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:

- $19 \bmod 4 = 3$.
- $-11 \bmod 5 = 4$.
- $333 \bmod 3 = 0$.

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. Since $a \equiv b \pmod{m}$, we know that $a = b + mk$ for some integer k, and since $c \equiv d \pmod{m}$, we know $c = d + ml$ for some integer l. So $ac = (b+mk)(d+ml) = bd + mbl + mdk + m^2kl = bd + m(bl + dk + mkl)$ where $bl + dk + mkl \in \mathbb{Z}$. Thus $ac \equiv bd \pmod{m}$.

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. Since $ak \equiv bk \pmod{m}$, we know that $m \mid (ak - bk)$, so $m \mid k(a - b)$. By the GCD Property 5 from Lecture 2.01, since $\gcd(m, k) = 1$, we must have that $m \mid (a - b)$, which is equivalent to saying $a \equiv b \pmod{m}$.

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. Let n be any natural number with $k+1$ digits $d_0, d_1, d_2, \dots, d_k$ from right to left, so that

$$n = 10^0 d_0 + 10^1 d_1 + 10^2 d_2 + \cdots + 10^k d_k$$

where each d_i is an integer between 0 and 9 inclusive. Then working modulo 3, since $10 \bmod 3 = 1$, we have

$$\begin{aligned} n &= 10^0 d_0 + 10^1 d_1 + 10^2 d_2 + \cdots + 10^k d_k \\ &\equiv 1^0 d_0 + 1^1 d_1 + 1^2 d_2 + \cdots + 1^k d_k \pmod 3 \\ &\equiv d_0 + d_1 + d_2 + \cdots + d_k \pmod 3. \end{aligned}$$

Thus n has the same residue modulo 3 as its digit sum. So in particular, $n \bmod 3 = 0$ if and only if n's digit sum is congruent to 0 modulo 3, meaning n is divisible by 3 if and only if its digit sum is divisible by 3.

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. Checking small powers of 7, we first find that $7^2 \equiv 49 \equiv 1 \pmod{12}$. So we have

$$7^{1001} \equiv \left(7^2\right)^{500} \times 7^1 \equiv 1^{500} \times 7 \equiv 7 \pmod{12},$$

meaning $7^{1001} \bmod 12 = 7$.

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

Solution. First we can note that $12^{1001} \equiv (-2)^{1001} \pmod 7$. Checking small powers of 2, we find that $(-2)^3 = -8 \equiv -1 \pmod 7$, so

$$(-2)^{1001} \equiv \left((-2)^3\right)^{333} \times (-2)^2 \equiv (-1)^{333} \times 4 \equiv -4 \equiv 3 \pmod 7.$$

Thus $12^{1001} \bmod 7 = 3$.

Reducing powers modulo m – Example 2

Example. Find 5^{1001} mod 93.

Solution. In order to check small powers of 5 here, it can be useful to use a table. Working modulo 93, we have:

n	1	2	3	4	5	6	...
5^n	5	25	32	-26	-37	1	...

Notice that to find each entry in this table, we only needed to multiply the previous entry by 5 and reduce the result modulo 93. To keep the multiplications manageable, we can always choose to use the reduced value that is closest to 0. For example, to find 5^4 modulo 93, we did the following:

$$5^4 = 5^3 \times 5 \equiv 32 \times 5 \equiv 160 \equiv 67 \equiv -26 \pmod{93}.$$

Seeing that $5^6 \equiv 1 \pmod{93}$, we can deduce that

$$5^{1001} \equiv \left(5^6\right)^{166} \times 5^5 \equiv 1^{166} \times (-37) \equiv -37 \equiv 56 \pmod{93}.$$

That is, 5^{1001} mod $93 = 56$.

Reducing powers modulo m – Example 3

Example. Find 3^{103} mod 15.

Solution. We can again check small powers of 3 here, working modulo 15:

n	1	2	3	4	5	...
3^n	3	9	12	6	3	...

In this case, we can see we will never encounter a power of 3 that gives 1 modulo 15. But we can also see that the powers of 3 modulo 15 repeat with period 4. So $3 \equiv 3^5 \equiv 3^9 \equiv 3^{13} \equiv \cdots \equiv 3^{101} \pmod{15}$, and thus

$$3^{103} \equiv 3^{101} \times 3^2 \equiv 3 \times 9 \equiv 27 \equiv 12 \pmod{15}.$$

Alternate solution. We can divide both the value and its modulus by the common factor of 3 and first find 3^{102} mod 5. In this case, we can notice that $3^2 = 9 \equiv -1 \pmod 5$, so

$$3^{102} \equiv (3^2)^{51} \equiv (-1)^{51} \equiv -1 \equiv 4 \pmod 5.$$

So $3^{102} \equiv 4 \pmod 5$, and we can now multiply both sides of the congruence and the modulus through by 3 to find $3^{103} \equiv 12 \pmod{15}$.

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. Since 101 is prime, by FLT, $a^{100} \equiv 1 \pmod{101}$ for all integers a where $101 \nmid a$. So in this case we must have $99^{100} \bmod 101 = 1$.

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

  Solution. We just showed that $99^{100} \bmod 101 = 1$, so

$$99^{909} = (99^{100})^9 \times 99^9 \equiv 1 \times (-2)^9 \equiv -512 \equiv 94 \pmod{101}.$$