Written Homework 02

Assigned: Wed 20 Sep 2017
Due: Fri 06 Oct 2017

Instructions:
- The assignment has to be uploaded to Blackboard by the due date. NO assignment will be accepted after 11:59pm on that day.
- We expect that you will study with friends and often work out problem solutions together, but you must write up your own solutions, in your own words. Cheating will not be tolerated. Professors, TAs, and peer tutors will be available to answer questions but will not do your homework for you. One of our course goals is to teach you how to think on your own.
- You may turn in work to Blackboard that is either handwritten and scanned, written in a word processor such as Word, or typeset in LaTeX. In the case of handwritten work, we may deduct points if the scan is upside down or the work is illegible.
- To get full credit, show INTERMEDIATE steps leading to your answers, throughout.

Problem 1 [18 pts; (6,6,6)]: Prime Factorization and Euclid’s Algorithm

Compute the following. Show all of your work.

i. \( \gcd(6000, 1280) \) using prime factorization.

ii. \( \gcd(1275, 135) \) using Euclid’s algorithm.

iii. \( \text{lcm}(364, 260) \) by first computing the \( \gcd \) using Euclid’s algorithm.

Solution:

i. 
\[
\gcd(6000, 1280) = \gcd(6 \times 10^3, 2^7 \times 10) \\
= \gcd(2^4 \times 3 \times 5^3, 2^8 \times 5) \\
= 2^4 \times 5 \\
= 80
\]

ii. 
\[
\gcd(1275, 135) = \gcd(135, 1275 \mod 135) \\
= \gcd(135, 60) \\
= \gcd(60, 135 \mod 60) \\
= \gcd(60, 15) \\
= \gcd(15, 60 \mod 15) \\
= \gcd(15, 0) \\
= 15
\]
iii.

\[
gcd(364, 260) = gcd(260, 364 \mod 260) \\
= gcd(260, 104) \\
= gcd(104, 260 \mod 104) \\
= gcd(104, 52) \\
= gcd(52, 104 \mod 52) \\
= gcd(52, 0) \\
= 52
\]

\[
364 \times 260 = gcd(364, 260) \times lcm(364, 260) 
\]
\[
\Leftrightarrow \quad lcm(364, 260) = \frac{364 \times 260}{gcd(364, 260)} \\
= \frac{364 \times 260}{52} \\
= 1820
\]

**Problem 2** [24 pts; (6,6,6,6)]: A New Algorithm for Computing GCD

Given two positive integers \(a\) and \(b\), \(a \geq b\). Euclid’s algorithm computes the gcd of \(a\) and \(b\) by reducing the problem to that of computing the gcd of \(b\) and \((a \mod b)\), where \(a \mod b\) is often much smaller than \(a\). Thus the algorithm rapidly converges to a final result. While the calculation of \(a \mod b\) is not hard, it requires division by arbitrary values of \(b\) which can be difficult to perform mentally and which can be computationally expensive for simple computing devices. As we saw in the context of converting to and from binary numbers, multiplying and dividing by 2 is much simpler mentally (and, as it turns out, computationally). Consider the following alternative algorithm for gcd using only subtraction and division by 2, developed below through a series of exercises.

i. Prove that if \(a\) and \(b\) are both even, then \(gcd(a, b) = 2 \cdot gcd(a/2, b/2)\).

ii. Prove 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. Prove that if \(a\) and \(b\) are both odd, then \(gcd(a, b) = gcd((a - b)/2, b)\).

*Hint:* Use the fact that \(gcd(a, b) = gcd(a - b, b)\) and an earlier fact you have proven. If \(a\) and \(b\) are both odd, what is true of \(a - b\)?

iv. Apply the above three claims repeatedly to compute the following:

- \(gcd(294, 210)\)
- \(gcd(464, 88)\)

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 \(a \geq b\). We have that \(gcd(a, b) = gcd(a - b, b)\). Since \(a\) and \(b\) are both odd, \(a - b\) must be even. We now have \(a - b\) even and \(b\) odd, so our result from part ii applies, yielding \(gcd(a, b) = gcd(a - b, b) = gcd((a - b)/2, b)\).

iv.
\[
gcd(294, 210) = 2 \cdot gcd(147, 105) = 2 \cdot gcd(21, 105) = 2 \cdot gcd(42, 21) = 2 \cdot gcd(21, 21) = 2 \cdot gcd(0, 21) = 2 \cdot 21 = 42
\]
\[
gcd(464, 88) = 2 \cdot gcd(232, 44) = 2 \cdot 2 \cdot gcd(116, 22) = 2 \cdot 2 \cdot gcd(58, 11) = 2 \cdot 2 \cdot 2 \cdot gcd(29, 11) = 2 \cdot 2 \cdot 2 \cdot gcd(9, 11) = 2 \cdot 2 \cdot 2 \cdot 1 = 8
\]

Problem 3 [38 pts; (2,4,4,8,8,8,2,2)]: Linear Ciphers

At an archeological dig, you recover a set of documents. Linguists who have studied the documents believe that they have been encrypted. Furthermore, since the site is thousands of years old, the source language is unknown and certainly not English. Your job is to decrypt what appears to be an important passage contained in the documents, determine the source language, and translate the original text into English.

