Recap

Rec Yesterday, we defined, for $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$,

$a \equiv b \pmod{m}$ to mean $m \mid (a-b)$

$a \bmod m$ to mean the remainder after dividing a by m.

and showed

$a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$

iff $a = km + b$ for some $k \in \mathbb{Z}$.

Ex Note that $38 - 16 = 22 = 2 \cdot 11$. So $11 \mid (38-16)$. Then

① By definition, $38 \equiv 16 \pmod{11}$

② $38 \bmod 11 = 16 \bmod 11$

$38 = 3 \cdot 11 + 5 \Rightarrow 38 \bmod 11 = 5$

$16 = 1 \cdot 11 + 5 \quad\quad 16 \bmod 11 = 5$

③ $38 = 11k + 16$

$38 - 16 = 22 = 11k \Rightarrow k = 2$

$38 = 2 \cdot 11 + 16$

Rec By the Division Algorithm, $0 \leq a \bmod m < m$. Since $a \equiv b \pmod{m} \iff a \bmod m = b \bmod m$, we can associate all congruent numbers to a number in $\{0, 1, \ldots, m-1\}$.

Ex Consider the integers mod 3.

$\{\ldots, -6, -3, 0, 3, 6, \ldots\}$ $(\equiv 0 \pmod 3$ i.e. $3k)$

$\{\ldots, -5, -2, 1, 4, 7, \ldots\}$ $(\equiv 1 \pmod 3$ i.e. $3k+1)$

$\{\ldots, -4, -1, 2, 5, 8, \ldots\}$ $(\equiv 2 \pmod 3$ i.e. $3k+2)$

When working with respect to a modulus m, we only have to think about $\{0, 1, \ldots, m-1\}$

If a number is not in that range, we can repeatedly shift by m until it is.

Rec As a result of what we proved, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$a + c \equiv b + d \pmod{m}$ $\quad\quad ac \equiv bd \pmod{m}$

Ex Note that $154324 \equiv 4 \pmod 5$ and $-76938 \equiv 2 \pmod 5$.

$154324 - 76938 \equiv 4 + 2 \equiv 6 \equiv 1 \pmod 5$

$154324 \cdot (-76938) \equiv 4(2) \equiv 8 \equiv 3 \pmod 5$

Exponentiation

Rec For $a \in \mathbb{Z}$, $n \in \mathbb{N}$, a^n denotes $\underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ times}}$

Alg We want to compute $a^n \bmod m$.

Observe: if $n = 2k$, $a^n = a^{2k} = a^k a^k$

if $n = 2k+1$, $a^n = a^{2k+1} = a^k a^k a$

This implies a recursive algorithm.

(Repeat Squares)

```
mod-exp(a, n, m):
    if n=0, return 1
    if n is even,
        a_k = mod-exp(a, n/2, m)
        return a_k · a_k mod m
    if n is odd,
        a_k = mod-exp(a, (n-1)/2, m)
        return a_k · a_k · a mod m
```

Ex Calculate $10^{20} \bmod 7$.

$10 \equiv 3 \pmod 7$

$\underbrace{10 \cdot 10 \cdot \ldots \cdot 10}_{20 \text{ times}} \equiv \underbrace{3 \cdot 3 \cdot \ldots \cdot 3}_{20 \text{ times}} \pmod 7$

Now

$3^1 \equiv 3 \pmod 7$

$3^2 \equiv 9 \equiv 2 \pmod 7$

$3^4 \equiv 4 \pmod 7$

$3^8 \equiv 16 \equiv 2 \pmod 7$

$3^{16} \equiv 4 \pmod 7$

Note that

$3^{20} = 3^{16} \cdot 3^4 \equiv 4 \cdot 4 \equiv 2 \pmod 7$

So $10^{20} \bmod 7 = 2$.

Linear Congruences

Def A linear congruence is of the form

$ay \equiv b \pmod{m}$

for $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, and y a variable

If $ax \equiv 1 \pmod{m}$, we say x is the inverse of a modulo m, denoted $a^{-1} \bmod m$.

The inverse of a exists and is unique iff $\gcd(a, m) = 1$.

The inverse can be found using the extended Euclidean algorithm.

Ex Find all solutions, if any exist, to $31x \equiv 33 \pmod{225}$

① Check for solutions ($\gcd(225, 31) = 1$)

Use $\gcd(a,b) = \gcd(b, a \bmod b)$

$\gcd(225, 31) = \gcd(31, 8)$
$= \gcd(8, 7)$
$= \gcd(7, 1)$
$= \gcd(1, 0) = 1$ ✓

a	b	r
$225 = 7 \times 31 + 8$		
$31 = 3 \times 8 + 7$		
$8 = 1 \times 7 + 1$		
$7 = 7 \times 1 + 0$		

② Find the inverse ($31^{-1} \bmod 225$)

Use extended Euclidean algorithm

(i) Reverse equations

$225 = 7 \times 31 + 8$ $\quad 8 = 225 - 7 \times 31$

$31 = 3 \times 8 + 7$ $\quad 7 = 31 - 3 \times 8$

$8 = 1 \times 7 + 1$ $\quad 1 = 8 - 1 \times 7$

(ii) Substitute

$1 = 8 - 1 \times 7$
$= 8 - (31 - 3 \times 8) = 4 \times 8 - 31$
$= 4 \times (225 - 7 \times 31) - 31 = 4 \times 225 - 29 \times 31$

(iii) Extract the inverse

$1 = 4 \times 225 - 29 \times 31$, so $31^{-1} \equiv -29 \pmod{225}$

③ Use inverse to isolate x.

