CS201: Discrete Mathematics (Fall 2024)
Written Assignment #3 - Solutions
(100 points maximum but 110 points in total)
Deadline: 11:59pm on Nov 8 (please submit to Blackboard)
PLAGIARISM WILL BE PUNISHED SEVERELY
Hint: Corollary 1 of Bézout's Theorem is heavily used in this assignment.

Q.1 (**5p**) Show that if a, b, and c are integers such that $ac \mid bc$, where $a \neq 0$ and $c \neq 0$, then $a \mid b$.
Solution: By definition, $ac \mid bc$ implies that there exists an integer k such that $bc = ack$. Divide c on both sides and we get $b = ak$. Again, by definition, this shows $a \mid b$.

□

Q.2 (**5p**) Evaluate the following quantities:

(a) (**1p**) -2024 div 33

(b) (**2p**) $(20234 - 2024) \bmod 25$

(c) (**2p**) $94232 \cdot 2982 \bmod 7$

Solution:

(a) $-2024 = 33 \cdot -62 + 22$, so -2024 div $33 = -62$.

(b) $(20234 - 2024) \bmod 25 = (20234 \bmod 25 - 2024 \bmod 25) \bmod 25 = (9 - 24) \bmod 25 = 10$.

(c) $94232 \cdot 2982 \bmod 7 = (94232 \bmod 7)(2982 \bmod 7) \bmod 7 = ((94232 \bmod 7) \cdot 0) \bmod 7 = 0$.

□

Q.3 (**10p**) Integer representations.

(a) (**2p**) Convert $(11011)_2$ to its decimal expansion.

(b) (**2p**) Convert $(101100)_2$ to its octal expansion.

(c) (**3p**) Convert $(AE01F)_{16}$ to its binary expansion.

(d) (**3p**) Convert $(720235)_8$ to its hexadecimal expansion.

Solution:

(a) $(11011)_2 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^3 + 1 \cdot 2^4 = (27)_{10}$

(b) Since $(101)_2 = (5)_8$ and $(100)_2 = (4)_8$, we have $(101100)_2 = (101|100)_2 = (5|4)_8 = (54)_8$.

(c) Since $(A)_{16} = (1010)_2$, $(E)_{16} = (1110)_2$, $(0)_{16} = (0000)_2$, $(1)_{16} = (0001)_2$, $(F)_{16} = (1111)_2$, we have $(AE01F)_{16} = (1010|1110|0000|0001|1111)_2 = (10101110000000011111)_2$.

(d) Similarly, we have $(720235)_8 = (111|010|000|010|011|101)_2 = (0011|1010|0000|1001|1101)_2 = (3|A|0|9|D)_{16} = (3A09D)_{16}$.

□

Q.4 (**5p**) Find the prime factorization of the following integers:

(a) (**2p**) 8085

(b) (**3p**) 12!

Solution:

(a) $8085 = 3 \cdot 5 \cdot 7^2 \cdot 11$

(b) $12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$

□

Q.5 (**20p**) The (extended) Euclidean algorithm.

(a) (**4p**) Use the Euclidean algorithm to find $\gcd(267, 79)$.

(b) (**4p**) Find Bézout coefficients of 267 and 79.

(c) (**2p**) Solve the linear congruence $267x \equiv 3 \pmod{79}$.

(d) (**6p**) Use the extended Euclidean algorithm (see page 286∼287 of the textbook) to express $\gcd(252, 356)$ as a linear combination of 252 and 356.

(e) (**4p**) Prove that the number of divisions required by the Euclidean algorithm to find $\gcd(a, b)$, where $a \geq b > 0$, is $O(\log b)$. (Hint: prove that the remainders r_i satisfy $r_{i+2} < r_i/2$.)

Solution:

(a) By the Euclidean algorithm, we have

$$\begin{aligned} 267 &= 3 \cdot 79 + 30 \\ 79 &= 2 \cdot 30 + 19 \\ 30 &= 1 \cdot 19 + 11 \\ 19 &= 1 \cdot 11 + 8 \\ 11 &= 1 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1. \end{aligned}$$

Thus, $\gcd(267, 79) = 1$.

