CS201: Discrete Math for Computer Science
2020 Fall Semester   Written Assignment # 3
Due: Nov. 6th, 2020, please submit at the beginning of class

Q.1 What are the prime factorizations of

(a) 497

(b) 6560

(c) 10!

Solution:

(a) $497 = 7 \cdot 71$.

(b) $6560 = 2^5 \cdot 5 \cdot 41$.

(c) $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$.

$\square$

Q.2

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

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

Solution:

(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

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

$\square$

Q.3 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 $d|\gcd(a, b)$ and $d|y$. As $d|\gcd(a, b)$ we know $d|a$ and $d|b$. Thus, $d|a$ and $d|y$ so $d|\gcd(a, y) = d_1$. Similarly, $d|b$ and $d|y$ so $d|\gcd(b, y) = d_2$. Because $d|d_1$ and $d|d_2$ we know $d|\gcd(d_1, d_2)$. Hence we have $d \leq \gcd(d_1, d_2)$.

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

$\square$

Q.4

(a) Give the prime factorization of 312.

(b) Use Euclidean algorithm to find $\gcd(312, 97)$.

(c) Find integers s and t such that $\gcd(312, 97) = 312s + 97t$.

(d) Solve the modular equation

$$312x \equiv 3 \pmod{97}.$$

Solution:

(a) The prime factorization is $312 = 2^3 \cdot 3 \cdot 13$.

(b) Applying Euclidean algorithm, we have

$$\begin{aligned}
\gcd(312, 97) &= \gcd(97, 21) \qquad [312 = 3 \cdot 97 + 21] \\
&= \gcd(21, 13) \qquad [97 = 4 \cdot 21 + 13] \\
&= \gcd(13, 8) \qquad [21 = 1 \cdot 13 + 8] \\
&= \gcd(8, 5) \qquad [13 = 1 \cdot 8 + 5] \\
&= \gcd(5, 3) \qquad [8 = 1 \cdot 5 + 3] \\
&= \gcd(3, 2) \qquad [5 = 1 \cdot 3 + 2] \\
&= \gcd(2, 1) \qquad [3 = 1 \cdot 2 + 1] \\
&= 1.
\end{aligned}$$

(c) Reading Euclidean algorithm backwards we have

$$1 = 37 \cdot 312 - 119 \cdot 97.$$

(d) So $312 \cdot 37 \equiv 1 \pmod{97}$. Thus, $312 \cdot (37 \cdot 3) \equiv 3 \pmod{97}$. Now $37 \cdot 3 = 111 \equiv 14 \pmod{97}$. Hence, the solution is $x \equiv 14 \pmod{97}$.

□

Q.5

(a) State Fermat's little theorem.

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

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

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

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

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.6 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.7 Solve the following modular equations.

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

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

Solution:

(a) By Q.2 (a), we know that $29 \cdot 267 \equiv 1 \pmod{79}$. Thus, we have $x \equiv 29 \cdot 3 \equiv 87 \equiv 8 \pmod{79}$.

(b) 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 $x \equiv 10 \cdot 10 \equiv 190 \pmod{379}$. Reading Euclidean algorithm backwards we have $1 = 37 \cdot 312 - 119 \cdot 97$. So, $312 \cdot 37 \equiv 1 \pmod{97}$. Thus, $x \equiv 37 \cdot 3 \equiv 111 \equiv 14 \pmod{97}$.

$\square$

Q.8 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.

$\square$

Q.9 Convert the decimal expansion of each of these integers to a binary expansion.
(a) 231 (b) 4532 (c) 97644
Solution: (a) 11100111
(b) 1000110110100
(c) 10111110101101100

$\square$

Q.10
Convert the binary expansion of each of these integers to a octal expansion.

(a) $(1010\ 1010\ 1010)_2$

(b) $(101\ 0101\ 0101\ 0101)_2$

Solution:

(a) $(1010\ 1010\ 1010)_2 = (101\ 010\ 101\ 010)_2 = (5252)_8$

(b) $(101\ 0101\ 0101\ 0101)_2 = (101\ 010\ 101\ 010\ 101)_2 = (52525)_8$

$\square$

Q.11 Show that $\log_2 3$ is an irrational number. Recall that an irrational number is a real number x cannot be written as the ratio of two integers.
Solution: Suppose that $\log_2 3 = a/b$ where $a, b \in \mathbf{Z}^+$ and $b \neq 0$. Then $2^{a/b} = 3$, so $2^a = 3^b$. This violates the fundamental theorem of arithmetic. Hence $\log_2 3$ is irrational.