$31x \equiv 33 \pmod{225}$
$31^{-1} \cdot 31x \equiv 31^{-1} \cdot 33 \pmod{225}$
$x \equiv -29 \cdot 33 \pmod{225}$

Solutions are of the form $x = 225k - 29 \cdot 33$ for each $k \in \mathbb{Z}$. Alternatively, $x \equiv 168 \pmod{225}$

Chinese Remainder Theorem

Our goal is to solve systems of linear congruences.

Ex $x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$ (a solution is 23)
$x \equiv 2 \pmod 7$

Which number has remainder
- 2 when divided by 3
- 3 when divided by 5
- 2 when divided by 7?

Note The existence of a solution to a general system of linear congruences is not guaranteed

$x \equiv 1 \pmod 2 \Rightarrow x$ is odd
$x \equiv 0 \pmod 4 \Rightarrow x$ is even
has no solution

Def $a, b \in \mathbb{Z}$ are relatively prime or coprime if $\gcd(a,b) = 1$.

Thm (Chinese Remainder Theorem)
Let $1 < m_1, m_2, \dots, m_n \in \mathbb{Z}^+$ be pairwise coprime. $(\forall i \neq j,\ \gcd(m_i, m_j) = 1)$
Let $a_1, a_2, \dots, a_n \in \mathbb{Z}$. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a solution, and that solution is unique mod $m_1 \cdot m_2 \cdot \dots \cdot m_n$. (for any two solutions x_1 and x_2, $x_1 \equiv x_2 \pmod{m_1 \cdot m_2 \cdot \dots \cdot m_n}$)

Pf (Existence) Let $M_i = \prod_{i \neq j} m_j$

Since the moduli are coprime, $\gcd(M_i, m_i) = 1$.* So $M_i^{-1} \pmod{m_i}$ exists, i.e.
$(\exists y_i \in \mathbb{Z})(M_i y_i \equiv 1 \pmod{m_i})$
Then, since $M_i \equiv 0 \pmod{m_j}$, $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n$ is a solution.
(Uniqueness) In discussion

* You can prove this using the prime factorization version of the gcd.

Using Chinese Remainder Theorem

Ex Consider $n = 3$

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$x \equiv a_3 \pmod{m_3}$$

Since the moduli are coprime, we can use them to split into cases:

$$x = z_1 \cdot m_2 m_3 + z_2 m_1 m_3 + z_3 m_1 m_2$$

Notice that

$$x \equiv z_1 \cdot m_2 \cdot m_3 + z_2 \cdot 0 \cdot m_3 + z_3 \cdot 0 \cdot m_2 \equiv z_1 \cdot m_2 m_3 \pmod{m_1}$$
$$x \equiv z_1 \cdot 0 \cdot m_3 + z_2 \cdot m_1 \cdot m_3 + z_3 \cdot m_1 \cdot 0 \equiv z_2 \cdot m_1 m_3 \pmod{m_2}$$
$$x \equiv z_1 \cdot m_1 \cdot 0 + z_2 \cdot m_1 \cdot 0 + z_3 \cdot m_1 \cdot m_2 \equiv z_3 \cdot m_1 m_2 \pmod{m_3}$$

For x to be a solution,

$$x \equiv z_1 \cdot m_2 m_3 \equiv a_1 \pmod{m_1} \qquad z_1 \equiv a_1 (m_2 m_3)^{-1} \pmod{m_1}$$
$$x \equiv z_2 \cdot m_1 m_3 \equiv a_2 \pmod{m_2} \implies z_2 \equiv a_2 (m_1 m_3)^{-1} \pmod{m_2}$$
$$x \equiv z_3 \cdot m_1 m_2 \equiv a_3 \pmod{m_3} \qquad z_3 \equiv a_3 (m_1 m_2)^{-1} \pmod{m_3}$$

So our solution is

$$x = \left(a_1 [(m_2 m_3)^{-1} \bmod m_1]\right) m_2 m_3 + \left(a_2 [(m_1 m_3)^{-1} \bmod m_2]\right) m_1 m_3 + \left(a_3 [(m_1 m_2)^{-1} \bmod m_3]\right) m_1 m_2$$

Ex Find the smallest positive integer solution to the system

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

① Compute the M_i

$M_1 = 5 \cdot 7 = 35$, $M_2 = 3 \cdot 7 = 21$, $M_3 = 3 \cdot 5 = 15$

② Compute the $y_i = M_i^{-1} \bmod m_i$

$M_1 \equiv 35 \equiv 2 \pmod{3}$. $2 \cdot 2 \equiv 4 \equiv 1 \pmod{3}$, so $y_1 = 2^{-1} \bmod 3 = 2$

$M_2 \equiv 21 \equiv 1 \pmod{5}$. So $y_2 = 1^{-1} \bmod 5 = 1$

$M_3 \equiv 15 \equiv 1 \pmod{7}$. So $y_3 = 1^{-1} \bmod 7 = 1$

③ Construct a solution $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

$x = 2(35)(2) + 3(21)(1) + 2(15)(1) = 140 + 63 + 30 = 233$

All solutions are congruent mod $3 \cdot 5 \cdot 7 = 105$

$233 \equiv 23 \pmod{105}$, so the smallest positive integer solution is 23