Integers modulo n

From last time: For $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we define

$$a \equiv b \bmod n \iff n \mid a-b.$$

- Equality modulo n is an equivalence relation on $\mathbb{Z}$.
- A complete set of distinct equivalence classes is (residue classes)

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}.$$

(May also simply write

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-1\}.)$$

Two binary operations on $\mathbb{Z}/n\mathbb{Z}$:

- Addition: $\forall a, b \in \mathbb{Z}$,

$$\bar{a} + \bar{b} = \overline{a+b}$$

- Multiplication: $\forall a, b \in \mathbb{Z}$,

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

First questions:

- Are these binary operations well_defined?

  i.e. Are the definitions independent of the choices of representatives for the equivalence classes mod n?

  If $\overline{a}_1 = \overline{a}_2$ and $\overline{b}_1 = \overline{b}_2$, do $\overline{a}_1 + \overline{b}_1 = \overline{a}_2 + \overline{b}_2$ and $\overline{a}_1 \cdot \overline{b}_1 = \overline{a}_2 \cdot \overline{b}_2$?

- What additional properties do they have?

  Is $(\mathbb{Z}/n\mathbb{Z}, +)$ a group?

  Is $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ a group?

Addition modulo n $\quad (\forall a,b\in\mathbb{Z},\ \bar{a}+\bar{b}=\overline{a+b})$

- **Well-defined:**

Suppose $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $\bar{a}_1 = \bar{a}_2$, and $\bar{b}_1 = \bar{b}_2$. Then

$$\left.\begin{array}{l} a_1 \equiv a_2 \bmod n \Rightarrow n \mid a_1 - a_2 \Rightarrow a_1 - a_2 = nk \text{ for some } k\in\mathbb{Z}, \\ b_1 \equiv b_2 \bmod n \Rightarrow n \mid b_1 - b_2 \Rightarrow b_1 - b_2 = n\ell \text{ for some } \ell\in\mathbb{Z} \end{array}\right\}$$

$$\Rightarrow a_1 + b_1 = (a_2 + nk) + (b_2 + n\ell) = a_2 + b_2 + n(k+\ell)$$

$$\Rightarrow n \mid (a_1+b_1) - (a_2+b_2) \Rightarrow a_1 + b_1 \equiv a_2 + b_2 \bmod n$$

$$(\overline{a_1+b_1} = \overline{a_2+b_2})$$

- $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group:

Associativity: ✓

$$(\bar{a}+\bar{b})+\bar{c} = \overline{a+b}+\bar{c} = \overline{(a+b)+c} \underset{\text{(assoc. in } (\mathbb{Z},+))}{=} \overline{a+(b+c)} = \bar{a}+\overline{b+c} = \bar{a}+(\bar{b}+\bar{c})$$

Identity $= \bar{0}$ ✓

$$\forall a\in\mathbb{Z},\quad \bar{a}+\bar{0} = \overline{a+0} = \bar{a} = \overline{0+a} = \bar{0}+\bar{a}.$$

Inverse of $\bar{a}$ is $\overline{-a}$ $\quad (=\overline{n-a})$ ✓

$$\bar{a}+\overline{-a} = \overline{a+(-a)} = \bar{0}.$$

Furthermore, $(\mathbb{Z}/n\mathbb{Z}, +)$ is:

- Abelian
- cyclic: $\langle\bar{1}\rangle = \{\underbrace{\bar{1}+\cdots+\bar{1}}_{k\text{-times}} : k\in\mathbb{Z}\} = \{\bar{0},\bar{1},\bar{2},\dots,\overline{n-1}\} = \mathbb{Z}/n\mathbb{Z}$.

$(\mathbb{Z}/n\mathbb{Z} \cong C_n)$

Subtraction modulo n:

$$\bar{a}-\bar{b} = \bar{a}+(-\bar{b}) = \bar{a}+\overline{-b} = \overline{a+(-b)} = \overline{a-b}.$$

Multiplication modulo n $\quad (\forall a,b\in\mathbb{Z},\ \bar{a}\cdot\bar{b}=\overline{ab})$

- Well-defined:

Suppose $a_1,a_2,b_1,b_2\in\mathbb{Z}$, $\bar{a}_1=\bar{a}_2$, and $\bar{b}_1=\bar{b}_2$. Then

$a_1-a_2=nk$ and $b_1-b_2=n\ell$ for some $k,\ell\in\mathbb{Z}$, so

$$a_1b_1=(a_2+nk)(b_2+n\ell)=a_2b_2+a_2n\ell+b_2nk+n^2k\ell$$
$$=a_2b_2+n(a_2\ell+b_2k+nk\ell)$$

$$\Rightarrow n\mid a_1b_1-a_2b_2 \Rightarrow \overline{a_1b_1}=\overline{a_2b_2}.$$

Notational convention: When working in $\mathbb{Z}/n\mathbb{Z}$, $a=\bar{a}$.

- Is $(\mathbb{Z}/n\mathbb{Z},\cdot)$ a group? (<u>not if $n\geq 2$</u>)

Associativity ✓

Identity $=1$ ✓

$a1=1a=a$.

