CS215: Discrete Math (H)
2025 Fall Semester Written Assignment # 3
Due: Nov. 10th, 2025, please submit at the beginning of class

Q.1 What are the prime factorizations of

(1) 6560

(2) 12!

Solution:

(1) $6560 = 2^5 \cdot 5 \cdot 41$.

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

$\square$

Q.2 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

$\square$

Q.3 For two integers a, b, prove that if $\gcd(a, b) = 1$, then

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

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.

$\square$

Q.4

(1) Give the prime factorization of 312.

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

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

(4) Solve the modular equation

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

Solution:

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

(2) Applying Euclidean algorithm, we have

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

(3) Reading Euclidean algorithm backwards we have

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

(4) 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.5 Suppose that p, q and r are distinct primes. Show that there exist integers a, b and c, such that

$$a(pq) + b(qr) + c(rp) = 1.$$

Solution: Since p, q and r are distinct primes, we have $\gcd(p, r) = 1$ and by Bezout's theorem, we have $1 = sp + tr$ and further $s(pq) + t(qr) = q$. Now by $\gcd(q, rp) = 1$, so there exist integers u and v such that

$$uq + v(rp) = 1.$$

Therefore, we have

$$u(s(pq) + t(qr)) + v(rp) = (us)(pq) + (ut)(qr) + v(rp) = 1.$$

$\square$

Q.6 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.7 Prove that there are infinitely many primes of the form $6k + 5$.

Solution: (Proof by contradiction) Suppose not. Then the primes of this form are a finite set, say $S = \{p_1, p_2, \ldots, p_n\}$ is all of them. Let $P =$

$6p_1p_2\cdots p_n+5$. It is clear that none of p_i's can divide P. If P is prime, since it is of the form $6k+5$, and is bigger than each p_i, this contradicts the assumption that the list S is complete. If P is not prime, it can be divisible by neither 2 nor 3, and all other primes are either of the form $6a+5$ or $6a+1$. If all the prime factors of P have the form $6a+1$, their product would also have the form $6a+1$, so at least one prime factor of P must have form $6a+5$, a prime of from $6k+5$ not on the assumed complete list S.

$\square$

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

(1) Show that there is no integer solution x to the equation

$$x^2 \equiv 31 \pmod{36}.$$

(2) Find the integer solutions x to the system of equations

$$\begin{cases} x^2 \equiv 10 \pmod{31}, \\ x^2 \equiv 30 \pmod{37}. \end{cases}$$

Solution:

(1) Note that $36 = 4 \cdot 9$. If x is a solution to the equation, then we also have that

$$\begin{aligned} x^2 &\equiv 31 \equiv 3 \pmod{4}, \\ x^2 &\equiv 31 \equiv 4 \pmod{9}. \end{aligned}$$

Yet, there is no x such that $x^2 \equiv 3 \pmod{4}$. Hence there is no solution to this equation.

(2) Let $y = x^2$. Since $y \equiv 30 \pmod{37}$, we have that

$$y = 30 + 37k$$

for some integer k. The first equation becomes

$$30 + 37k \equiv 10 \pmod{31} \Leftrightarrow 6k \equiv -20 \equiv 11 \pmod{31}.$$

To solve this equation, we note that

$$31 = 5 \cdot 6 + 1 \Rightarrow (-5) \cdot 6 \equiv 1 \pmod{31}.$$

Hence, we have

$$(-5) \cdot 6k \equiv (-5) \cdot 11 \pmod{31} \Leftrightarrow k \equiv -55 \equiv 7 \pmod{31}.$$

As a consequence, k is of the form $7 + 31m$ for some integer m, which yields that

$$\begin{aligned} x^2 = y &= 30 + 37(7 + 31m) \\ &= 30 + 37 \cdot 7 + 37 \cdot 31m \\ &= 289 + 1147m = 17^2 + 1147m. \end{aligned}$$

Choosing $m = 0$, we obtain that $x = 17, -17$ are the integer solutions.