$\square$

Q.12

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 $\gcd(a, m) = \gcd(b, m)$.

$\square$

Q.13 Show that if a and m are relatively prime positive integers, then the inverse of a modulo m is unique modulo m.
Solution:

Suppose that b and c are both the inversed of a modulo m. Then $ba \equiv 1 \pmod{m}$ and $ca \equiv 1 \pmod{m}$. Hence, $ba \equiv ca \pmod{m}$. Because $\gcd(a, m) = 1$ it follows by Theorem 7 in Section 4.3 that $b \equiv c \pmod{m}$.

$\square$

Q.14 Prove that there are infinitely many primes of the form $4k+3$, where k is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes $q_1, q_2, \ldots, q_n$, and consider the number $4q_1q_2\cdots q_n - 1$.]

Solution: Suppose that there are only finitely many primes of the form $4k+3$, namely $q_1, q_2, \ldots, q_n$, where $q_1 = 3$, $q_2 = 7$, and so on.

Let $Q = 4q_1q_2\cdots q_n - 1$. Note that Q is of the form $4k+3$ (where $k = q_1q_2\cdots q_n - 1$). If Q is prime, then we have found a prime of the desired form different from all those listed.

If Q is not prime, then Q has at least one prime factor not in the list $q_1, q_2, \ldots, q_n$, because the remainder when Q is divided by q_j is $q_j - 1$, and $q_j - 1 \neq 0$. Because all odd primes are either of the form $4k+1$ or of the form $4k+3$, and the product of primes of the form $4k+1$ is also of this form (because $(4k+1)(4m+1) = 4(4km+k+m)+1$), there must be a factor of Q of the form $4k+3$ different from the primes we listed.

$\square$

Q.15

(a) Use Fermat's little theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, and $5^{2003} \bmod 13$.

(b) Use your results from part (a) and the Chinese remainder theorem to find $5^{2003} \bmod 1001$. (Note that $1001 = 7 \cdot 11 \cdot 13$.)

Solution:

(a) By Fermat's little theorem we know that $5^6 \equiv 1 \pmod 7$; therefore $5^{1998} = (5^6)^{333} \equiv 1^{75} \equiv 1 \pmod 7$, and so $5^{2003} = 5^5 \cdot 5^{1998} \equiv 3 \cdot 1 = 3 \pmod 7$, so $5^{2003} \bmod 7 = 3$. Similarly, $5^{10} \equiv 1 \bmod 11$; therefore $5^{2000} = (5^{10})^{200} \equiv 1 \pmod{11}$, and so $5^{2003} = 5^3 \cdot 5^{2000} \equiv 4 \pmod{11}$, so $5^{2003} \bmod 11 = 4$. Finally, $5^{12} \equiv 1 \pmod{13}$; therefore $5^{1992} = (5^{12})^{166} \equiv 1 \pmod{13}$, and so $5^{2003} = 5^{11} \cdot 5^{1992} \equiv 8 \pmod{13}$, so $5^{2003} \bmod 13 = 8$.

(b) 983

$\square$

Q.16 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.17 Show that the simultaneous solution of a system of linear congruences modulo pairwise relatively prime moduli is *unique* modulo the product of these moduli.
Solution: Suppose that there are two solutions to the system of linear congruences. Thus, suppose that $x \equiv a_i \pmod{m_i}$ and $y \equiv a_i \pmod{m_i}$ for all i. We want to show that these solutions are the same modulo m. This will guarantee that there is only one nonnegative solution less than m. The assumption certainly implies that $x \equiv y \pmod{m_i}$ for all i. But then the previous problem tells us that $x \equiv y \pmod{m}$, as desired.

□

Q.18 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 $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3$

(mod 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.

$\square$

Q.19 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.

$\square$

Q.20

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 text 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, $C^d \equiv M \pmod{pq}$.

$\square$