CS201: Discrete Math for Computer Science
2024 Spring Semester Written Assignment #3
Due: Apr. 2th, 2025

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.

Q. 1. 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. Let a, b, and c be integers. Suppose m is an integer greater than 1 and $ac \equiv bc \pmod{m}$. Prove $a \equiv b \pmod{m/\gcd(c, m)}$.

Solution: Let $m' = m/\gcd(c, m)$. Because all the common factors of m and c are divided out of m to obtain m', it follows that m' and c are relatively prime. Since $ac \equiv bc \pmod{m}$, we have m divides $ac - bc = (a - b)c$, which follows that m' divides $(a - b)c$. Since m' and c are relatively prime, we see that m' divides $a - b$, which leads to $a \equiv b \pmod{m'}$.

Q. 3. 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. Given an integer a, we say that a number n passes the "Fermat primality test (for base a)" if $a^{n-1} \equiv 1 \pmod{n}$.

(a) For $a = 2$, does $n = 561$ pass the test?

(b) Did the test give the correct answer in this case?

Solution:

(a) We have

$$\begin{aligned} 2^{560} &\equiv 2^{20\cdot 28} \pmod{561} \\ &\equiv (2^{20})^{28} \pmod{561} \\ &\equiv (67)^{28} \pmod{561} \\ &\equiv (67^4)^7 \pmod{561} \\ &\equiv 1^7 \pmod{561} \\ &\equiv 1. \end{aligned}$$

Thus, $2^{560} \equiv 1 \pmod{561}$. So 561 passes the Fermat test with test value 2.

(b) We have $561 = 3 \cdot 11 \cdot 17$. So, 561 is not a prime, and thus the test failed.

Q. 5. 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. 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. 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. 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 $m = m_1 m_2 \cdots m_n$.

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. 9. 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.