(b) By (a), we have

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (8 - 2 \cdot 3) \\
&= 3 \cdot 3 - 8 \\
&= 3 \cdot (11 - 8) - 8 \\
&= 3 \cdot 11 - 4 \cdot 8 \\
&= 3 \cdot 11 - 4 \cdot (19 - 11) \\
&= 7 \cdot 11 - 4 \cdot 19 \\
&= 7 \cdot (30 - 19) - 4 \cdot 19 \\
&= 7 \cdot 30 - 11 \cdot 19 \\
&= 7 \cdot 30 - 11 \cdot (79 - 2 \cdot 30) \\
&= 29 \cdot 30 - 11 \cdot 79 \\
&= 29 \cdot (267 - 3 \cdot 79) - 11 \cdot 79 \\
&= 29 \cdot 267 - 98 \cdot 79.
\end{aligned}$$

Thus, the Bézout coefficients of 267 and 79 are 29 and -98.

(c) From (b), we know 29 is an inverse of 267 modulo 79. Multiplying both sides of the linear congruence by 29, we have $x \equiv 29 \cdot 3 \equiv 87 \equiv 8 \pmod{79}$.

(d) By the Euclidean algorithm, we have

$$\begin{aligned}
356 &= 1 \cdot 252 + 104 \\
252 &= 2 \cdot 104 + 44 \\
104 &= 2 \cdot 44 + 16 \\
44 &= 2 \cdot 16 + 12 \\
16 &= 1 \cdot 12 + 4 \\
12 &= 3 \cdot 4.
\end{aligned}$$

Therefore, $q_1 = 1, q_2 = 2, q_3 = 2, q_4 = 2, q_5 = 1, q_6 = 3$.

By the extended Euclidean algorithm, set $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$ and do the following:

$$\begin{aligned}
&s_2 = s_0 - q_1 s_1 = 1 - 1 \cdot 0 = 1, && t_2 = t_0 - q_1 t_1 = 0 - 1 \cdot 1 = -1 \\
&s_3 = s_1 - q_2 s_2 = 0 - 2 \cdot 1 = -2, && t_3 = t_1 - q_2 t_2 = 1 - 2 \cdot (-1) = 3 \\
&s_4 = s_2 - q_3 s_3 = 1 - 2 \cdot (-2) = 5, && t_4 = t_2 - q_3 t_3 = -1 - 2 \cdot 3 = -7 \\
&s_5 = s_3 - q_4 s_4 = -2 - 2 \cdot 5 = -12, && t_5 = t_3 - q_4 t_4 = 3 - 2 \cdot (-7) = 17 \\
&s_6 = s_4 - q_5 s_5 = 5 - 1 \cdot (-12) = 17, && t_6 = t_4 - q_5 t_5 = -7 - 1 \cdot 17 = -24.
\end{aligned}$$

Therefore, $\gcd(252, 356) = 17 \cdot 356 - 24 \cdot 252$.

(Note that the above two sets of equations can be calculated along with the Euclidean algorithm, i.e., the extended Euclidean algorithm requires only *one pass* through the steps of the Euclidean algorithm.)

(e) Recall that in the Euclidean algorithm, we have $r_0 = a$, $r_1 = b$ and $r_i = r_{i+1}q_{i+1} + r_{i+2}$ for $i \geq 0$. We prove that $r_{i+2} < r_i/2$ by considering two cases: $r_{i+1} \leq r_i/2$ and $r_{i+1} > r_i/2$.

First, note that $0 < r_{i+1} < r_i$ holds for all $i \geq 0$ such that $r_{i+1} > 0$. If $r_{i+1} \leq r_i/2$, it is easy to see that $r_{i+2} < r_{i+1} \leq r_i/2$ holds. If $r_{i+1} > r_i/2$, we have $r_{i+2} = r_i - r_{i+1}q_{i+1} \leq r_i - r_{i+1} < r_i - r_i/2 = r_i/2$.

The above shows that it takes at most $2\lceil \log_2(b+1) \rceil$ divisions to complete the Euclidean algorithm, i.e., to reach some $r_n = 0$. That is, the number of divisions is $O(\log b)$.

□

Q.6 (**5p**) Prove that if $c \mid ab$ then $c \mid a \cdot \gcd(b, c)$.

