# Multiplicative inverses in $\mathbb{Z}/n\mathbb{Z}$

**Def'n**: Fix $n \in \mathbb{N}$, $a \in \mathbb{Z}$. We say $a$ has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ iff $\exists b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$

If such a $b$ exists, we sometimes write $b = a^{-1}$.

↗ not unique, but unique up to $\equiv$ class.

**ex**: 3 has a multiplicative inverse in $\mathbb{Z}/7\mathbb{Z}$, since $3 \cdot 5 = 15 \equiv 1 \pmod{7}$

**Prop'n** Fix $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Then $a$ has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ iff $\gcd(a, n) = 1$.

Pf: ($\Rightarrow$) assume $\exists b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$

- then $n \mid 1 - ab$
- i.e. $\exists k \in \mathbb{Z}$ $kn = 1 - ab$

so $kn + ab = 1$.

- since 1 is a linear combo of a, n
we have $\gcd(a,n) \leq 1$
- hence $\gcd(a,n) = 1$ ✓

($\Leftarrow$) Now suppose $\gcd(a,n) = 1$.
Then, by Bezout, $\exists b, k \in \mathbb{Z}$ s.t.

$$ab + nk = 1$$

So $nk = 1 - ab$

$\Rightarrow n \mid 1-ab \Rightarrow ab \equiv 1 \pmod{n}$

Ex's: ① $5x \equiv 1 \pmod{21}$
does have a solution, since
$\gcd(5,21) = 1$.

indeed $x = 17$ works since

$$5 \cdot 17 = 85 = \underbrace{84}_{21 \cdot 4} + 1 \equiv 1 \pmod{21}$$

↪ only $x \in \mathbb{Z}$ congruent to 17 mod 21 also work, e.g. $x = -4, 38, \ldots$ work fec.

check: $5 \cdot (-4) = -20 = 21(-1) + 1$
$\equiv 1 \pmod{21}$

- i.e. set of sol'ns is exactly $[17]_{21}$
- might write $[5]_{21} \cdot [17]_{21}$ " = " $[1]_{21}$ in the sense that:

$$\forall a \in [5]_{21} \quad \forall b \in [17]_2$$
we have $a \cdot b \equiv 1 \pmod{21}$
i.e. $ab \in [1]_{21}$.

(2) The congruence $6x \equiv 1 \pmod{21}$ has no soln: such an $x$ would be a mult. inv. for 6 in $\mathbb{Z}/21\mathbb{Z}$.
but $\gcd(6,21) = 3 \neq 1$, so no such inverse exists.

(3) Find all sol'ns $x \in \mathbb{Z}$ to:

$$4x \equiv 5 \pmod{7}.$$

Soln since 7 is prime and $7 \nmid 4$ we have $\gcd(4,7) = 1$. Hence 4 has a mult. inverse in $\mathbb{Z}/7\mathbb{Z}$.
indeed 2 works: $4 \cdot 2 = 8 \equiv 1 \pmod{7}$.

Idea: instead of "dividing both sides" of $4x \equiv 5 \pmod 7$ by 4, can multiply by 2:

$$\begin{aligned} & 4x \equiv 5 \pmod 7 \\ \Leftrightarrow\ & 2 \cdot 4x \equiv 2 \cdot 5 \pmod 7 \\ \Leftrightarrow\ & 8x \equiv 10 \pmod 7 \\ \Leftrightarrow\ & x \equiv 3 \pmod 7 \end{aligned}$$

Hence $[3]_7$ is set of solutions!

Prop'n: For a given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, there is a sol'n to $ax \equiv b \pmod n$ iff $\gcd(a,n) \mid b$.

Pf: Let $d = \gcd(a,n)$

($\Rightarrow$) Assume there is a sol'n $x = \ell$ to $ax \equiv b \pmod n$, i.e. $a\ell \equiv b \pmod n$

then $n \mid b - a\ell$

$\Rightarrow \exists k \in \mathbb{Z}$ $b - a\ell = nk$

$\Rightarrow b = a\ell + nk$

$\Rightarrow$ $b$ is a linear combo of $a, n$

$\Rightarrow$ $\gcd(a,n) \mid b$ (i.e. $d \mid b$)

↑ by quiz 9 problem!

($\Leftarrow$) Now assume $d \mid b$, i.e. $\exists \ell$ s.t. $b = \ell d$.

- By Bezout $\exists k, k' \in \mathbb{Z}$ s.t.

$$ak + nk' = d$$

$\Rightarrow ak\ell + nk'\ell = d\ell = b$

$\Rightarrow n(k'\ell) = b - a(k\ell)$

$\Rightarrow a(k\ell) \equiv b \pmod{n}$

$\Rightarrow x = k\ell$ is a soln to $ax \equiv b \pmod{n}$ ✓

---

Ex's ① There is a soln to

$6x \equiv 4 \pmod{8}$

why: $\gcd(6,8) = 2$ and $2 \mid 4$ ✓

indeed $x = 2$ works:

$6 \cdot 2 = 12 \equiv 4 \pmod{8}$ ✓

② There is no soln to

$4x \equiv 3 \pmod{8}$

why: $\gcd(4,8) = 4 \nmid 3$ ✓

# Euclidean Algorithm:

Q: how to find $\gcd(a,b)$ for (potentially large) $a,b \in \mathbb{Z}$

A: Euclidean algorithm!

↳ really just a combination of division algorithm + following crucial lemma:

**Lemma**: Fix $a, b, q, r \in \mathbb{Z}$.

If $a = bq + r$

Then $\gcd(a,b) = \gcd(b,r)$

Pf: Let $d = \gcd(a,b)$
$d' = \gcd(b,r)$

WTS: $d = d'$

observe: since $a = bq + r$ and $d' \mid b$ and $d' \mid r$, we have $d' \mid a$.

