CS201: Discrete Math for Computer Science
2022 Spring Semester Written Assignment # 3
Due: Apr. 6th, 2022, please submit one pdf file through Sakai
Please answer questions in English. Using any other language will lead to a zero point.

Q. 1. (5 points) Show that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Solution: If $a \mid b$, then there exists an integer k such that $a = kb$. If $b \mid a$, then there exists an integer l such that $b = al$. Thus, $b = klb$. Since k and l are integers and $b = b$, we have $kl = 1$. This implies that either $(k = 1, l = 1)$ or $(k = -1, l = -1)$. Consequently, either $a = b$ or $a = -b$.

Q. 2. (5 points)

(a) Convert $(1768)_{10}$ to hexadecimal

(b) Convert $(10101)_2$ to octal

(c) Convert $(3B5A)_{16}$ to binary number

Solution:

(a) $1768 = 6 \cdot 16^2 + 14 \cdot 16 + 8 \cdot 16^0$, Thus, $(1768)_{10} = (6E8)_{16}$

(b) Since $(010)_2 = (2)_8$ and $(101)_2 = (5)_8$, we have $(10101)_2 = (25)_8$.

[Alternative solution] We first convert binary to decimal, i.e., $1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 = 21$. Then, we can convert decimal to octal, i.e., $21 = 5 \cdot 8^0 + 2 \cdot 8$. Thus, $(21)_{10} = (25)_8$.

(c) Since $(3)_{16} = (11)_2$, $(B)_{16} = (1011)_2$, $(5)_{16} = (0101)_2$, and $(A)_{16} = (1010)_2$. Thus, $(3B5A)_{16} = (11101101011010)_2$.

[Alternative solution] Convert hexadecimal to decimal first. Then, convert decimal to binary number. ...

Q. 3. (5 points) What are the prime factorizations of

(a) 256

(b) 1890

(c) 5!

Solution:

(a) $256 = 2^8$.

(b) $1890 = 2 \cdot 3^3 \cdot 5 \cdot 7$.

(c) $5! = 2^3 \cdot 3 \cdot 5$.

□

Q. 4. (5 points)

(a) Use Euclidean algorithm to find $\gcd(267, 79)$.

(b) Find integers s and t such that $\gcd(267, 79) = 79s + 267t$.

(a) By Euclidean algorithm, we have

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

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, $s = -98$ and $t = 29$.

□

Q. 5. (5 points) For three integers a, b, y, suppose that $\gcd(a, y) = d_1$ and $\gcd(b, y) = d_2$. Prove that

$$\gcd(\gcd(a, b), y) = \gcd(d_1, d_2).$$

Solution: To begin, we show $\gcd(\gcd(a, b), y) \leq \gcd(d_1, d_2)$. Suppose that $d \mid \gcd(a, b)$ and $d \mid y$. As $d \mid \gcd(a, b)$, we know $d \mid a$ and $d \mid b$. Thus, $d \mid a$ and $d \mid y$ so $d \mid \gcd(a, y) = d_1$. Similarly, $d \mid b$ and $d \mid y$, so $d \mid \gcd(b, y) = d_2$. Because $d \mid d_1$ and $d \mid d_2$ we know $d \mid \gcd(d_1, d_2)$. Hence we have $\gcd(\gcd(a, b), y) = d \leq \gcd(d_1, d_2)$.

Next we show $\gcd(d_1, d_2) \leq \gcd(\gcd(a, b), y)$. Suppose that $d \mid d_1$ and $d \mid d_2$. As $d \mid \gcd(a, y) = d_1$ we know $d \mid a$ and $d \mid y$. Similarly, as $d \mid \gcd(b, y) = d_2$, we know $d \mid b$ and $d \mid y$. Thus, $d \mid a$, $d \mid b$, and $d \mid y$. Because $d \mid a$ and $d \mid b$, we show $d \mid \gcd(a, b)$. Then $d \mid \gcd(a, b)$ and $d \mid y$. We know $d \mid \gcd(\gcd(a, b), y)$. Hence, $\gcd(d_1, d_2) = d \leq \gcd(\gcd(a, b), y)$.

The theorem follows.

