CS1802 Week4: Modulo Arithmetic, Inverse, Euclid, proofs

Modular Arithmetic

i. Compute each value. Recall that a value mod $n$ should always produce a number in the range $[0, n)$.

1. $(5 + 6) \mod 7$

2. $(3 - 4) \mod 6$

3. $6^2 \mod 7$

4. Notice that $-1 \mod 7$ is equal to $6 \mod 7$. The reverse is true as well; you can think of $6$ as $-1 \pmod{7}$, which is easier to square, and you will get the same result. Using this trick (put away that calculator), what is the square of $99998 \mod 100000$?

5. Compute $9999^{40000} \mod 10000$, again without using a calculator.

Solution:

1. $11 = 4 \mod 7$

2. $-1 = 5 \mod 6$

3. $36 = 1 \mod 7$

4. $(-2)^2 = 4 \mod 100000$

5. This is $(-1)^{20000} = 1^{20000} = 1$. (Alternately, you could reason that the result will alternate between $n - 1$ and $1$, and $40000$ is even.)

ii. The additive inverse mod $n$ of a number $a$ is the number $b$ that must be added to $a$ to get $0 \pmod n$. Find the additive inverses of these numbers.
1. 12 mod 31

2. 127 mod 256

3. Convert the additive inverse of 127 mod 256 to binary. What does this value mean if interpreted as 8-bit two’s complement? Is this a coincidence?

**Solution:**

1. 19
2. 129
3. 10000001 in two’s complement is -127, the additive inverse of 127. 8-bit two’s complement is specifically finding numbers that add to 100000000 = 256, so it makes sense that the additive inverse in decimal would always be the same as the two’s complement in binary.

**Proofs**

Recall that a proof is essentially an argument that would lead a reasonable reader to conclude that the statement in question must be true.

i. Prove this fact suggested in the last section, using the other facts you know about modular arithmetic and some algebra: \((n - m)^2 \mod n = m^2 \mod n\) for integers \(m\) and \(n\) where \(0 < m < n\).

**Solution:** \((n - m)^2 \mod n = n^2 - 2mn + m^2\), and since \(n^2 - 2mn = 0 \mod n\), we’re left with \(m^2 \mod n\).

ii. Prove that for all integers \(n > 2\), there are at least two integers \(a\) such that \(0 < a < n\) and \(a^2 \mod n = 1\).
Solution: We know from the previous problem that \((n - 1)^2 = 1 \mod n\). Also, \(1^2 = 1 \mod n\). As long as these two numbers are different, these are the required two numbers that square to 1. Since \((n - 1) \neq 1\) for \(n > 2\), these numbers are different, so these are the two required numbers.

iii. Prove by contradiction that repeatedly applying the function \(f(x) = ax \mod n\) to a number, for arbitrary whole numbers \(a\) and \(n\), must eventually repeat a number. (For example, if \(f(x) = 5x + 3 \mod 7\), then \(f(2) = 6, f(6) = 5, f(5) = 0, f(3) = 4, f(4) = 2\) and we’re back to the beginning.)

Solution: Suppose applying the function never repeats a value; then repeatedly applying this function will produce different values forever. But that’s not possible because there are only a finite number of different possible results \(\mod n\). Contradiction; the function must repeat a value.

Division and powers mod n

i. Compute by hand

1. \(2017^0 \mod 5\)
2. \(2017^1 \mod 5\)

3. \(2017^{10} \mod 5\)

4. \(2017^{100} \mod 5\)

**Solution:**

1. 1
2. 2
3. 4
4. 1

**Solution:** Considering the powers \(a^i \mod p, i = 1, 2, \ldots\) it is clear that the sequence must repeat at some point since there are only a finite number of different values (at most \(p - 1\)) that it can take. Let \(x\) and \(y > x\) be positive integers such that \(a^x = a^y \mod p\), i.e. \(a^x(a^{y-x} - 1) = 0 \mod p\). But \(a\) is coprime to \(p\) and hence we see that \(n = y - x\) satisfies \(a^n = 1 \mod p\).

**Primes**

i. Compute the prime factorization of

1. 120

2. \(\text{lcm}(3^3 \cdot 5^2, 2 \cdot 3^4)\)
3. $7!$, i.e. $7$ factorial

Solution:

1. $2^3 \cdot 3 \cdot 5$
2. $2 \cdot 3^4 \cdot 5^2$
3. $2^4 \cdot 3^2 \cdot 5 \cdot 7$

Solution: Proof by contradiction. Assume not. Let there be $k$ primes and let them be $p_1, p_2, \ldots, p_k$. Consider $X = 1 + \prod_{i=1}^{k} p_i$. Observe that $X \equiv 1 \pmod{p_i}$ for all primes $p_i$ and hence $X$ cannot be written as the product of the existing primes and so there must exist a prime different from any of the $p_i$ - a contradiction.
Euclid’s Algorithm

i. Compute using Euclid’s algorithm

1. $\text{gcd}(600, 658)$

2. $\text{gcd}(28, 441)$

Solution:

1. $\text{gcd}(658, 600) = \text{gcd}(600, 58) = \text{gcd}(58, 20) = \text{gcd}(20, 18) = \text{gcd}(18, 2) = \text{gcd}(2, 0) = 2$

2. $2 \cdot \text{gcd}(441, 28) = \text{gcd}(28, 21) = \text{gcd}(21, 7) = \text{gcd}(7, 0) = 7$

ii. Prove that, for all positive integers $a, b$ that $\text{lcm}(a, b) \cdot \text{gcd}(a, b) = a \cdot b$.