Inverses: ✗

$\forall a\in\mathbb{Z}/n\mathbb{Z}$, $0\cdot a=0\neq 1$ (if $n\geq 2$)

To fix this, define

$$(\mathbb{Z}/n\mathbb{Z})^\times=\{a\in\mathbb{Z}/n\mathbb{Z} : \exists b\in\mathbb{Z}/n\mathbb{Z} \text{ s.t. } ab=1 \bmod n\}$$

(<u>primitive residue classes</u> mod n)

Things to note:

- If $a_1, a_2 \in (\mathbb{Z}/n\mathbb{Z})^\times$ then $\exists\, b_1, b_2 \in \mathbb{Z}$ s.t. $a_1 b_1 = 1 \bmod n$ and $a_2 b_2 = 1 \bmod n$.

  Then $(a_1 a_2)(b_1 b_2) = (a_1 b_1)(a_2 b_2) = 1 \cdot 1 = 1 \bmod n$

  $$\Rightarrow a_1 a_2 \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

  So multiplication, restricted to $(\mathbb{Z}/n\mathbb{Z})^\times$, is a binary operation.

- $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ is an Abelian group:

  Associativity ✓ Commutativity ✓

  Identity ✓

  $1 \cdot 1 = 1 \bmod n \Rightarrow 1 \in (\mathbb{Z}/n\mathbb{Z})^\times$

  Inverses ✓

  If $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ then $\exists\, b \in \mathbb{Z}/n\mathbb{Z}$ s.t. $ab = 1 \bmod n$.

  By symmetry of the definition, $b \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Notational conventions:

$\mathbb{Z}/n\mathbb{Z} = (\mathbb{Z}/n\mathbb{Z}, +)$ (additive group of integers modulo n)

$(\mathbb{Z}/n\mathbb{Z})^\times = ((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ (multiplicative group of integers modulo n)

Exs: 1) $n=8$, $\mathbb{Z}/8\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$

Scratch work:

- If $2b \equiv 1 \mod 8$ then $2b-1 = 8k$

$$\Rightarrow 1 = 2b - 8k = 2(b-4k) \Rightarrow 2 \mid 1 \quad \times$$

Therefore $2 \notin (\mathbb{Z}/8\mathbb{Z})^\times$.

Similarly, $0, 4, 6 \notin (\mathbb{Z}/8\mathbb{Z})^\times$.

- $\underline{1} \cdot 1 = \underline{3} \cdot 3 = \underline{5} \cdot 5 = \underline{7} \cdot 7 = 1 \mod 8 \Rightarrow 1, 3, 5, 7 \in (\mathbb{Z}/8\mathbb{Z})^\times$

Group structure:

$|(\mathbb{Z}/8\mathbb{Z})^\times| = 4 \Rightarrow (\mathbb{Z}/8\mathbb{Z})^\times \cong C_4$ or V_4

All elements of the group square to 1, so it is not cyclic. Therefore $(\mathbb{Z}/8\mathbb{Z})^\times \cong V_4$.

2) $n=9$, $\mathbb{Z}/9\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$$(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$$

Scratch work:

- Suppose $d = \gcd(a, 9) > 1$. If $ab \equiv 1 \mod 9$ then $ab - 1 = 9k \Rightarrow 1 = ab - 9k = d\left(\left(\frac{a}{d}\right)b - \left(\frac{9}{d}\right)k\right)$ (integers)

  $\Rightarrow d \mid 1$ (contradiction).

  Therefore $0, 3, 6 \notin (\mathbb{Z}/9\mathbb{Z})^\times$.

- $1 \cdot 1 = 2 \cdot 5 = 4 \cdot 7 = 8 \cdot 8 = 1 \mod n$

  $\Rightarrow 1, 2, 4, 5, 7, 8 \in (\mathbb{Z}/9\mathbb{Z})^\times$.

Group structure:

$|(\mathbb{Z}/9\mathbb{Z})^\times| = 6 \Rightarrow (\mathbb{Z}/9\mathbb{Z})^\times \cong C_6$ or D_6.

Since $(\mathbb{Z}/9\mathbb{Z})^\times$ is Abelian, $(\mathbb{Z}/9\mathbb{Z})^\times \cong C_6$.

Find a generator: $(\mathbb{Z}/9\mathbb{Z})^\times = \langle 2 \rangle$

$1^1 = 1$ x

$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 7$, $2^5 = 5$, $2^6 = 1$

$$\overset{\shortparallel}{-1} \overset{\times 2}{\longmapsto} \overset{\shortparallel}{-2} \overset{\times 2}{\longmapsto} \overset{\shortparallel}{-4} \overset{\times 2}{\longmapsto} \overset{\shortparallel}{-8}$$

More about $(\mathbb{Z}/n\mathbb{Z})^\times$: $(n \geq 2)$

- $(\mathbb{Z}/n\mathbb{Z})^\times = \{1 \leq a \leq n-1 : \gcd(a,n)=1\}$

Pf: Let $0 \leq a \leq n-1$, write $d=(a,n)$.

