UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 2 – Number theory and relations
Lecture 2.03 – Modular arithmetic

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

The mod operator

Recall the Division Theorem states that for any integers a and b with $b \neq 0$, there exist unique integers q and r such that both

$$a = qb + r \quad \text{and} \quad 0 \leq r < |b|.$$

In many situations, we are particularly interested in the remainder r.

Notation. The modulo operator mod returns the canonical remainder when one integer is divided by another. We write $a \bmod b$, read as "a modulo b", to mean the (smallest non-negative) remainder when a is divided by b. That is, given integers a and b with $b \neq 0$, we have $a \bmod b = r$ where $0 \leq r < |b|$ and $a = qb + r$ for some $q, r \in \mathbb{Z}$.

Example. Find the following values:

- $19 \bmod 4 =$
- $-11 \bmod 5 =$
- $333 \bmod 3 =$

Notice that $a \bmod b = 0$ if and only if $b \mid a$.

In most computer programming languages, the mod operator is represented by the character %. However, this symbol is never used for this purpose in mathematical texts.

Modular congruence

We saw that $19 \bmod 4 = 3$, and of course there are infinitely many integers x such that $x \bmod 4 = 3$. We can think of all such numbers as having something in common, and say they belong to the same equivalence class. Instead of writing (for example) $19 \bmod 4 = 47 \bmod 4$, we can use a special congruence notation $19 \equiv 47 \pmod 4$.

Notation. Given integers a and b and a positive integer m, we say that a and b are congruent modulo m and write $a \equiv b \pmod m$ to mean that $a \bmod m = b \bmod m$.

The following are all equivalent statements:

- $a \equiv b \pmod m$.
- $a \bmod m = b \bmod m$.
- a and b have the same remainder when divided by m.
- $a = b + mk$ for some integer k.
- $m \mid (a - b)$.

Challenge. Prove the above statements are equivalent.

Properties of modular arithmetic

Suppose $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Below are several useful properties of modular arithmetic:

- If $a \equiv b \pmod{m}$, and $k \in \mathbb{Z}^+$ satisfies $k \mid m$, then $a \equiv b \pmod{k}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
- If $a \equiv b \pmod{m}$, then $a + k \equiv b + k \pmod{m}$ for all $k \in \mathbb{Z}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for all $k \in \mathbb{Z}$.
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{mk}$ for all $k \in \mathbb{Z}^+$.
- If $ak \equiv bk \pmod{mk}$ for some $k \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$.
  (If there is a divisor common to both sides of the congruence and the modulus, we can "divide" all terms through by that common divisor.)
- If $ak \equiv bk \pmod{m}$ for some $k \in \mathbb{Z}$, and $\gcd(m, k) = 1$, then $a \equiv b \pmod{m}$.
  (If there is a divisor common to both sides of the congruence and it is coprime with the modulus, we can "divide" both sides of the congruence through by that common divisor.)
- If $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$ for all $k \in \mathbb{Z}^+$.

Properties of modular arithmetic – Proofs

Proofs are provided for two of these properties...

Theorem. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof.

Theorem. If $ak \equiv bk \pmod{m}$ for some $k \in \mathbb{Z}$, and $\gcd(m, k) = 1$, then $a \equiv b \pmod{m}$.

Proof.

Challenge. Using similar approaches, prove that the other properties hold.

Similar problems appear in Problem Set 2, Questions 6 and 8.

Problem-solving with modular arithmetic

Having established these properties of modular arithmetic, we now have a useful set of tools for solving problems that involve divisibility or remainders.

Example. Prove that a natural number is divisible by 3 if and only if its digit sum is divisible by 3.

Solution.

Reducing powers modulo m

Finding large powers of the form a^k modulo m can be difficult, since while we are allowed to reduce a modulo m, we cannot reduce the power k in the same way. However, it is always possible to simplify the expression by finding small powers of a that reduce to smaller values modulo m, helping to decrease the value of a^k in steps. Typically, we look for a small power of a that is close to 0 (ideally 1 or -1) modulo m.

Example. Find $7^{1001} \bmod 12$.

Solution.

Example. Find $12^{1001} \bmod 7$.

Solution.

Reducing powers modulo m – Example 2

Example. Find $5^{1001} \bmod 93$.

Solution.

Reducing powers modulo m – Example 3

Example. Find $3^{103} \bmod 15$.

Solution.

Alternate solution.

Fermat's Little Theorem

A useful theorem for simplifying powers in prime moduli is Fermat's Little Theorem:

Theorem. (Fermat's Little Theorem)
For any prime p and any integer a such that $p \nmid a$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. (See MATH2400 – Finite Mathematics!)

Note that $p - 1$ is not necessarily the smallest non-negative power of a that is 1 modulo p.

Example. Find the following values.

- $99^{100} \bmod 101$.

  Solution.

- $99^{909} \bmod 101$.

  Solution.