Solution: Since $c \mid ab$, we know that $kc = ab$ for some integer k. By Bézout's theorem, we also know that $\gcd(b, c) = sb + tc$ for some integers s and t. Thus, we have

$$\begin{aligned} a \cdot \gcd(b, c) &= a \cdot (sb + tc) \\ &= asb + atc \\ &= skc + atc \\ &= (sk + at) \cdot c. \end{aligned}$$

Therefore, we have $c \mid a \cdot \gcd(b, c)$. □

Q.7 (**10p**) In class, we already proved that "if $\gcd(a, m) = 1$ for positive integers a and m, then there exists an inverse of a modulo m". Now, show that the following statements are also true.

(a) (**5p**) Prove that the above inverse of a is *unique* modulo m. That is, suppose $\bar{a} \in \mathbf{Z}_m$ is an inverse of a modulo m, then every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.

(b) (**5p**) Prove that "if $\gcd(a, m) > 1$ for positive integers a and m, then a does *not* have an inverse modulo m".

Note that the above tells us that "for positive integers a and m, there exists an inverse of a modulo m if and only if $\gcd(a, m) = 1$".

Solution:

(a) Suppose that b and c are two inverses of a modulo m. By definition, we have $ab \equiv 1 \pmod{m}$ and $ac \equiv 1 \pmod{m}$. The difference of these two congruences yields $a(b - c) \equiv 0 \pmod{m}$, i.e., $m \mid a(b - c)$. Since $\gcd(m, a) = 1$, we have $m \mid (b - c)$ and hence $b \equiv c \pmod{m}$. The proof is concluded.

(b) We prove this by contrapositive. Assume that a has an inverse modulo m, denoted by $\bar{a}$, i.e., $a\bar{a} \equiv 1 \pmod{m}$. Therefore, we have $a\bar{a} = 1 + km$ for some integer k. Suppose that d is any common divisor of a and m, i.e., $d \mid a$ and $d \mid m$. Since $\bar{a}$ and k are integers, it follows that $d \mid (a\bar{a} - km)$, so $d \mid 1$. Thus, we must have $d = 1$, which completes the proof.

□

Q.8 (**10p**) In class, we proved that one can use the Chinese remainder theorem to construct a solution of the system of linear congruences $\{x \equiv a_i \pmod{m_i}\}_{1 \leq i \leq n}$ where the moduli $m_1, m_2, \ldots, m_n$ are pairwise coprime integers greater than or equal to 2. Now, let us prove that the solution is *unique* modulo $m = m_1 m_2 \cdots m_n$.

(a) (**7p**) Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers greater than or equal to 2. Show that if $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, n$, then $a \equiv b \pmod{m}$, where $m = m_1 m_2 \cdots m_n$.

(b) (**3p**) Use (a) to complete the proof of uniqueness in the Chinese remainder theorem.

Solution:

(a) First, we show that for any $1 < k \leq n$ we have $\gcd(m_k, m_1 \cdots m_{k-1}) = 1$. By Bézout's theorem, for each $1 \leq i < k$ there are integers s_i, t_i such that $s_i \cdot m_k + t_i \cdot m_i = 1$. Multiplying these $k-1$ equations together yields an equation of the form $s \cdot m_k + t_1 \cdots t_{k-1} m_1 \cdots m_{k-1} = 1$, where s is an integer. This implies that $\gcd(m_k, m_1 \cdots m_{k-1}) = 1$ holds. Then, we show that $a \equiv b \pmod{m}$ holds. By definition, $a \equiv b \pmod{m_1}$ implies that $m_1 \mid (a - b)$, i.e., $a - b = m_1 k_1$ for some integer k_1, and $a \equiv b \pmod{m_2}$ implies that $m_2 \mid (a - b)$, so we have $m_2 \mid m_1 k_1$. Since $\gcd(m_2, m_1) = 1$, we have $m_2 \mid k_1$, i.e., $k_1 = m_2 k_2$ for some integer k_2 and hence $a - b = m_1 m_2 k_2$. Continuing with the above argument and noting that $\gcd(m_k, m_1 \cdots m_{k-1}) = 1$ holds, we can prove that $m_3 \mid k_2$, $m_4 \mid k_3$ where $a - b = m_1 m_2 m_3 k_3$, $m_5 \mid k_4$ where $a - b = m_1 m_2 m_3 m_4 k_4$, etc., and finally we have $a - b = m_1 m_2 \ldots m_n k_n$ for some integer k_n. Therefore, $m_1 m_2 \cdots m_n$ divides $a - b$ and hence $a \equiv b \pmod{m_1 m_2 \cdots m_n}$.

