

Practice questions:

1. Draw out the multiplication table for integers mod 6.

| \cdot | [0] | [1] | [2] | [3] | [4] | [5] |
|---------|-----|-----|-----|-----|-----|-----|
| [0] | [0] | [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] | [3] | [4] | [5] |
| [2] | [0] | [2] | [4] | [0] | [2] | [4] |
| [3] | [0] | [3] | [0] | [3] | [0] | [3] |
| [4] | [0] | [4] | [2] | [0] | [4] | [2] |
| [5] | [0] | [5] | [4] | [3] | [2] | [1] |

2. Let p be a prime number and assume $a, b \in \mathbb{Z}$. Prove that if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. Let p be a prime number, $a, b \in \mathbb{Z}$, and assume $p \mid ab$. We proceed with proof by cases.

- If $p \mid a$, then we are done.
- If $p \nmid a$, since p is a prime, it follows that $\gcd(a, p) = 1$. By Bézout's identity, we know there exists $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Multiplying both sides by b gives $abx + bpy = b$ and by assumption, we know $ab = pk$ for some $k \in \mathbb{Z}$ so $p(kx + by) = b$. Since $kx + by \in \mathbb{Z}$, it follows that $p \mid b$ as required.

This proves both cases and hence the result follows. \square

3. Prove that for all $n \in \mathbb{Z}$, n and $n + 1$ are coprime.

Proof. Let $n \in \mathbb{Z}$ and assume $p \mid n$ and $p \mid n + 1$ for some $p \in \mathbb{Z}$. Then, $n = pk$ and $n + 1 = p\ell$ for some $k, \ell \in \mathbb{Z}$. Hence, $1 = n + 1 - n = p(\ell + k)$ so $p \mid 1$. It follows that $p = \pm 1$ so the only natural number that can divide n and $n + 1$ is 1, n and $n + 1$ are coprime as required. \square

4. Let $m, n \in \mathbb{Z}$, and let r be the remainder of m under division by n . Prove that $\gcd(m, n) = \gcd(n, r)$.

Proof. Let $m, n \in \mathbb{Z}$, and let r be the remainder of m under division by n . We show that m and n have the same set of common divisors as n and r . Suppose $d \mid m$ and $d \mid n$ for some $d \in \mathbb{Z}$. Notice $m \equiv 0 \pmod{d}$ and $n \equiv 0 \pmod{d}$, and since $m = nk + r$ for some $k \in \mathbb{Z}$,

$$0 \equiv m \equiv nk + r \equiv r \pmod{d}$$

So $d \mid r$ and so we have $d \mid m$, $d \mid n$, and $d \mid r$. Now suppose $e \mid n$ and $e \mid r$ for some $e \in \mathbb{Z}$. Then, $m = nk + r$, so obviously $e \mid m$. It follows that $e \mid m$, $e \mid n$ and $e \mid r$ and thus any common divisor of m and n is also a common divisor of n and r . It follows that m, n and n, r have the same set of common divisors so they must also have the same greatest common divisors. Hence, $\gcd(m, n) = \gcd(n, r)$ as required. \square

5. Prove that for all odd $a, b, c \in \mathbb{Z}$, there exists no rational solutions to $ax^2 + bx + c = 0$. (Hint: Proof by contradiction under mod 2)

Proof. Let $a, b, c \in \mathbb{Z}$ and assume there exists a rational x such that $ax^2 + bx + c = 0$. Then, $x = \frac{p}{q}$ for some coprime $p, q \in \mathbb{Z}$ where $q \neq 0$. Substituting x for $\frac{p}{q}$ and simplifying the equation gives $ap^2 + bpq + cq^2 = 0$. Consider this equation under mod 2.

- p, q cannot both be even by coprimeness.
- If p is even and q is odd, then

$$\begin{aligned} ap^2 + bpq + cq^2 &\equiv 0 \pmod{2} \\ 0 + 0 + 1 &\equiv 0 \pmod{2} \end{aligned}$$

And this is a contradiction.

- If q is even and p is odd, then

$$\begin{aligned} ap^2 + bpq + cq^2 &\equiv 0 \pmod{2} \\ 1 + 0 + 0 &\equiv 0 \pmod{2} \end{aligned}$$

And this is a contradiction.

- If p, q are both odd,

$$\begin{aligned} ap^2 + bpq + cq^2 &\equiv 0 \pmod{2} \\ 1 + 1 + 1 &\equiv 0 \pmod{2} \\ 1 &\equiv 0 \pmod{2} \end{aligned}$$

And this is a contradiction.