$\Rightarrow$ hence $d'$ is a common divisor of $a, b$

$\Rightarrow d' \leq d$.

QTOH: - By Bezout, $\exists m, n \in \mathbb{Z}$ s.t.

$d' = rm + bn$

- but $r = a - bq$ so:

$d' = (a - bq)m + bn$

$\Rightarrow d' = am + b(n - qm)$

- so $d'$ is a linear combo of $a, b$.

$\Rightarrow d' \geq d$, by Bezout

$\Rightarrow d' = d$ ✓

---

This Lemma allows us to find $\gcd(a,b)$ by repeatedly "reducing by remainders"

**Theorem:** (Euclidean algorithm)

Fix $a, b \in \mathbb{N}$ with $a \geq b$.

Using the division algorithm repeatedly define a decreasing (hence finite) sequence $r_j$ as follows:

$r_0 = a \qquad r_1 = b$

$r_j = r_{j+1} q_{j+1} + r_{j+2}$ (i.e. $r_{j+2} = r_j - r_{j+1} q_{j+1}$)

where $0 \le r_{j+2} < r_{j+1}$, and $q_{j+1}$ is the unique quotient making the above eq'n true (by div. alg).

Since $r_j \ge 0$ for every $j$ and the sequence is decreasing, there is some least $N \in \mathbb{N}$ s.t.

$$r_N = 0.$$

Define $r_N$ to be the <u>last term</u>

<u>Then</u> $\gcd(a,b) = r_{N-1}$.

<u>Pf (sketch)</u>: Consider the sequence of remainders as defined:

$$r_0 \ge r_1 > r_2 > \cdots > r_{N-1} > r_N$$
$$\| \qquad \| \qquad\qquad\qquad\qquad\quad \|$$
$$a \qquad b \qquad\qquad\qquad\qquad\quad 0$$

Observe: Since $r_j = r_{j+1} q_{j+1} + r_{j+2}$ $\forall j \leq N-2$, we have by prev. lemma:

$$\gcd(r_j, r_{j+1}) = \gcd(r_{j+1}, r_{j+2}) \quad \forall j \leq N-2$$

Hence $\gcd(a,b) = \gcd(r_0, r_1)$

$= \gcd(r_1, r_2)$ (lemma)

$= \gcd(r_2, r_3)$ (lemma)

$= \gcd(r_{N-1}, r_N)$ (lemma)

$= \gcd(r_{N-1}, 0) = r_{N-1}$ ✓

---

Ex's: ① Find gcd (68, 12).

Sol'n: $a = 68$, $b = 12$

$$\overset{r_0}{68} = \overset{r_1}{12} \cdot 5 + \overset{r_2}{8}$$

$$\overset{r_1}{12} = \overset{r_2}{8} \cdot 1 + \overset{r_3}{4}$$

$$\overset{r_2}{8} = \overset{r_3}{4} \cdot 2 + \overset{r_4}{0}$$

Hence $r_4 = 0$ is the last term

$\Rightarrow r_3 = 4$ is $\gcd(68, 12)$ ✓

(Why: by Lemma:

$$\gcd(68,12) = \gcd(12,8)$$
$$= \gcd(8,4)$$
$$= \gcd(4,0) = 4.)$$

② Find $m,n \in \mathbb{Z}$ s.t.

$$68m + 12n = 4$$

Soln: Bezout says: such $m,n$ exist. Euclid gives us a way to find them! By "reversing" above eq'ns:

$$4 = 12 - 8 \cdot 1$$
$$= 12 - (68 - 12 \cdot 5) \cdot 1$$
$$= 12 - 68 \cdot 1 + 12 \cdot 5$$
$$= 12 \cdot (6) + 68(-1)$$

so $m = -1$ $n = 6$ works!

↳ this method of back substitution to find $m,n$ is sometimes called the extended E.A.

Find $k, \ell \in \mathbb{Z}$ s.t.

$$64k + 111\ell = 1$$

Soln: For this to be possible, need $\gcd(64, 111) = 1$. Let's do EA:

$$111 = 64 \cdot 1 + 47$$
$$64 = 47 \cdot 1 + 17$$
$$47 = 17 \cdot 2 + 13$$
$$17 = 13 \cdot 1 + 4$$
$$* \quad 13 = 4 \cdot 3 + 1 \quad \leftarrow \gcd(111, 64) = 1$$
$$4 = 1 \cdot 4 + 0$$

now we go backwards from *:

$$1 = 13 - 4 \cdot 3 \qquad (\text{but: } 4 = 17 - 13 \cdot 1)$$
$$1 = 13 - (17 - 13 \cdot 1) \cdot 3$$
$$= 13 - 17 \cdot 3 + 13 \cdot 3$$
$$= 13 \cdot 4 - 17 \cdot 3$$
$$= 17(-3) + 13(4) \qquad (\text{but: } 13 = 47 - 17 \cdot 2)$$
$$= 17(-3) + (47 - 17 \cdot 2)(4)$$
$$= 47(4) + 17(-3) - 17(8)$$
$$= 47(4) + 17(-11) \qquad (\text{but } 17 = 64 \cdot (-47))$$

(31)

$= 47(4) + (64\cdot1 - 47)(-11)$

$= 47(4) + 64(-11) + 47(11)$

$= 64(-11) + 47(15)$ (but: $47 = 111 - 64\cdot1$)

$= 64(-11) + (111 - 64\cdot1)(15)$

$= 64(-11) + 111(15) + 64(-15)$

$= 111(15) + 64(-26)$

So $k = -26$ $\ell = 15$ works ✓