CS201: Discrete Math for Computer Science
Written Assignment on Set and Functions
Spring 2023

Due: Apr. 13th, 2023; Please submit through Sakai in ONE PDF file.
The assignment needs to be written in English. Assignments in any other language will get zero point.
Any plagiarism behavior will lead to zero point.
Does not accept late submissions. No exception!

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. (6 points)

(a) Use Euclidean algorithm to find $\gcd(561, 234)$.

(b) Use extended Euclidean algorithm to express $\gcd(561, 234)$ as a linear combination of 561 and 234.

Solution:

(a) By Euclidean algorithm, we have

$$\begin{aligned} 561 &= 2 \cdot 234 + 93 \\ 234 &= 2 \cdot 93 + 48 \\ 93 &= 1 \cdot 48 + 45 \\ 48 &= 1 \cdot 45 + 3. \end{aligned}$$

Thus, $\gcd(561, 234) = 3$.

(b) By (c), we have

$$\begin{aligned} 3 &= 1 \cdot 48 - 1 \cdot 45 \\ &= 1 \cdot 48 - 1 \cdot (93 - 48) \\ &= 2 \cdot 48 - 1 \cdot 93 \\ &= 2 \cdot (234 - 2 \cdot 93) - 1 \cdot 93 \\ &= 2 \cdot 234 - 5 \cdot 93 \\ &= 2 \cdot 234 - 5 \cdot (561 - 2 \cdot 234) \\ &= 12 \cdot 234 - 5 \cdot 561. \end{aligned}$$

□

Q. 3. (5 points) For two integers a, b, suppose that $\gcd(a, b) = 1$ and $b \geq a$. Prove that $\gcd(b + a, b - a) \leq 2$.

Solution: Now suppose that $d|(b+a)$ and $d|(b-a)$. Then $d|(b+a)+(b-a) = 2b$ and $d|(b+a)-(b-a) = 2a$. Thus, $d|\gcd(2b, 2a) = 2\gcd(a, b) = 2$. Thus, $d \leq 2$ and so $\gcd(b + a, b - a) \leq 2$.

[Alternate solution.] Since $\gcd(b, a) = 1$, then by Bezout's identity, there exist integers s and t such that $sb + ta = 1$. This gives us

$$\begin{aligned} (s + t)(b + a) + (s - t)(b - a) &= sb + sa + tb + ta + sb - sa - tb + ta \\ &= 2sb + 2ta \\ &= 2, \end{aligned}$$

from which we conclude that $\gcd(b + a, b - a)$ cannot exceed 2.

□

Q. 4. (10 points) Fermat's little theorem:

(a) State Fermat's little theorem.

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

(c) Computer $302^{302} \pmod{11}$.

Solution:

(a) If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

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

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

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

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

□

Q. 5. (10 points) Solve the following linear congruence equations.

(a) $778x \equiv 10 \pmod{379}$.

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

Solution:

(a) Note that 379 is a prime. To find the modular inverse of 778, we first apply Euclidean algorithm.

$$\begin{aligned} 778 &= 2 \cdot 239 + 20 \\ 379 &= 18 \cdot 20 + 19 \\ 20 &= 1 \cdot 19 + 1. \end{aligned}$$

Reading backwards we have $1 = 19 \cdot 778 - 39 \cdot 379$. Thus, we have $x \equiv 10 \cdot 10 \equiv 190 \pmod{379}$.

(b) Applying Euclidean algorithm, we have

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

Reading Euclidean algorithm backwards we have $1 = 37 \cdot 312 - 119 \cdot 97$. So, $312 \cdot 37 \equiv 1 \pmod{97}$. Thus, $x \equiv 37 \cdot 3 \equiv 111 \equiv 14 \pmod{97}$.

□

Q. 6. (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. 7. (10 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. 8. (8 points)

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

(b) Use (a) 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: 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 $n^2 \equiv 1 \pmod 4$.