All cases yield contradictions and hence the result follows. \square

6. Let \mathbb{Z}_p be the set $\{[0], [1], [2], [3], \dots, [p-1]\}$ with the usual modular arithmetic. Prove that if p is prime, then for all $[a] \neq [0] \in \mathbb{Z}_p$, there exists $[a]^{-1}$ such that $[a] \cdot [a]^{-1} = [1]$ (Note that \cdot is multiplication in modular arithmetic; Hint: Bézout's identity)

Proof. Let p be prime $[a] \neq [0] \in \mathbb{Z}_p$. Then, $[a] = [m]$ for some $1 < m < p$ and since p is prime, $\gcd(m, p) = 1$. By Bézout's identity, we know there exists $x, y \in \mathbb{Z}$ such that $mx + py = 1$ so $mx = 1 - py$ and $mx \equiv 1 \pmod{p}$. It follows that this x is an x such that $mx \equiv 1 \pmod{p}$ and by the rules of modular arithmetic, we know $[a][x] = [m][x] = [mx] = [1]$ so we have found an $[a]^{-1}$ as required. \square

7. Let \mathbb{Z}_n be the set $\{[0], [1], [2], [3], \dots, [n-1]\}$ under addition mod n and suppose $M \subseteq \mathbb{Z}_n$ is a non-empty subset such that for all $[a], [b] \in M$, $[a] + [n-b] \in M$ (Note that $+$ denotes addition mod n).

- (a) Prove that $[0] \in M$.

Proof. Let everything be as stated. Since M is non-empty, we know $[a] \in M$, so $[a] + [n - a] = [a + n - a] = [n] = [0] \in M$ as required. \square

- (b) Prove that for all $[a] \in M$, $[n - a] \in M$.

Proof. Let everything be as stated. From Q7a, we know $[0] \in M$. Let $[a] \in M$. Then, from the definition, $[0] + [n - a] = [n - a] \in M$ and hence the result follows. \square

- (c) Prove that $|M|$ divides n . (Hint: consider equivalence classes under the relation where for all $[a], [b] \in \mathbb{Z}_n$, $[a] \sim [b]$ if and only if $[a] + [n - b] \in M$)

Proof. Let everything be as stated. For all $[c] \notin M$ but $[c] \in \mathbb{Z}_n$, construct a set $[c] + M$ where for all $[x] \in [c] + M$, $[x] = [c] + [a]$ for some $[a] \in M$. Notice by construction, $[c] + M$ has $|M|$ elements and every element in \mathbb{Z}_n lies in some $[c] + M$. Notice if $[y] \in [c] + M$ and $[y] \in [d] + M$ for some $[c], [d] \in \mathbb{Z}_n$, then $[y] = [c] + [a_0] = [d] + [a_1]$ where $[a_0], [a_1] \in M$ so $[c] = [d] + [a_0] + [a_1] = [d] + [a_0 + a_1]$ so $[c] \in [d] + M$ and the same argument could be applied backwards, yielding $[c] + M = [d] + M$. It follows that $[c] + M, [d] + M$ are disjoint or the same for all $[c], [d] \in \mathbb{Z}_n$. Hence, we know that \mathbb{Z}_n is a disjoint union of sets of the form $[c] + M$, all of which have $|M|$ elements. It follows that the number of elements in \mathbb{Z}_n , which is n , is equal to $\ell|M|$ for some $\ell \in \mathbb{Z}$ so $|M|$ divides n as required. \square

8. We will prove Fermat's little theorem, i.e. for all $a, p \in \mathbb{Z}$ such that p is prime and $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$. Let \mathbb{Z}_p be the set $\{[0], [1], [2], [3], \dots, [p-1]\}$ with the usual modular arithmetic. By Q6, we know every element in the set $\mathbb{Z}_p \setminus \{[0]\}$ is invertible under multiplication.

- (a) Assume k is the smallest natural number such that $a^k \equiv 1 \pmod{p}$ for some $a \in \mathbb{Z}$ such that $1 \leq a \leq p-1$. Let $S \subseteq \mathbb{Z}_p \setminus \{[0]\}$ be a non-empty subset such that $S = \{[1], [a], [a]^2, \dots, [a]^{k-1}\}$. Similarly to Q7c, prove that $|S| = k$ divides $|\mathbb{Z}_p \setminus \{[0]\}| = p-1$.

Proof. Let everything be as stated and for all $[c] \in \mathbb{Z}_p \setminus \{[0]\}$, construct a set $[c]S$ where its elements are defined as $[c] \cdot [a]$ for every $[a] \in S$. It follows that $[c]S$ has $|S| = k$ elements. Notice if $[x] \in [c]S$ and $[x] \in [d]S$, $[x] = [c][a_0] = [d][a_1]$ where $[a_0], [a_1] \in S$ so $[c] = [d][a_1][a_0] = [d][a_1 \cdot a_0]$ and thus $[c] \in [d]S$ and the same argument could be applied backwards, yielding $[c]S = [d]S$. It follows that that $[c]S, [d]S$ are disjoint or the same for all $[c], [d] \in \mathbb{Z}_p \setminus \{[0]\}$. It follows that the number of elements in $\mathbb{Z}_p \setminus \{[0]\}$, which is $p-1$, is equal to $m|S| = km$ for some $m \in \mathbb{Z}$ so $k \mid p-1$ as required. \square

- (b) Hence, prove that $a^{p-1} \equiv 1 \pmod{p}$.

Proof. We know from Q8a that $a^{p-1} = a^{km}$ where k is the smallest natural number such that $a^k \equiv 1 \pmod{p}$ and $m \in \mathbb{Z}$. It follows that $a^{p-1} \equiv a^{km} \equiv 1^m \equiv 1 \pmod{p}$ so $a^{p-1} \equiv 1 \pmod{p}$ as required. \square