[Alternate solution.] We can also prove this via unique prime factorizations. Let $p_1, p_2, \ldots, p_k$ be the first k primes for some large k, then for a, b and y, we can define sequences of integers (possibly zero) $a_1, \ldots, a_k$, $b_1, \ldots, b_k$ and $y_1, \ldots, y_k$ such that

$$a = \prod_{i=1}^{k} p_i^{a_i} = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad b = \prod_{i=1}^{k} p_i^{b_i} \quad \text{and } y = \prod_{i=1}^{k} p_i^{y_i}.$$

Now we have

$$\gcd(a, b) = \prod_{i=1}^{k} p_i^{\min\{a_i, b_i\}} \quad \text{and } \gcd(a, b) = \prod_{i=1}^{k} p_i^{\min\{\min\{a_i, b_i\}, y\}}.$$

Similarly,

$$d_1 = \gcd(a, y) = \prod_{i=1}^{k} p_i^{\min\{a_i, y_i\}} \quad \text{and } d_2 = \gcd(b, y) = \prod_{i=1}^{k} p_i^{\min\{b_i, y_i\}}$$

so

$$\gcd(d_1, d_2) = \prod_{i=1}^{k} p_i^{\min\{\min\{a_i, y_i\}, \min\{b_i, y_i\}\}}.$$

But, since $\min\{\min\{a_i, b_i\}, y_i\} = \min\{\min\{a_i, y_i\}, \min\{b_i, y_i\}\}$, these values are equal.

□

Q. 6. (5 points) Suppose that $\gcd(b, a) = 1$. Prove that $\gcd(b+a, b-a) \leq 2$.

Solution: W.l.o.g., assume that $b \geq a$. Now suppose that $d \mid (b + a)$ and $d \mid (b - a)$. Then, $d \mid [(b + a) + (b - a)] = 2b$ and $d \mid [(b + a) - (b - a)] = 2a$. Thus, we have

$$d \mid \gcd(2b, 2a) = 2 \gcd(b, a) = 2.$$

Therefore, we have $d \leq 2$.

□

Q. 7. (10 points) Fermat's little theorem: If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

(a) Show that Fermat's little theorem does not hold if p is not prime.

(b) Computer $302^{302} \pmod{11}$, $4762^{5367} \pmod{13}$, $2^{39674} \pmod{523}$.

Solution:

(a) Take $p = 4$ and $a = 6$. Note that 6 is not divisible by 4 and that

$$\begin{aligned} 6^{4-1} \bmod 4 &\equiv (3 \cdot 2)^3 \pmod{4} \\ &\equiv 2^3 \cdot 3^3 \pmod{4} \\ &\equiv 8 \cdot 3^3 \pmod{4} \\ &\equiv 0. \end{aligned}$$

(b) By Fermat's little theorem, we have

$$\begin{aligned} 302^{302} \pmod{11} &\equiv (27 \cdot 11 + 5)^{302} \pmod{11} \\ &\equiv 5^{302} \pmod{11} \\ &\equiv 5^{30 \cdot 10 + 2} \pmod{11} \\ &\equiv 5^2 \cdot (5^{10})^{30} \pmod{11} \\ &\equiv 5^2 \pmod{11} \\ &\equiv 3. \end{aligned}$$

Note that 13 is a prime. Then by Fermat's little theorem, we have

$$\begin{aligned} 4762^{5367} \pmod{13} &\equiv (366 \cdot 13 + 4)^{5367} \pmod{13} \\ &\equiv 4^{5367} \pmod{13} \\ &\equiv 4^{447 \cdot 12 + 3} \pmod{13} \\ &\equiv 4^3 \pmod{13} \\ &\equiv 64 \pmod{13} \\ &\equiv 12. \end{aligned}$$

Note that 523 is a prime. Then by Fermat's little theorem, we have

$$\begin{aligned} 2^{39674} \pmod{523} &\equiv 2^{76 \cdot 522 + 2} \pmod{523} \\ &\equiv 2^2 \pmod{523} \\ &\equiv 4. \end{aligned}$$

□

Q. 8. (5 points) Solve the following modular equations.

(a) $267x \equiv 3 \pmod{79}$.

(b) $312x \equiv 3 \pmod{97}$.