Suppose $d>1$. If $\exists b \in \mathbb{Z}$ s.t. $ab \equiv 1 \mod n$

then $n \mid ab-1 \Rightarrow ab-1=nk$ for some $k \in \mathbb{Z}$.

Then $1 = ab-nk = d\left(\left(\frac{a}{d}\right)b - \left(\frac{n}{d}\right)k\right)$

$\Rightarrow d \mid 1$ (contradiction).

Therefore $a \notin (\mathbb{Z}/n\mathbb{Z})^\times$.

Suppose $d=1$. By Bézout's lemma,

$\exists\, b,k \in \mathbb{Z}$ s.t. $ab+nk=d=1$.

Then $n \mid ab-1 \Rightarrow ab \equiv 1 \mod n$

$\Rightarrow a \in (\mathbb{Z}/n\mathbb{Z})^\times$. ∎

- Fast algorithm for computing $a^{-1} \mod n$,

when $(a,n)=1$: (Reverse Euclidean algorithm)

Ex: Let $n=101$ (prime), $a=45$.

$101 = 2\cdot 45 + 11$ ↓ | ↑ $1 = 45 - 4\cdot(101 - 2\cdot 45) = 9\cdot 45 - 4\cdot 101$

$45 = 4\cdot 11 + 1$ | $1 = 45 - 4\cdot 11$

$11 = 11\cdot 1$

So, $1 \equiv 9\cdot 45 \mod 101 \Rightarrow 45^{-1} \equiv 9 \mod 101$.

- Division modulo n: Suppose $a, b \in \mathbb{Z}$. Is there a solution $x \in \mathbb{Z}$ to the equation $ax = b \mod n$?
  - If $(a,n) = 1$ then take $x = a^{-1} b \mod n$, and $ax = a(a^{-1}b) = (aa^{-1})b = b \mod n$.
  - If $d = (a,n) > 1$:

    $\exists x \in \mathbb{Z}$ s.t. $ax = b \mod n$

    $\Longleftrightarrow \exists x \in \mathbb{Z}\ k \in \mathbb{Z}$ s.t. $ax = b + nk$

    $\Longleftrightarrow \exists x, k \in \mathbb{Z}$ s.t. $ax - nk = b$

    $\Longleftrightarrow d \mid b$.

    Bezout's lemma

    If $d \mid b$ then any solution to $ax = b$ must satisfy $\left(\frac{a}{d}\right)x - \left(\frac{n}{d}\right)k = \frac{b}{d}$, and since $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, we have that $x = \left(\frac{a}{d}\right)^{-1} \cdot \frac{b}{d} \mod \left(\frac{n}{d}\right)$.

Thm: If $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ then the equation $ax \equiv b \bmod n$ has a solution $x \in \mathbb{Z}$ if and only if $d = (a,n) \mid b$. Furthermore, if $d \mid b$ and $x_0 \in \mathbb{Z}$ is any integer satisfying $x_0 \equiv \left(\frac{a}{d}\right)^{-1}\left(\frac{b}{d}\right) \bmod \left(\frac{n}{d}\right)$, then the set of all solutions is

$$\left\{ x_0 + \left(\frac{n}{d}\right)k : k \in \mathbb{Z} \right\}.$$

Ex: Determine the set of all solutions $x \in \mathbb{Z}$ to the equation $115x \equiv 69 \bmod 667$.

Step 1: Compute $d = (115, 667)$:

$667 = 5 \cdot 115 + 92$

$115 = 1 \cdot 92 + 23$

$92 = 4 \cdot 23 \implies d = 23.$

Step 2: Since $23 \mid 69$, the equation has solutions. Now

$$\frac{115}{d} = 5, \quad \frac{69}{d} = 3, \quad \frac{667}{d} = 29,$$

so we want to compute

$$x_0 \equiv 5^{-1} \cdot 3 \bmod 29.$$

(pretend it's not obvious)

To compute $5^{-1} \bmod 29$, go back to the Euc. alg. calc. and divide by d:

$$\begin{aligned} 667 &= 5 \cdot 115 + 92 & \qquad & & 29 &= 5 \cdot 5 + 3 \\ 115 &= 1 \cdot 92 + 23 & \longmapsto & & 5 &= 1 \cdot 3 + 1 \\ 92 &= 4 \cdot 23 & & & 3 &= 4 \cdot 1 \end{aligned}$$

Then use the reverse Euc. alg:

$$\begin{aligned} 29 &= 5 \cdot 5 + 3 & \qquad 1 &= 5 - 1 \cdot (29 - 5 \cdot 5) = 6 \cdot 5 - 1 \cdot 29 \\ 5 &= 1 \cdot 3 + 1 & 1 &= 5 - 1 \cdot 3 \\ 3 &= 4 \cdot 1 \end{aligned}$$

This gives $6 \cdot 5 = 1 \bmod 29 \Rightarrow 5^{-1} = 6 \bmod 29$.

Then $x_0 = 5^{-1} \cdot 3 = 18 \bmod 29$, so the set of all solutions is

$$\{ 18 + k \cdot 29 : k \in \mathbb{Z} \}$$