Quick problems to start with

1. (i) What is $33 \cdot 71$ modulo 31? (Here, you should find an integer $a \in \{0, \dots, 30\}$ so that $33 \cdot 71 \equiv a \pmod{31}$).
   (ii) What is $37 \cdot 51$ modulo 18?
   (iii) What is $19 \cdot 21$ modulo 41?

2. (i) What is 3^{20} modulo 11? (Here, you should find an integer $a \in \{0, \dots, 10\}$ so that $3^{20} \equiv a \pmod{11}$).
   (ii) What is 2^{10} modulo 100?
   (iii) What is 3^{10} moduloe 7?

3. In these cases, being prime is the same as being *irreducible*,i.e. if p is a product of a and b, then either a or b is invertible.
   (i) Is 91 prime?
   (ii) Is 127 prime?
   (iii) Is 221 prime?

4. Find p and r in $\mathbb{Z}$ (or $\mathbb{Q}[X]$), so that
   (i) $169 = 91p + r$ with $0 \leq r < 91$,
   (ii) $4199 = 1001p + r$ with $0 \leq r < 1001$

5. You may use the Euclidean Algorithm to calculate
   (i) $\gcd(91, 169)$
   (ii) $\gcd(1001, 4199)$

   Can you find elements x, y such that $ax + by = \gcd(a, b)$?

6. (Slightly harder, with polynomials)
   (i) Is $X^4 + 1$ prime in $\mathbb{Z}[X]$? What about in $\mathbb{R}[X]$?
   (ii) $X^5 - X + 1 = (X - 1)p(X) + r(X)$ with $0 \leq \deg r(X) < \deg p(X)$
   (iii) $\gcd(X^5 - X + 1, X^6 - X^2 + 2X - 1)$
   (iv) For $a, b, c \in \mathbb{Z}$ show that $\gcd(ac, bc) = |c| \gcd(a, b)$

Fun problems

1. Suppose that n is a positive integer for which all three of n, $n + 2$ and $n + 4$ are prime numbers. Prove that n must equal 3.
2. Does there exist integers x and y for which $x^2 - y^2 = 2026$?
3. Prove that for all positive integers n, we have $\gcd(21n + 4, 14n + 3) = 1$.

4. Consider the polynomial $p(n) = n^2 + n + 41$. Note that $p(0) = 41$, $p(1) = 43$, $p(2) = 47$, $p(3) = 53$, $p(4) = 61$ are each prime numbers. Does there exist a positive integer n for which n is not a prime number?

5. Find all positive integers a, b and c which satisfy the condition $a+b+c = \mathrm{lcm}(a,b,c)$. Here $\mathrm{lcm}(a,b,c)$ denotes the least integer N so that $a|N$, $b|N$ and $c|N$.

Slightly harder questions

1. Let n be a positive integer. Prove that there exists a positive integer k so that none of the integers $k, k+1, \ldots, k+n$ is a prime number.

2. Let m and n be distinct positive integers. Prove that $\gcd(2^{2^m}+1, 2^{2^n}+1) = 1$.

3. Suppose that $2^n - 1$ is a prime number, where n is a positive integer. Prove that n must be a prime number.

4. Suppose that 2^a+1 is a prime number, where a is a positive integer. Prove that there exists a non-negative integer n for which $a = 2^n$.

5. Let F_n be a sequence of integers defined by setting $F_0 = F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for every $n \geq 2$. Prove that $\gcd(F_n, F_{n-1}) = 1$ for every integer n. (The sequence F_n is the Fibonacci sequence).

6. Let n be an integer. Let k and $a_i \in \{0, 1, \ldots, 9\}$ be integers chosen so that $n = \sum_{j=0}^{k} 10^j a_j$, i.e. the base 10 representation of n is $a_k a_{k-1} \ldots a_1 a_0$. Prove that $9|n$ if and only if $9|\sum_{j=0}^{k} a_j$, i.e. an integer n is divisible by 9 if and only if the sum of its digits is divisible by 9.

7. Show that $p \in \mathbb{Z}$ is prime if and only if it is *irreducible*, i.e. if $p = ab$ for some $a, b \in \mathbb{Z}$, then a or b is invertible (± 1) (Hint: For the harder direction, what can you say about $\gcd(a, p)$?).