By (a), the sum of two squares must be either $0+0=0$, $0+1=1$, or $1+1=2$, modulo 4, never 3, and therefore not of the form $4k+3$.

□

Q. 9. (8 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 $m|(ab-1)$, 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., $d|a$ and $d|m$. Since b and k are integers, it follows that $d|(ba - km)$, so $d|1$. Thus, we must have $d = 1$, which completes the proof.

□

Q. 10. (8 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. 11. (5 points) 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 $m = m_1 m_2 \cdots m_n$.

Solution:

Suppose that p is a prime appearing in the prime factorization of $m_1 m_2 \cdots m_n$. Because the m_i's are relatively prime, p is a factor of exactly one of the m_i's, say m_j. Because m_j divides $a - b$, it follows that $a - b$ has the factor p in its prime factorization to a power at least as large as the power to which it appears in the prime factorization of m_j. It follows that $m_1 m_2 \cdots m_n$ divides $a - b$, so $a \equiv b \pmod{m_1 m_2 \cdots m_n}$.

□

Q. 12. (5 points) Show that we can easily factor n when we know that n is the product of two primes, p and q, and we know the value of $(p-1)(q-1)$.

Solution: Suppose that we know both $n = pq$ and $(p-1)(q-1)$. To find p and q, first note that $(p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$. From this we can find $s = p+q$. Then with $n = pq$, we can use the quadratic formula to find p and q.

□

Q. 13. (10 points) Consider the RSA encryption method. Let our public key be $(n, e) = (65, 7)$, and our private key be d.

(a) What is the encryption $\hat{M}$ of a message $M = 8$?

(b) To decrypt, what value d do we need to use?

(c) Using d, run the RSA decryption method on $\hat{M}$.

Solution:

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

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

So the encrypted message is $\hat{M} = 57$.

(b) From $n = 65 = 5 \times 13$, we have $(p-1)(q-1) = 48$. Recall we can find d by running Euclidean algorithm.

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

Thus $d = \gcd(48, 7) = 1$. Reading backwards we get $1 = 7 \cdot 7 - 1 \cdot 48$. Then the private key $d = 7$.

(c) To complete the RSA decryption, we calculate

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

Therefore, the original message is $M = 8$ as desired.

□

Q. 14. (Optional, bonus 10 points) The following ciphertext is encrypted with one of the encryption methods we taught in lecture. Try to recover the plaintext and describe the method (and parameters) used for encryption. Please explain the process how you get the answer. For example, if you write a program, please provide the code (uploading the source file as well). If you make a guess and use number theory, please provide the details.

"Pwno vrj'an vrjot, wbuuzondd zd drlngwzot gr en wbk; bd vrj btn, wbuuzondd enhrlnd b trbi gwbg vrj hwbdn; orp vrj'mn tarpo, wbuuzondd zd b dgbgn rq lzok gwbg vrj gav gr joknadgbok."

Solution: "When you're young, happiness is something to be had; as you age, happiness becomes a goal that you chase; now you've grown, happiness is a state of mind that you try to understand." (1 point). It is encrypted with affine cipher with $a = 5$ and $b = 3$ (1 point), where $c = (ap + b) \mod 26$, where c is a letter in ciphertext and p is a letter in plaintext.

Explanation (8 points):

- The student wrote a program: Run the program. If it works well (i.e., inputting the ciphertext can lead to an output of the plaintext), then he or she can get the point. Note: If the program can output the correct sentence, but he or she did not write the sentence in the homework. It is ok to give he or she the above 1 point. So as a and b.

- The student used number theory techniques (on page 296 in our textbook): He or she needs to show $p \equiv \bar{a}(c - b) \pmod{26}$.

- The student used approaches other than programming and number theory: If the explanation makes sense, he or she can get the points. For example, the student may guess "vrj'an" as "you're" based on English language using, and solve a and b using linear equation systems. Note that the explanation must be complete and make sense.