□

Q.10 Compute the following without calculator. You may find Fermat's little theorem useful for some of these.

(1) The last decimal digit of 3^{1000}

(2) 3^{1000} mod 31

(3) $3/16$ in $\mathbb{Z}_{31}$

Solution:

(1) The last decimal digit of 3^{1000} is equivalent to computing 3^{1000} mod 10. By Fermat's little theorem, we have $3^4 \equiv 1 \pmod 5$. Thus, $3^{1000} \equiv 1 \pmod 2$ and $3^{1000} \equiv 3^{4\times 250} \equiv 1 \pmod 5$. Then by Chinese remainder theorem, we have 3^{1000} mod $10 = 1$.

(2) By Fermat's little theorem, we have $3^{30} \equiv 1 \pmod{31}$. Then we have

$$3^{1000} \bmod 31 = 3^{30*33+10} \bmod 31 = 3^{10} \bmod 31.$$

By $3^2 \bmod 31 = 9$, $3^4 \bmod 31 = 9 * 9 \bmod 31 = 19$, $3^8 \bmod 31 = 19 * 19 \bmod 31 = 20$, we have $3^10 \bmod 31 = 9 * 20 \bmod 31 = 25$.

(3) In $\mathbb{Z}_{31}$, we have $3/16 = 3 * 16^{-1} \pmod{31}$. Since $\gcd(16, 31) = 1$, by extended Euclidean algorithm, we have $1 = 2 \times 16 - 31$. Thus, the modular inverse of 16 in $\mathbb{Z}_{31}$ is 2. Then we have $3/16 = 3 * 2 = 6$.

$\square$

Q.11 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.12 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 $m_1m_2\cdots m_n$ divides $a-b$, so $a \equiv b \pmod{m_1m_2\cdots m_n}$.

□

Q.13 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.14 Recall how the *linear congruential method* works in generating pseudorandom numbers: Initially, four parameters are chosen, i.e., the modulus m, the multiplier a, the increment c, and the seed x_0. Then a sequence of numbers $x_1, x_2, \ldots, x_n, \ldots$ are generated by the following congruence

$$x_{n+1} = (ax_n + c) \pmod m.$$

Suppose that we know the generated numbers are in the range $0, 1, \ldots, 10$, which means the modulus $m = 11$. By observing three consecutive numbers $7, 4, 6$, can you predict the next number? Explain your answer.

Solution: By the linear congruential method, we know that

$$\begin{aligned} x_{n+2} &= (ax_{n+1} + c) \pmod m \\ x_{n+1} &= (ax_n + c) \pmod m. \end{aligned}$$

Then we have

$$x_{n+2} - x_{n+1} \equiv a(x_{n+1} - x_n) \pmod{m}.$$

By the three consecutive numbers $7, 4, 6$, we then have

$$\begin{aligned} &(1) \quad 6 - 4 \equiv a(4 - 7) \pmod{11}, \\ &(2) \quad x - 6 \equiv a(6 - 4) \pmod{11}, \end{aligned}$$

where x denotes the next number. Eq. (1) gives $8a \equiv 2 \pmod{11}$, and we further have $a \equiv 3 \pmod{11}$. Then by Eq. (2), we have $x \equiv 6 + 3 \cdot 2 \equiv 1 \pmod{11}$. This means the next number is 1.

□

Q.15

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

(2) 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:

(1) 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 $5^{2003} \bmod 13 = 8$.

(2) 983

□

Q.16 Given an integer a, we say that a number n passes the "Fermat primality test (for base a)" if $a^{n-1} \equiv 1 \pmod{n}$.

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

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

Solution:

(1) 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.

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

□

Q.17 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.18 Consider the RSA encryption method. Let our public key be $(n, e) = (65, 7)$, and our private key be d.

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

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

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

Solution:

(1) 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 $\hat{M} = 57$.

(2) 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 $d = 7$.

(3) 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.19 Consider the RSA system. Let (e, d) be a key pair for the RSA. Define

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

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.

$\square$