**CS201: Discrete Math for Computer Science**
**2024 Spring Semester   Written Assignment #3**
**Due: Apr. 16th, 2023**

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.** Compute the following without calculator and explain your answer.

(1) $(33^{15} \mod 32)^3 \mod 15$

(2) $\gcd(210, 1638)$

(3) $34x \equiv 77 \pmod{89}$

(4) The last decimal digit of $3^{1000}$ (Hint: Fermat's little theorem)

**Solution:**

(1) This is mainly computed based on Corollary 2 on page 242, i.e., $ab \mod m = ((a \mod m)(b \mod m)) \mod m$. It is perfectly fine if the student does not mention this corollary.

$$\begin{aligned}
& (33^{15} \mod 32)^3 \mod 15 \\
= \; & ((33 \mod 32)^{15} \mod 32)^3 \mod 15 \\
= \; & (1 \mod 32)^3 \mod 15 \\
= \; & 1 \mod 15 \\
= \; & 1
\end{aligned}$$

(2) Using Euclidean Algorithm

$$\begin{aligned}
&1638 = 210 \cdot 7 + 168 \\
&210 = 168 \cdot 1 + 42 \\
&168 = 42 \cdot 4
\end{aligned}$$

Thus, $\gcd(210, 1638) = 42$.

(3) Consider the inverse $\bar{a}$ such that $\bar{a} \cdot 34 \equiv 1 \pmod{89}$. We use the extended Euclidean to solve $\bar{a}$. In particular,

$$\begin{aligned}
&89 = 34 \cdot 2 + 21\\
&34 = 21 \cdot 1 + 13\\
&21 = 13 \cdot 1 + 8\\
&13 = 8 \cdot 1 + 5\\
&8 = 5 \cdot 1 + 3\\
&5 = 3 \cdot 1 + 2\\
&3 = 2 \cdot 1 + 1\\
&2 = 1 \cdot 1
\end{aligned}$$

Thus,

$$\begin{aligned}
1 &= 3 - 2 \cdot 1 & \\
&= 3 - (5 - 3 \cdot 1) \cdot 1 & &= -5 \cdot 1 + 3 \cdot 2\\
&= -5 \cdot 1 + (8 - 5 \cdot 1) \cdot 2 & &= 8 \cdot 2 - 5 \cdot 3\\
&= 8 \cdot 2 - (13 - 8 \cdot 1) \cdot 3 & &= -13 \cdot 3 + 8 \cdot 5\\
&= -13 \cdot 3 + (21 - 13 \cdot 1) \cdot 5 & &= 21 \cdot 5 - 13 \cdot 8\\
&= 21 \cdot 5 - (34 - 21 \cdot 1) \cdot 8 & &= -34 \cdot 8 + 21 \cdot 13\\
&= -34 \cdot 8 + (89 - 34 \cdot 2) \cdot 13 & &= 89 \cdot 13 - 34 \cdot 34
\end{aligned}$$

Thus, we have $-34 \cdot 34 \mod 89 = 1$, which implies that $55 \cdot 34 \mod 89 = 1$. Thus, $\bar{a} = 55$. As a result, we have $x \equiv 55 \cdot 77 \pmod{89} \equiv 52 \pmod{89}$.

(4) The last decimal digit of $3^{1000}$ is equivalent to computing $3^{1000} \bmod 10$. By Fermat's little theorem, we have $3^4 \equiv 1 \pmod 5$. Thus, $3^{1000} \equiv 3^{4 \times 250} \equiv 1 \pmod 5$. In addition, $3^{1000} \equiv 1 \pmod 2$, because $3^{1000}$ has only 3 as its factor and hence is an odd number. Then, since system $3^{1000} \equiv 1 \pmod 5$ and $3^{1000} \equiv 1 \pmod 2$ is equivalent to $3^{1000} \equiv 1 \pmod{10}$, we have $3^{1000} \bmod 10 = 1 \bmod 10 = 1$.

**Q. 2.** Use extended Euclidean algorithm to express $\gcd(561, 234)$ as a linear combination of 561 and 234.

**Solution:** 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, $\gcd(561, 234) = 3$. Accordingly, we can derive the linear combination:

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

**Q. 3.** 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. 4.** 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. 5.** 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. 6.** 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. 7.** 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. 8.** (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.** 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.** 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. 11.** 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. 12.** 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.

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

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.