(b) Suppose that there are two solutions x and y to the system of linear congruences. Then, by definition, $x \equiv a_i \pmod{m_i}$ and $y \equiv a_i \pmod{m_i}$ hold for all i. This further implies that $x \equiv y \pmod{m_i}$ for all i. From (a), we have $x \equiv y \pmod{m}$, which concludes our proof.

□

Q.9 (**10p**) We learned from class that a system of linear congruences can be solved by the Chinese remainder theorem. However, this requires all pairs of moduli be relatively prime. Now, let us solve this system of linear congruences: $x \equiv 5 \pmod{6}$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{35}$.

(a) (**5p**) Transform the above system of linear congruences into a new equivalent system that can be solved by the Chinese remainder theorem, i.e., the moduli for the new system are pairwise coprime. Explain your answer. (Hint: Do prime factorization of the moduli.)

(b) (**5p**) Find all solutions to the new system derived in (a).

Solution:

(a) Let us start from the first linear congruence $x \equiv 5 \pmod{6}$. From this congruence we must have $x \equiv 5 \equiv 1 \pmod{2}$ and $x \equiv 5 \equiv 2 \pmod{3}$. Then, by Chinese remainder theorem, the latter two linear congruences also imply $x \equiv 5 \pmod{6}$. That is, $x \equiv 5 \pmod{6}$ is equivalent to $\{x \equiv 1 \pmod{2}, x \equiv 2 \pmod{3}\}$. Similarly, the second congruence is equivalent to $\{x \equiv 1 \pmod{2}, x \equiv 3 \pmod{5}\}$, and the third congruence is equivalent to $\{x \equiv 3 \pmod{5}, x \equiv 1 \pmod{7}\}$. Since these six statements are consistent, the original system is equivalent to the system $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 1 \pmod{7}$.

(b) We solve the new system derived in (a) using the Chinese remainder theorem. First, the modulus $m = 2 \cdot 3 \cdot 5 \cdot 7 = 210$. Then, compute $M_1 = 105, M_2 = 70, M_3 = 42, M_4 = 30$. Note that $105 \equiv 1 \pmod{2}$, $70 \equiv 1 \pmod{3}$, $42 \cdot 3 \equiv 1 \pmod{5}$, $30 \cdot 4 \equiv 1 \pmod{7}$, so $y_1 = 1$, $y_2 = 1$, $y_3 = 3$, $y_4 = 4$. Finally, we can solve the system as $x = 1 \cdot 105 \cdot 1 + 2 \cdot 70 \cdot 1 + 3 \cdot 42 \cdot 3 + 1 \cdot 30 \cdot 4 = 743 \equiv 113 \pmod{210}$. From Q.8, we know that all solutions are of the form $113 + 210k$, where k is an integer.

□

Q.10 (**15p**) Let us prove Fermat's little theorem. Suppose p is prime and a is not divisible by p.

(a) (**5p**) Prove that *no* two of the integers $1 \cdot a$, $2 \cdot a, \ldots, (p-1)a$ are congruent modulo p.

(b) (**5p**) Based on (a), prove that $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$.

(c) (**3p**) Based on (b) and $p \nmid (p-1)!$, prove that $a^{p-1} \equiv 1 \pmod{p}$.

(d) (**2p**) Based on (c), prove that $a^p \equiv a \pmod{p}$ holds for any integer a. (Note that a could be divisible by p.)

Solution:

(a) We prove this by contradiction. Suppose there are two of the integers $i \cdot a$ and $j \cdot a$ that are congruent modulo p, where $1 \leq i < j \leq q-1$. Then, we have $i \cdot a \equiv j \cdot a \pmod{p}$ and by definition this means $p \mid (j-i)a$. Since p is a prime and $1 \leq j - i < p$, we have $\gcd(p, j-i) = 1$ and hence $p \mid a$. This contradicts the premise that a is not divisible by p, which concludes the proof.

(b) Similar to the proof of (a), we can conclude that $p \nmid k \cdot a$ for $k = 1, 2, \ldots, p-1$. Then, the key observation is that $\{1 \cdot a \bmod p, 2 \cdot a \bmod p, \ldots, (p-1)a \bmod p\} = \{1, 2, ..., p-1\}$, because none of the $p-1$ integers in the left set is divisible by p and from (a) we know these $p-1$ integers are distinct from each other when modulo p. Therefore, multiplying all integers in each set results in the congruence: $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$.