Solution: Let $a = \Pi_i p_i^{\alpha_i}$ and $b = \Pi_i p_i^{\beta_i}$ be the prime factorizations of $a$ and $b$ respectively. Then $\text{lcm}(a, b) = \Pi_i p_i^{\max(\alpha_i, \beta_i)}$ and $\text{gcd}(a, b) = \Pi_i p_i^{\min(\alpha_i, \beta_i)}$ and since $\max(\alpha, \beta) + \min(\alpha, \beta) = \alpha + \beta$ it follows that $\text{lcm}(a, b) \cdot \text{gcd}(a, b) = a \cdot b$. 
Modulo inverse via enumerating powers

i. Calculate the multiplicative inverse of \(a=9\) modulo \(n=26\) by constructing the set of \(9\)-powers \(P_9 = \{9, 9^2, 9^3, ..., 9^v = 1\} \mod 26\) and finding the order \(v\) of \(9 \mod 26\).

\[
\text{Solution: } 9^2 = 81 = 3 \mod 26 \\
9^3 = 27 = 1 \mod 26 \\
P_9 = \{9, 3, 1\} \\
\text{order } v = 3 \text{ inverse is } 9^{v-1} = 9^2 = 3
\]

ii. Calculate the multiplicative inverse of \(a=7\) modulo \(n=26\) by constructing the set of \(7\)-powers \(P_7 = \{7, 7^2, 7^3, ..., 7^v = 1\} \mod 26\), and finding the order \(v\) of \(7 \mod 26\).

\[
\text{Solution: } 7^2 = 49 = 23 = -3 \mod 26 \\
7^3 = -3 \times 7 = -21 = 5 \mod 26 \\
7^4 = (7^2)^2 = (-3)^2 = 9 \mod 26 \\
7^5 = 9 \times 7 = 63 = 11 \mod 26 \\
7^6 = (7^3)^2 = 25 = -1 \mod 26 \\
7^7 = 7^3 \times 7^4 = 45 = 19 \mod 26 \\
7^8 = (7^4)^2 = 81 = 3 \mod 26 \\
7^9 = 3 \times 7 = 21 \mod 26 \\
7^{10} = 7^6 \times 7^4 = -9 = 17 \mod 26 \\
7^{11} = 7^6 \times 7^5 = -11 = 15 \mod 26 \\
7^{12} = (7^6)^2 = 1 \mod 26 \\
P_7 = \{7, 23, 5, 9, 11, 25, 19, 3, 21, 17, 15, 1\} \\
\text{order } v = 12 \text{ inverse is } 7^{v-1} = 7^{11} = 15
\]

iii. Calculate the multiplicative inverse of \(a=4\) modulo \(n=15\) by constructing the set of \(4\)-powers \(P_4 = \{4, 4^2, 4^3, ..., 4^v = 1\} \mod 15\) and finding the order \(v\) of \(4 \mod 15\).

\[
\text{Solution: } 4^2 = 16 = 1 \mod 15 \\
P_4 = \{4, 1\} \\
\text{order } v = 2 \text{ inverse is } 4^{v-1} = 4^1 = 4
\]

iv. Calculate the multiplicative inverse of \(a=6\) modulo \(n=15\) by constructing the set of \(6\)-powers \(P_6 = \{6, 6^2, 6^3, ..., 6^v = 1\} \mod 15\) and finding the order \(v\) of \(6 \mod 15\).

\[
\text{Solution: } \text{There is no inverse because } \gcd(6, 15) = 3. \text{ But we can still build up the powers of } 6 \text{ mod 15 until they repeat} \\
6^2 = 36 = 6 \mod 15 \\
P_6 = \{6\}
\]
EXTRA : 10 wise men

10 wise men leave in a village; each man has a color dot on the forehead either R or B not known to him; knowing his color means immediate death. But everyone knows the other men’s colors, so B person sees 5R and 4B.

The men don’t speak/communicate to each other, but each morning they meet in a circle and they can see if anyone died. They are extremely smart (can infer anything) and know when someone dies its because he must have figured out his color.

For quite a few days this goes unchanged, until one day a stranger passes to the village and remarks “the number of B colors is not 20”. Prove that eventually everyone in the village will figure out his color and die.

hint1. Put yourself in the shoes of a B wise man. He knows there are 5R and 4B, so what an R person sees?
- if you have B, the R person sees 5B and 4R : that implies a total 5B+5R
- if you have R, the R person sees 5R and 4B : that implies a total 4B+6R

An R person would kill himself the moment he figure out his color (R), and thats equivalent with figuring out which one of the two cases above is correct, or equivalent with figuring out that there are not a total of 6R.

How can an R person tell there are not 6R+4B total ? Well suppose there are 6R+4B (from his point of view that is possible). What would happen then ? What a different R person sees?

EXTRA : implement binary search in your favorite language. Easy choices: Python, Perl, Matlab, Ruby, Groovy; best for CS=Python; best for Math=Matlab