Modular Arithmetic

Definition 1. Given an integer m called the *modulus*, we say for $a, b \in \mathbb{Z}$ that $a \equiv b \pmod{m}$ (a is *congruent* to b modulo m) if $m \mid a - b$.

Example 1. $5 \equiv 2 \pmod{3}$, $29 \equiv 5 \pmod{8}$, $-3 \equiv -7 \pmod{4}$

Consider $a = mq + r$, where r is the remainder when dividing a by m. Then $a \equiv r \pmod{m}$, i.e., computing modulo m means taking the remainder when dividing by m.

The following three statements are equivalent:

(1) $a \equiv b \pmod{m}$.
(2) There is $k \in \mathbb{Z}$ with $a = b + km$.
(3) When divided by m, both a and b leave the same remainder.

Note. $a \equiv 0 \pmod{m}$ means that $m \mid a$.

Note. When performing modular arithmetic on a computer, it is usually convienient to work with least positive remainders. In other words, represent $a \bmod m$ by the unique integer $r \in \{0, 1, \ldots, m-1\}$ such that $a \equiv r \pmod{m}$. In most languages, the % operator returns a negative remainder if one of the operands is negative; you need to make it positive yourself.

```
a = -5 % 3     // a = -2
if (a < 0)
  a += 3       // a = 1
```

Congruence modulo m satisfies the following properties:

(1) $a \equiv a \pmod{m}$ (reflexive)
(2) $a \equiv b \pmod{m} \longrightarrow b \equiv a \pmod{m}$ (symmetric)
(3) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$ (transitive property)
(4) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Rules for working modulo m :

(1) Constants can be reduced modulo m (use least positive remainders).
(2) You can add or subtract anything from both sides of an equation.
(3) You can multiply anything to both sides of an equation.
(4) You can divide both sides by r if $\gcd(r, m) = 1$. If $d = \gcd(r, m) \neq 1$, you can do the same but the result is correct modular m/d.
(5) To change $-k \pmod{m}$ to its positive equivalent, add enough m's to $-k$ until it is positive.
(6) (Cancellation laws) If $a + k \equiv b + k \pmod{m}$, then $a \equiv b \pmod{m}$. If $ak \equiv bk \pmod{m}$, then $a \equiv b \pmod{m/\gcd(m, k)}$.

Example 2. Solve $6x + 5 \equiv -7 \pmod{4}$.

We have

$$\begin{aligned} 6x + 5 &\equiv -7 \pmod{4} \\ 2x + 1 &\equiv 1 \pmod{4} && \text{(reduce constants modulo 4)} \\ 2x &\equiv 0 \pmod{4} && \text{(subtract 1 from both sides)} \\ x &\equiv 0 \pmod{2} && \text{(divide both sides by 2)} \ . \end{aligned}$$

Inversion

Division (except for the cancellation law) in not defined for modular arithmetic per se. However, the essence of division is captured by the notion of *multiplicative inverses*. For example, in the real numbers $\mathbb{R}$, the multiplicative inverse of $x \in \mathbb{R}$ is defined to be the real number x^{-1} such that $xx^{-1} = x^{-1}x = 1$. Division in $\mathbb{R}$ can be viewed as multiplication by inverses, for example, x/y is the same as xy^{-1}.

Multiplicative inverses modulo m are defined analogously.

Definition 2. A multiplicative inverse of a modulo m is any integer a^{-1} such that $aa^{-1} \equiv a^{-1}a \equiv 1 \pmod{m}$.

Any integer x which satisfies the linear congruence

$$ax \equiv 1 \pmod{m}$$

is an inverse of a modulo m. Note that this linear congruence is soluble if and only if $\gcd(a, m) = 1$, i.e., a has a multiplicative inverse modulo m if and only if $\gcd(a, m) = 1$. Also, if it is soluble, then there are infinitely many solutions; if a^{-1} is an inverse of a, then $a^{-1} + km$ is also an inverse for any $k \in \mathbb{Z}$.

Example 3. $7^{-1} \equiv 15 \pmod{26}$, since

$$7 \cdot 15 \equiv 15 \cdot 7 \equiv 105 \equiv 1 \pmod{26} \ .$$

$7^{-1} \pmod{26}$ exists because $\gcd(7, 26) = 1$. $41 = 15 + 26$, $67 = 15 + 2 \cdot 26$, and $-63 = 15 - 3 \cdot 26$ are also inverses. Indeed, $15 + 26k$, $k \in \mathbb{Z}$, are all inverses of 7, since

$$7(15 + 26k) \equiv (15 + 26k)7 \equiv 105 + 26(7k) \equiv 1 \pmod{26} \ .$$

Example 4. Compute $D = \left(\begin{smallmatrix} 7 & 9 \\ 3 & 12 \end{smallmatrix}\right)^{-1} \pmod{26}$.

We will use the fact that if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbb{R}^{2\times 2}$, then

$$A^{-1} = \frac{1}{|A|}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \ .$$

In our case, $A = \left(\begin{smallmatrix} 7 & 9 \\ 3 & 12 \end{smallmatrix}\right)$, $|A| = 57$, and

$$A^{-1} = \frac{1}{57}\begin{pmatrix} 12 & -9 \\ -3 & 7 \end{pmatrix} \ .$$

To verify that this is indeed an inverse (over $\mathbb{R}^{2\times 2}$) we compute

$$A^{-1}A = \frac{1}{57}\begin{pmatrix} 12 & -9 \\ -3 & 7 \end{pmatrix}\begin{pmatrix} 7 & 9 \\ 3 & 12 \end{pmatrix} = \frac{1}{57}\begin{pmatrix} 57 & 0 \\ 0 & 57 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ .$$

To compute $A^{-1} \pmod{26}$, we first need to compute $57^{-1} \pmod{26}$. Since $\gcd(57, 26) = 1$, we know it exists, i.e., the linear congruence

$$57x \equiv 5x \equiv 1 \pmod{26} \tag{1}$$

has a solution. To compute 57^{-1}, we can either solve (1) using the extended Euclidean algorithm, or (since the modulus 26 is so small), simply find it by trial and error. We compute $57^{-1} \equiv 5^{-1} \equiv 21 \pmod{26}$.

Once we have $57^{-1} \pmod{26}$, the rest of the computation proceeds as follows:

$$\begin{aligned} A^{-1} &\equiv 57^{-1} \begin{pmatrix} 12 & -9 \\ -3 & 7 \end{pmatrix} \pmod{26} \\ &\equiv 21 \begin{pmatrix} 12 & 17 \\ 23 & 7 \end{pmatrix} \pmod{26} \\ &\equiv \begin{pmatrix} 252 & 357 \\ 483 & 147 \end{pmatrix} \pmod{26} \\ &\equiv \begin{pmatrix} 18 & 19 \\ 15 & 17 \end{pmatrix} \pmod{26} \ . \end{aligned}$$

Verify:

$$A^{-1}A = \begin{pmatrix} 261 & 286 \\ 234 & 261 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26} \ .$$