Linguists analyzing the documents have determined that the source language uses the familiar 26 English letters, which are encoded and decoded using the numbers \(\{0, \ldots, 25\}\) in the usual way.
Based on evidence found at the site, you suspect that the documents were encrypted using a linear encryption scheme with $m = 15$ and $k = 9$. The linguists are particularly interested in decrypting and determining the source language and translation of the following passage which appears throughout the documents:

```
clnrwcl cztnzhxt
```

i. Encode each letter in the above phrase in the usual way, i.e., $c \rightarrow 2$, $l \rightarrow 11$, $n \rightarrow 13$, and so on.

ii. Since you suspect that these values were encrypted using the function

\[ num \rightarrow (15 \cdot num + 9) \mod 26 \]

you must subtract 9 (mod 26) and then multiply by the multiplicative inverse of 15 (mod 26) in order to decrypt these values. Start by subtracting 9 (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 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

\[
\varphi(n) = n \cdot \prod_{p\mid n} \left(1 - \frac{1}{p}\right) = n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)
\]

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

\[
\varphi(10) = 10 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 10 \cdot \left(\frac{1}{2}\right) \cdot \left(\frac{4}{5}\right) = 4
\]

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.

4
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 15 \( \pmod{26} \) using the method described above.

v. Now verify that your answer above is correct by computing the multiplicative inverse of 15 \( \pmod{26} \) using the Extended Euclidean Algorithm.

vi. Given the multiplicative inverse of 15, you can now complete the decryption you started in part ii above. Decrypt each encoded character by inverting the linear encryption.

vii. Decode these values in the usual way to obtain a phrase in the unknown source language.

viii. 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 is the source language of the documents?

Solution:

i. Encoded: 2 11 13 17 22 2 11 2 25 19 13 25 7 23 19

ii. Subtract 9 \( \pmod{26} \): 19 2 4 8 13 19 2 19 16 10 4 16 24 14 10

iii. \( \varphi(26) = 26 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{13}\right) = 26 \cdot \frac{1}{2} \cdot \frac{12}{13} = 12 \)

iv. We need to compute \( 15^{11} \pmod{26} \). To do so, we will use fast exponentiation, computing \( 15^1, 15^2, 15^4, 15^8 \), and then \( 15^{11} = 15^8 \cdot 15^2 \cdot 15^1 \), all \( \pmod{26} \).
$15^1 \mod 26 = 15$

$15^2 \mod 26 = 225 \mod 26$
$= 17$

$15^4 \mod 26 = ((15^2 \mod 26) \cdot (15^2 \mod 26)) \mod 26$
$= (17 \cdot 17) \mod 26$
$= 289 \mod 26$
$= 3$

$15^8 \mod 26 = ((15^4 \mod 26) \cdot (15^4 \mod 26)) \mod 26$
$= (3 \cdot 3) \mod 26$
$= 9 \mod 26$
$= 9$

$15^{11} \mod 26 = (15^8 \cdot 15^2 \cdot 15^1) \mod 26$
$= (9 \cdot 17 \cdot 15) \mod 26$
$= ((9 \cdot 17) \cdot 15) \mod 26$
$= (153 \cdot 15) \mod 26$
$= ((153 \mod 26) \cdot (15 \mod 26)) \mod 26$
$= (23 \cdot 15) \mod 26$
$= 345 \mod 26$
$= 7$

v. Applying the Extended Euclidean Algorithm, we have:

\[
\begin{align*}
gcd(26, 15) & : 26 = 1 \times 15 + 11 \iff 11 = 26 - 1 \times 15 \\
gcd(15, 11) & : 15 = 1 \times 11 + 4 \iff 4 = 15 - 1 \times 11 \\
gcd(11, 4) & : 11 = 2 \times 4 + 3 \iff 3 = 11 - 2 \times 4 \\
gcd(4, 3) & : 4 = 1 \times 3 + 1 \iff 1 = 4 - 1 \times 3 \\
gcd(3, 1) & : 3 = 3 \times 1 + 0
\end{align*}
\]

The remainder is zero, so the GCD is 1, as expected. Back-substituting to determine Bezout’s Identities:

\[
\begin{align*}
gcd(4, 3) & : 1 = 1 \times 4 + -1 \times 3 \\
gcd(11, 4) & : 1 = -1 \times 11 + 3 \times 4 \\
gcd(15, 11) & : 1 = 3 \times 15 + -4 \times 11 \\
gcd(26, 15) & : 1 = -4 \times 26 + 7 \times 15
\end{align*}
\]

Thus, 7 is the multiplicative inverse of 15 (mod 26).

vi. Multiply by 7 (mod 26): 3 14 2 4 13 3 14 3 8 18 2 8 12 20 18
vii. Decoded: docendo discimus

viii. The source language is Latin, and the phrase translates to “by teaching, we learn.”

Problem 4 [20 pts]: The RSA cryptosystem.

Decipher the following message to get the initials of an organization:

8 8 17 2

Each letter is encoded using the same 0–25 scheme as the previous problem, then individually encrypted in RSA with public key \( (e = 23, n = 55) \).

For example, the message “HEY” will be encoded and encrypted as follows. The letter H corresponds to 7, and \( 7^{23} \mod 55 \) equals 13. The letter E corresponds to 4, and \( 4^{23} \mod 55 \) equals 9. The letter Y corresponds to 24, and \( 24^{23} \mod 55 \) equals 19. So the message “HEY”, when encoded and encrypted, reads as follows.

13 9 19

Solve for the private key \( d \), then decrypt and decode the “8 8 17 2” message. What initials do you find? Remember to show all your work.

Solution:

The factors of 55 are 5 and 11, so \( \varphi(n) = 4 \times 10 = 40 \). Given the encryption exponent \( e = 23 \), to find the private key \( d \), we need to determine the multiplicative inverse of 23 (mod 40). This can be accomplished via the Extended Euclidean Algorithm or the method described in Problem 3 above. The result is \( d = 7 \).

Now that we have \( d \), decryption is straightforward via (fast) exponentiation:

\[
\begin{align*}
8^7 \mod 55 &= 2 = C \\
8^7 \mod 55 &= 2 = C \\
17^7 \mod 55 &= 8 = I \\
2^7 \mod 55 &= 18 = S
\end{align*}
\]

The message is the initials of our home college, CCIS.