(c) Since p is prime and $p \nmid (p-1)!$, it follows that $\gcd(p, (p-1)!) = 1$. Then, by definition, (b) shows that $p \mid (a^{p-1} - 1)(p-1)!$. Therefore, we have $p \mid (a^{p-1} - 1)$, i.e., $a^{p-1} \equiv 1 \pmod{p}$.

(d) If a is not divisible by p, the congruence $a^p \equiv a \pmod{p}$ can be easily derived by multiplying a on both sides of $a^{p-1} \equiv 1 \pmod{p}$ proved in (c). If a is divisible by p, we have $a \equiv 0 \pmod{p}$ and hence $a^p \equiv 0 \pmod{p}$, so $a^p \equiv a \pmod{p}$ also holds.

□

Q.11 (**5p**) Compute the following quantities:

(a) (**2p**) Use Fermat's little theorem to compute $5^{2023} \bmod 7$.

(b) (**3p**) Use Euler's theorem to compute $8^{2023} \bmod 15$.

Solution:

(a) By Fermat's little theorem, we know that $5^6 \equiv 1 \pmod{7}$. Therefore, $5^{2023} = 5^{6 \cdot 337} \cdot 5 = (5^6)^{337} \cdot 5 \equiv 1^{337} \cdot 5 \equiv 5 \pmod{7}$ and we have $5^{2023} \bmod 7 = 5$.

(b) Note that $15 = 3 \cdot 5$, so $\phi(15) = 2 \cdot 4 = 8$. By Euler's theorem, we have $8^8 \equiv 1 \pmod{15}$. Therefore, $8^{2023} = 8^{8 \cdot 252 + 7} = (8^8)^{252} \cdot 8^7 \equiv 1^{252} \cdot 8^7 \equiv 8^7 \equiv (8^2)^3 \cdot 8 \equiv (64)^3 \cdot 8 \equiv 4^3 \cdot 8 \equiv 4^2 \cdot 4 \cdot 8 \equiv 1 \cdot 4 \cdot 8 \equiv 32 \equiv 2 \pmod{15}$ and hence $8^{2023} \bmod 15 = 2$.

□

Q.12 (**10p**) Consider the RSA encryption scheme. Let our public key be $(n, e) = (65, 7)$, and our private key be d. Answer the following questions and show your computation steps.

(a) (**3p**) What is the ciphertext C (i.e., the encryption) of the message $M = 8$?

(b) (**4p**) Find the decryption key d.

(c) (**3p**) Using d, run the RSA decryption of the above ciphertext C.

Solution:

(a) To encrypt $M = 8$, we have

$$\begin{aligned} C &= M^e \bmod n \\ &= 8^7 \bmod 65 \\ &= 8^{2\cdot 3+1} \bmod 65 \\ &= 64^3 \cdot 8 \bmod 65 \\ &= (-1)^3 \cdot 8 \bmod 65 \\ &= -8 \bmod 65 \\ &= 57 \bmod 65. \end{aligned}$$

So the ciphertext of M is $C = 57$.

(b) Recall that $de \equiv 1 \pmod{\phi(n)}$. First, note that $65 = 5 \cdot 13$, so $\phi(65) = 4 \cdot 12 = 48$. Then, we can find the decryption key $d = 7$ by observing that $ed = 7 \cdot 7 = 49 \equiv 1 \pmod{48}$.

Alternatively, one can find d by running the Euclidean algorithm as follows.

$$\begin{aligned} \gcd(\phi(n), e) &= \gcd(48, 7) \\ &= \gcd(7, 6) && \text{as } 48 = 6 \cdot 7 + 6 \\ &= \gcd(6, 1) && \text{as } 7 = 1 \cdot 6 + 1 \\ &= 1. \end{aligned}$$

Then, by working backwards through the above divisions, we have $1 = 7 \cdot 7 - 1 \cdot 48$. Therefore, the private key $d = 7$.

(c) To run the RSA decryption, we have

$$\begin{aligned} C^d \bmod n &= 57^7 \bmod 65 \\ &= (-8)^7 \bmod 65 \\ &= (-8)^{2\cdot 3+1} \bmod 65 \\ &= (64)^3 \cdot (-8) \bmod 65 \\ &= (-1)^3 \cdot (-8) \bmod 65 \\ &= 8 \bmod 65. \end{aligned}$$

Now we derive the original message $M = 8$ as desired.

□