

Proposition 46 Let m be a positive integer. For all natural numbers k and l ,

$$k \equiv l \pmod{m} \iff \text{rem}(k, m) = \text{rem}(l, m) .$$

PROOF: Have $k = q \cdot m + r$, $l = q' \cdot m + r'$
 where q, q' are ints. wos $0 \leq r < m$ & $0 \leq r' < m$.

(\Rightarrow) Assume $k \equiv l \pmod{m}$, i.e. $k - l = i \cdot m = (q - q') \cdot m + (r - r')$

Wlog we are assuming $r \geq r'$. $\therefore 0 \leq r - r' < m$.

Now, $0 = (q - q' - i) \cdot m + (r - r')$. By Lemma 43, $r = r'$.

(\Leftarrow) Assume $r = r'$. Then,

$$k = q \cdot m + r \quad \& \quad l = q' \cdot m + r$$

$$\therefore k - l = (q - q') \cdot m. \quad \therefore k \equiv l \pmod{m}.$$

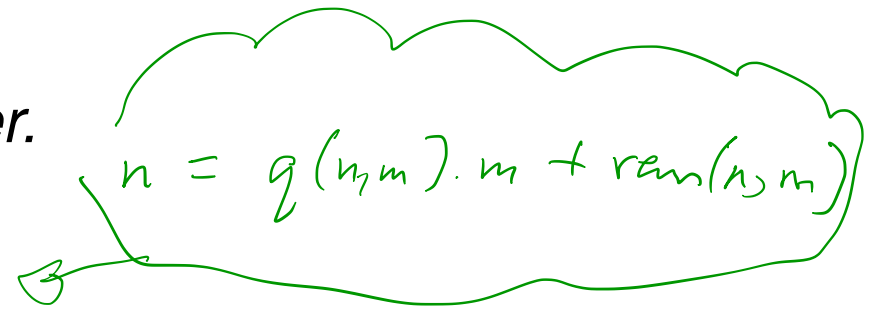


Lemma 9.

Corollary 47 Let m be a positive integer.

1. For every natural number n ,

$$n \equiv \text{rem}(n, m) \pmod{m} .$$


$$n = q(n, m) \cdot m + \text{rem}(n, m)$$

PROOF:

Corollary 47 Let m be a positive integer.

1. For every natural number n ,

$$n \equiv \text{rem}(n, m) \pmod{m}$$

2. For every integer k there exists a unique integer $[k]_m$ such that

$$0 \leq [k]_m < m \text{ and } k \equiv [k]_m \pmod{m}.$$

PROOF: Assume $k > 0$. Then, $k \equiv \text{rem}(k, m) \pmod{m}$.

$$\therefore -k \equiv -\text{rem}(k, m) \text{ with } 0 \leq \text{rem}(k, m) < m.$$

$$[-k]_m \stackrel{\text{def}}{=} \begin{cases} m - \text{rem}(k, m) & \text{if } \text{rem}(k, m) \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

q, q' are integers and

Uniqueness: Assume $q \cdot m + r = q' \cdot m + r'$ where $0 \leq r, r' < m$ & wlog. $r \geq r'$. Then $0 = (q - q') \cdot m + (r - r')$ where $0 \leq r - r' < m$. So, by Lemma 43, $r = r'$. This ensures the uniqueness of $[k]_m$. \square

$$\begin{aligned} k - r &= q \cdot m \\ -k - (-r) &= -q \cdot m \\ \therefore -k &\equiv -r \end{aligned}$$

Modular arithmetic

For every positive integer m , the integers modulo m are:

$$\mathbb{Z}_m : 0, 1, \dots, m-1.$$

with arithmetic operations of addition $+_m$ and multiplication \cdot_m defined as follows

$$k +_m l = [k + l]_m = \text{rem}(k + l, m),$$

$$k \cdot_m l = [k \cdot l]_m = \text{rem}(k \cdot l, m)$$

for all $0 \leq k, l < m$.

$$-k = [m - k]_m$$

$$2 \cdot 1 = 2 \cdot 3$$

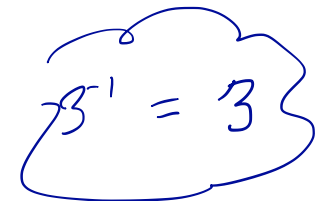
$$2^{-1} \cdot 2 \cdot 1 = 2^{-1} \cdot 2 \cdot 3$$

$$\Rightarrow 1 = 3 \quad \text{✗}$$

Example 49 *The addition and multiplication tables for \mathbb{Z}_4 are:*

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

\cdot_4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1



$$3^{-1} = 3$$

Note that the addition table has a cyclic pattern, while there is no obvious pattern in the multiplication table.

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

	<i>additive inverse</i>		<i>multiplicative inverse</i>
0	0	0	—
1	3	1	1
2	2	2	—
3	1	3	3

Interestingly, we have a non-trivial multiplicative inverse; namely, 3.

Example 50 *The addition and multiplication tables for \mathbb{Z}_5 are:*

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

\cdot_5	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Again, the addition table has a cyclic pattern, while this time the multiplication table restricted to non-zero elements has a permutation pattern.

FLT: (2) $z^{(p-1)} \equiv 1 \pmod{p}$ p prime
 $z \equiv 0 \pmod{p}$

inverse of z $z \cdot z^{(p-2)} \equiv 1$

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

	<i>additive inverse</i>		<i>multiplicative inverse</i>
0	0	0	—
1	4	1	1
2	3	2	3
3	2	3	2
4	1	4	4

Surprisingly, every non-zero element has a multiplicative inverse.

Proposition 51 For all natural numbers $m > 1$, the modular-arithmetic structure

$$(\mathbb{Z}_m, 0, +_m, 1, \cdot_m)$$

is a commutative ring.

NB Quite surprisingly, modular-arithmetic number systems have further mathematical structure in the form of multiplicative inverses :

When m is a prime p the multiplicative inverse of $i \in \mathbb{Z}_p$ when $i \neq 0$ is $[i^{(p-2)}]_p$. \mathbb{Z}_p is a field.