \bmod b$ is often much smaller than a . Thus the algorithm rapidly converges to the final result. While the calculation of $a \bmod b$ is not hard, it requires division and may be more expensive to do on some very simple computing devices. In the world of binary arithmetic, division by 2 is much easier to compute. Consider the following alternative algorithm for gcd using subtraction and division by 2, developed below through a series of exercises.

- i. Show that if a and b are both even, then $\gcd(a, b) = 2 \cdot \gcd(a/2, b/2)$.
- ii. Show that if a is even and b is odd, then $\gcd(a, b) = \gcd(a/2, b)$. (Similarly, if a is odd and b is even, then $\gcd(a, b) = \gcd(a, b/2)$.)
- iii. Show that if a and b are both odd, then $\gcd(a, b) = \gcd((a - b)/2, b)$.
Hint: Show that $\gcd(a, b) = \gcd(a - b, b)$; for inspiration, see the proof of correctness for the Euclidean Algorithm given in the text. If a and b are both odd, what is true about $a - b$? Now apply your result from part ii above...
- iv. Apply the above three claims repeatedly to compute the following: $\gcd(252, 76)$, $\gcd(612, 378)$. Show your work.

Solution:

- i. Any even number is divisible by 2. If a and b are both even numbers, then 2 is a common divisor for a and b :

$$\gcd(a, b) = \gcd(2 \times \frac{a}{2}, 2 \times \frac{b}{2}) = 2 \cdot \gcd(a/2, b/2).$$
- ii. If a is even and b is odd, then 2 is a divisor of a , but not a divisor of b ; therefore 2 is not a common divisor of a and b :

$$\gcd(a, b) = \gcd(a/2, b).$$
- iii. Let us consider that $a \geq b$.

Since $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, from the definition of divides there exist integers m and n such that:

$$a = m \times \gcd(a, b)$$

$$b = n \times \gcd(a, b)$$

Subtracting the left and right hand sides of the two equations above, we obtain:

$$a - b = m \times \gcd(a, b) - n \times \gcd(a, b) = (m - n) \times \gcd(a, b)$$

So, by definition of divides:

$$\gcd(a, b) \mid (a - b)$$

Since $\gcd(a, b)$ divides both b and $a - b$, then $\gcd(a, b) \mid \gcd((a - b), b)$. Similarly, since $\gcd((a - b), b)$ divides both a and b , then $\gcd((a - b), b) \mid \gcd(a, b)$. Hence $\gcd(a, b) = \gcd((a - b), b)$.

(Observation: This is one step of the Euclidean algorithm, which uses subtraction at each step.)

Since a and b are both odd numbers, their difference is an even number. To show this, we can write a as: $a = 2 \times m + 1$ and b as: $b = 2 \times n + 1$, which is a general form of odd numbers.

$$a - b = 2 \times m + 1 - 2 \times n - 1 = 2 \times (m - n), \text{ which is even.}$$

Since $(a - b)$ is even and b is odd, we can apply **ii.** discussed before:

$$\gcd(a, b) = \gcd((a - b), b) = \gcd((a - b)/2, b)$$

iv.

$$\begin{aligned}\gcd(252, 76) &= 2 \times \gcd(252/2, 76/2) \\ &= 2 \times \gcd(126, 38) \\ &= 2 \times 2 \times \gcd(126/2, 38/2) \\ &= 4 \times \gcd(63, 19) \\ &= 4 \times \gcd((63 - 19)/2, 19) \\ &= 4 \times \gcd(22, 19) \\ &= 4 \times \gcd(22/2, 19) \\ &= 4 \times \gcd(11, 19) \\ &= 4 \times \gcd(11, (19 - 11)/2) \\ &= 4 \times \gcd(11, 4) \\ &= 4 \times \gcd(11, 4/2) \\ &= 4 \times \gcd(11, 2) \\ &= 4 \times \gcd(11, 2/2) \\ &= 4 \times \gcd(11, 1) \\ &= 4 \times \gcd((11 - 1)/2, 1) \\ &= 4 \times \gcd(5, 1) \\ &= 4 \times \gcd((5 - 1)/2, 1) \\ &= 4 \times \gcd(2, 1) \\ &= 4 \times \gcd(2/2, 1) \\ &= 4 \times \gcd(1, 1) \\ &= 4 \times \gcd((1 - 1)/2, 1) \\ &= 4 \times \gcd(0, 1) \\ &= 4 \times 1 \\ &= 4\end{aligned}$$

$$\begin{aligned}\gcd(612, 378) &= 2 \times \gcd(612/2, 378/2) \\ &= 2 \times \gcd(306, 189) \\ &= 2 \times \gcd(306/2, 189) \\ &= 2 \times \gcd(153, 189) \\ &= 2 \times \gcd(153, (189 - 153)/2) \\ &= 2 \times \gcd(153, 18) \\ &= 2 \times \gcd(153, 18/2) \\ &= 2 \times \gcd(153, 9) \\ &= 2 \times \gcd((153 - 9)/2, 9) \\ &= 2 \times \gcd(72, 9)\end{aligned}$$

$$\begin{aligned} &= 2 \times \gcd(72/2, 9) \\ &= 2 \times \gcd(36, 9) \\ &= 2 \times \gcd(36/2, 9) \\ &= 2 \times \gcd(18, 9) \\ &= 2 \times \gcd(18/2, 9) \\ &= 2 \times \gcd(9, 9) \\ &= 2 \times \gcd((9 - 9)/2, 9) \\ &= 2 \times \gcd(0, 9) \\ &= 2 \times 9 \\ &= 18 \end{aligned}$$