Solution:

(a) First, we compute the inverse of 267 modulo 79, denoted by $\bar{a}$. By Euclidean algorithm, we have

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

(For this part, it is ok for the students to directly refer to Q. 4.)

Since $\gcd(267, 79) = 1$, the inverse of 267 modulo 79 exists. Reading backwards, we have $29 \cdot 267 \equiv 1 \pmod{79}$, i.e., $\bar{a} = 29$. Thus, we have $x \equiv 29 \cdot 3 \equiv 87 \equiv 8 \pmod{79}$.

(b) We first compute the invest of 312 modulo 97, denoted by $\bar{a}$. Applying Euclidean algorithm, we have

$$\begin{aligned} 312 &= 3 \cdot 97 + 21 \\ 97 &= 4 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Since $\gcd(312, 97) = 1$, the inverse of 312 modulo 97 exists. Reading Euclidean algorithm backwards, we have $1 = 37 \cdot 312 - 119 \cdot 97$. So,

$312 \cdot 37 \equiv 1 \pmod{97}$, i.e., $\bar{a} = 37$. Thus, $x \equiv 37 \cdot 3 \equiv 111 \equiv 14 \pmod{97}$.

□

Q. 9. (5 points) Prove that if a and m are positive integer such that $\gcd(a, m) = 1$, then the function

$$f : \{0, \ldots, m-1\} \to \{0, \ldots, m-1\}$$

defined by

$$f(x) = (a \cdot x) \bmod m$$

is a bijection.

Solution: Since $\gcd(a, m) = 1$, we know that a has an inverse modulo m. Let b be such an inverse, i.e.,

$$ab \equiv 1 \pmod{m}.$$

To show that f is a bijection, we need to show that it is one-to-one and onto. Let $S = \{0, \ldots, m-1\}$ denote the domain and codomain. We first show that f is one-to-one. Assume that $x, y \in S$ and $f(x) = f(y)$, i.e.,

$$ax \bmod m = ay \bmod m.$$

This is equivalent to saying that

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

Multiplying both sides by b, we have

$$bax \equiv bay \pmod{m},$$

which is just

$$x \equiv y \pmod{m}.$$

Thus, $m|x - y$. Note that since $0 \leq x, y < m$, we have $|x - y| < m$. Thus, this is only possible if $x = y = 0$ or $x = y$ as desired.

To show that f is onto, let $z \in S$ be some element in the codomain. Let

$$x = bz \bmod m,$$

and note that $x \in S$ and

$$ax \equiv abz \equiv z \pmod{m}.$$

Since $z \in \{0, \ldots, m-1\}$, this means that $ax \bmod m = z$. Thus, $f(x) = z$, as desired.

□

Q. 10. (5 points) Show that if n is an integer, then $n^2 \equiv 0$ or $1 \pmod 4$.

Solution: There are two cases. If n is even, then $n = 2k$ for some integer k, so $n^2 = 4k^2$, which means that $n^2 \equiv 0 \pmod 4$. If n is odd, then $n = 2k+1$ for some integer k, so $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, which means that $n^2 \equiv 1 \pmod 4$.

□

Q. 11. (5 points) Use Q. 10 to show that if m is a positive integer of the form $4k + 3$ for some nonnegative integer k, then m is not the sum of the squares of two integers.

Solution: Assume that m is the sum of two integers, i.e., $m = s^2 + t^2$. By Q.10, $s^2 + t^2 \equiv 0 \pmod 4$, $s^2 + t^2 \equiv 1 \pmod 4$, or $s^2 + t^2 \equiv 2 \pmod 4$. However, $4k + 3 \equiv 3 \pmod 4$. This leads to contradiction.

□

Q. 12. (5 points) Prove that if a and m are positive integers such that $\gcd(a, m) \neq 1$, then a does *not* have an inverse modulo m.

Solution: We prove this by contrapositive. Assume that a has an inverse modulo m, i.e., there exists an integer b such that

$$ab \equiv 1 \pmod m.$$

This is equivalent to $m \mid (ab - 1)$, which means that there is an integer k such that

$$ab - 1 = mk,$$

which is

$$ba + (-k)m = 1.$$

Suppose that d is any common divisor of a and m, i.e., $d \mid a$ and $d \mid m$. Since b and k are integers, it follows that $d \mid (ba - km)$, so $d \mid 1$. Thus, we must have $d = 1$, which completes the proof.

