CS215: Discrete Math (H) for Computer Science
2021 Fall Semester Written Assignment # 3
Due: Nov. 5th, 2021, please submit at the beginning of class

Q.1 What are the prime factorizations of

(a) 511

(b) 6560

(c) 12!

Solution:

(a) $511 = 7 \cdot 73$.

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

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

$\square$

Q.2

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

(b) Find integers s and t such that $\gcd(561, 234) = 234s + 561t$.

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 (a), we have

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

$\square$

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.

□

Q.4 For two integers a, b, suppose that $\gcd(a, b) = 1$. Prove that

$$\gcd(b + a, b - a) \leq 2.$$

Solution: W.l.o.g., assume that $b \geq a$. 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.5 Prove that for three integers a, b, c, if $c|(a \cdot b)$, then $c|(a \cdot \gcd(b, c))$.
Solution: Since $c|(a \cdot b)$, we know that $kc = ab$ for some integer k. By Euclidean algorithm, 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 $c|(a \cdot \gcd(b, c))$.

$\square$

Q.6

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

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

(c) Solve the modular equation

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

Solution:

(a) Applying Euclidean algorithm, we have

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

(b) Reading Euclidean algorithm backwards we have

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

(c) 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 $x \equiv 14 \pmod{97}$.

$\square$

Q.7 Solve the following modular equations.

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

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

Solution:

(a) Applying Euclidean algorithm, we have

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

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

(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 Let a and b be positive integers. Show that $\gcd(a, b) + \operatorname{lcm}(a, b) = a + b$ if and only if a divides b, or b divides a.

Solution:

"only if" Assume that $\gcd(a, b) = d$, then we have $\operatorname{lcm}(a, b) = \frac{ab}{d}$, where d is an integer. Then we have $d + \frac{ab}{d} = a + b$, and we further have $d^2 - (a + b)d + ab = 0$, Solving this equation, we have $d = a$ or $d = b$. This means a divides b or b divides a.

"if" W.l.o.g., assume that $a|b$. Then we have $\gcd(a, b) = a$ and $\operatorname{lcm}(a, b) = b$. The conclusion then follows.

$\square$

Q.9 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.10

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

(b) 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:

(a) 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 $n^2 \equiv 1 \pmod{4}$.

(b) 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 $4k + 3$.

$\square$

Q.11 Find counterexamples to each of these statements about congruences.

(a) If $ac \equiv bc \pmod{m}$, where a, b, c, and m are integers with $m \geq 2$, then $a \equiv b \pmod{m}$.

(b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d, and m are integers with c and d positive and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$.

Solution:

(a) Let $m = c = 2$, $a = 0$ and $b = 1$. Then $0 = ac \equiv bc = 2 \pmod{2}$, but $0 = a \not\equiv b = 1 \pmod{2}$.

(b) Let $m = 5$, $a = b = 3$, $c = 1$, and $d = 6$. Then $3 \equiv 3 \pmod{5}$ and $1 \equiv 6 \pmod{5}$, but $3^1 = 3 \not\equiv 4 \equiv 729 = 3^6 \pmod{5}$.

□

Q.12 Convert the decimal expansion of each of these integers to a binary expansion.

(a) 321 (b) 1023 (c) 100632

Solution: (a) 101000001

(b) 1111111111

(c) 11000100100011000

□

Q.13

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

(a) $(1111\ 0111)_2$

(b) $(111\ 0111\ 0111\ 0111)_2$

Solution:

(a) $(1111\ 0111)_2 = (011\ 110\ 111)_2 = (367)_8$

(b) $(111\ 0111\ 0111\ 0111)_2 = (111\ 011\ 101\ 110\ 111)_2 = (73567)_8$

$\square$

Q.14 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.15

Prove that for every positive integer n, there are n consecutive composite integers.
Solution: There are n numbers in the sequences $(n+1)!+2$, $(n+1)!+3$, $\cdots$, $(n+1)!+(n+1)$. The first of these is composite because it is divisible by 2; the second is composite because it is divisible by 3; $\cdots$; the last is composite because it is divisible by $n+1$. This gives us the desired n consecutive composite integers.

$\square$

Q.16 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.17 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.

□

Q.18

(a) State Fermat's little theorem.

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

(c) Use Fermat's little theorem to compute $3^{302} \bmod 5$, $3^{302} \bmod 7$, and $3^{302} \bmod 11$.

(d) Use your results from part (c) and the Chinese remainder theorem to find $3^{302} \bmod 385$. (Note that $385 = 5 \cdot 7 \cdot 11$.)

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 know that $3^4 \equiv 1 \pmod{5}$; therefore $3^{300} = (3^4)^{75} \equiv 1^{75} \equiv 1 \pmod{5}$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \cdot 1 = 9 \pmod{5}$, so $3^{302} \bmod 5 = 4$. Similarly, $3^6 \equiv 1 \bmod 7$; therefore $3^{300} = (3^6)^{50} \equiv 1 \pmod{5}$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod{7}$, so $3^{302} \bmod 7 = 2$. Finally, $3^{10} \equiv 1 \pmod{11}$; therefore $3^{300} = (3^{10})^{30} \equiv 1 \pmod{11}$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod{11}$, so $3^{302} \bmod 11 = 9$.

(d) Since 3^{302} is congruent to 9 modulo 5, 7, and 11, it is also congruent to 9 modulo 385. (This is a particularly trivial application of the Chinese remainder theorem.)

□

Q.19 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.20 Solve the system of congruence $x \equiv 3 \pmod 6$ and $x \equiv 4 \pmod 7$ using the method of Chinese Remainder Theorem or 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.21 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.22 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) Recall we can find d by running Euclidean algorithm.

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

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.

$\square$

Q. 23 Consider the RSA system. Let (e, d) be a key pair for the RSA. Define

$$\lambda(n) = \mathrm{lcm}(p-1, q-1)$$

and compute $d' = e^{-1} \bmod \lambda(n)$. Will decryption using d' instead of d still work? (prove $C^{d'} \bmod n = M$)

Solution: <u>Case I:</u> $\gcd(M, n) = 1$.

$$\begin{aligned} C^{d'} \bmod n &= M^{ed'} \bmod n = M^{k\lambda(n)+1} \bmod n \\ &= (M^{k\lambda(n)} \bmod n)M \bmod n \\ &= \left(M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod n\right)^k M \bmod n \end{aligned}$$

By Fermat's theorem, $M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod p = \left(M^{(q-1)/\gcd(p-1,q-1)}\right)^{p-1} \bmod p = 1$ and $M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod q = 1$. Then by Chinese Remainder Theorem, we have $C^{d'} \bmod n = M$.

<u>Case II:</u> $\gcd(M, n) = p$. $M = tp$ for some integer $0 < t < q$. We have $\gcd(M, q) = 1$ and $ed' = k\lambda(n) + 1$ for some integer k. By Fermat's theorem, we have

$$(M^{k\lambda(n)} - 1) \bmod q = (M^{k(p-1)(q-1)/\gcd(p-1,q-1)} - 1) \bmod q = 0.$$

Then

$$\begin{aligned} (M^{ed'} - M) \bmod n &= M(M^{ed'-1} - 1) \bmod n \\ &= tp(M^{k\lambda(n)} - 1) \bmod pq \\ &= 0 \end{aligned}$$

<u>Case III:</u> $\gcd(M, n) = q$. Similar to Case II.
<u>Case IV:</u> $\gcd(M, n) = pq$. Trivial.

$\square$