□

Q. 13. (5 points)

(a) Convert $(1768)_{10}$ to hexadecimal

(b) Convert $(10101)_2$ to octal

(c) Convert $(3B5A)_{16}$ to binary number

Solution: ...

□

Q. 14. (5 points) Show that if a, b, and m are integers such that $m \geq 2$ and $a \equiv b \bmod m$, then $\gcd(a, m) = \gcd(b, m)$.

Solution: From $a \equiv b \bmod m$, we know that $b = a + sm$ for some integer s. Now if d is a common divisor of a and m, then it divides the right-hand side of this equation, so it also divides b. We can rewrite the equation as $a = b - sm$, and then by similar reasoning, we see that every common divisor of b and m is also a divisor of a. This shows that the set of common divisors of a and m is equal to the set of common divisors of b and m, so certainly $\gcd(a, m) = \gcd(b, m)$.

□

Q. 15. (5 points) Solve the system of congruence $x \equiv 3 \pmod 6$ and $x \equiv 4 \pmod 7$ using the method of back substitution.

Solution: By definition, the first congruence can be written as $x = 6t + 3$ where t is an integer. Substituting this expression for x into the second congruence tells us that $6t + 3 \equiv 4 \pmod 7$, which can be easily be solved to show that $t \equiv 6 \pmod 7$. From this we can write $t = 7u + 6$ for some integer u. Thus, $x = 6t + 3 = 6 \cdot (7u + 6) + 3 = 42u + 39$. Thus, our answer is all numbers congruent to 39 modulo 42.

□

Q. 16. (10 points) Find all solutions, if any, to the system of congruences $x \equiv 5 \pmod 6$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{15}$.

Solution: We cannot apply the Chinese remainder theorem directly, since the moduli are not pairwise relatively prime. However, we can using the Chinese remainder theorem, translate these congruences into a set of congruences that together are equivalent to the given congruence. Since we want $x \equiv 5 \pmod 6$, we must have $x \equiv 5 \equiv 1 \pmod 2$ and $x \equiv 5 \equiv 2 \pmod 3$. Similarly, fromt he second congruence we must have $x \equiv 1 \pmod 2$ and $x \equiv 3 \pmod 5$; and from the third congruence we must have $x \equiv 2 \pmod 3$ and $x \equiv 3 \pmod 5$. Since these six statements are consistent, we see that our system is equivalent to the system $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$. These can be solved using the Chinese remainder theorem to yield $x \equiv 23 \pmod{30}$. Therefore, the solutions are all integers of the form $23 + 30k$, where k is an integer.

□

Q. 17. (10 points) Suppose that (n, e) is an RSA encryption key, with $n = pq$ where p and q are large primes and $\gcd(e, (p-1)(q-1)) = 1$. Furthermore, suppose that d is an inverse of e modulo $(p-1)(q-1)$. Suppose that $C \equiv M^e \pmod{pq}$. In the lecture, we showed that RSA decryption, that is, the congruence $C^d \equiv M \pmod{pq}$ holds when $\gcd(M, pq) = 1$. Show that this decryption congruence also holds when $\gcd(M, pq) > 1$. [Hint: Use congruences modulo p and modulo q and apply the Chinese remainder theorem.]

Solution:

If $M \equiv 0 \pmod n$, then $C \equiv M^e \equiv 0 \pmod n$ and so $C^d \equiv 0 \equiv M \pmod n$. Otherwise, $\gcd(M, p) = p$ and $\gcd(M, q) = 1$, or $\gcd(M, p) = 1$ and $\gcd(M, q) = q$. By symmetry it suffices to consider the first case, where $M \equiv 0 \pmod p$. We have $C^d \equiv (M^e)^d \equiv (0^e)^d \equiv 0 \equiv M \pmod p$. As in the case considered in the text, $de = 1 + k(p-1)(q-1)$ for some integer k, so

$$C^d \equiv M^{de} \equiv M^{1+k(p-1)(q-1)} \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M \pmod q$$

by Fermat's little theorem. Thus by the Chinese remainder theorem, $C^d \equiv M \pmod{pq}$.

□