8. Prove that there are infinitely many primes p that are of the form $4n+3$ for some integer n.

9. Given $n > 1$ be a positive integer that is not a prime number, and let $1 = d_1 < d_2 < \cdots < d_k = n$ be the divisors of n for some $k \geq 3$. Find all such integers n for which $d_i | d_{i+1} + d_{i+2}$ for every $i \leq k-2$.

Tools

Euler's Theorem

In this section, we would like to prove Euler's theorem, which states that for any coprime $a, m \in \mathbb{Z}$, we have

$$a^{\varphi(m)} \equiv 1 \mod m$$

where φ is *Euler's totient function*, i.e.

$$\varphi(m) = \#\{a : \gcd(a, m) = 1,\ 0 \le a < m\}.$$

1. Show that $a \in \mathbb{Z}$ has an inverse modulo m if and only if $\gcd(a, m) = 1$, i.e. there exists $b \in \mathbb{Z}$ such that

   $$ab \equiv 1 \mod m.$$

   Further show that modulo m, there exist $\varphi(m)$ elements which are invertible.

2. For $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$ show that ka has an inverse modulo m if and only if $\gcd(k, m) = 1$ where $k \in \mathbb{Z}$.

3. Prove Euler's Theorem. You are allowed to use the fact that the invertible elements are modulo m unique. (Hint: The product of all invertible elements is constant modulo m).

Chinese Remainder Theorems

In this section, we want to prove the Chinese Remainder Theorem, i.e. for $m_1, \dots, m_k$ pairwise co-prime and $a_1, \dots, a_k$, there exists a solution $x \in \mathbb{Z}$, to the problem

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ &\dots \\ x &\equiv a_k \mod m_k. \end{aligned}$$

1. Using Bezout's identity, show that the CRT hold for $k = 2$, i.e there always exists a solution to

   $$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2. \end{aligned}$$

   if $\gcd(m_1, m_2) = 1$. Show that this solution is unique modulo $m_1 m_2$.

2. Prove the CRT. (Hint: Can we iterate this method?)

3. Consider $M = \prod_j m_j$ and define $M_j = M/m_j$. Using Bezout's identity to find N_j with $N_j M_j \equiv 1 \mod m_j$, can you find a direct solution to the problem?

4. Given a list of pairs $(x_1, y_1), \ldots (x_d, y_d)$ with x_j all distinct, can you find a polynomial f of degree d which interpolates all pairs, i.e. $f(x_j) = y_j$ for $j = 1, \ldots, d$?

Difficult problems

1. Call admissible a set A of integers that has the following property:

   If $x, y \in A($ possibly $x = y)$ then $x^2 + kxy + y^2 \in A$ for every integer k.

   Given integers m and n, prove that the only admissible set containing both m and n is the set of all integers if and only if $\gcd(m, n) = 1$.

2. The number $N = 4444^{4444}$ is written on the board. Let A denote the sum of the digits of N (when N is written in base 10), and let B denote the sum of the digits of A. What is the sum of the digits of B? (As an example, if the number 12411624662401682 is written on the board, its sum of digits is $1+2+4+1+1+6+2+4+6+6+2+4+0+1+6+8+2 = 56$, whose sum of digits is $5 + 6 = 11$, whose sum of digits is $1 + 1 = 2$.)

3. Let n be an odd integer greater than 1, and let $k_1, \ldots, k_n$ be given integers. Let $a = (a_1, \ldots, a_n)$ be any of the $n!$ orderings of the integers $1, 2, \ldots, n$, and define $S(a) = \sum_{j=1}^{n} a_j \cdot k_j$. Prove that there exist two distinct orderings b and c so that $n!$ divides the difference $S(b) - S(c)$. Here $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1) \cdot n$ denotes the number of distinct ways to order the numbers $1, 2, \ldots, n$.

Properties of congruences

In this section, we want to show for any integer m some well-definedness properties of $\mod m$.

1. Show that for any $a, b \in \mathbb{Z}$, we have
   - $m|a, m|b \implies m|(a+b)$,
   - $m|a \implies m|ab$

2. Show that $\mod m$ defines an *equivalence relation*, i.e. for any $a, b, c \in \mathbb{Z}$
   - (Reflexivity) $a \equiv a$, a is congruent to itself,
   - (Symmetry) $a \equiv b \implies b \equiv a$, if a is congruent to b, then so is b to a,

- (Transitivity) $a \equiv b, b \equiv c \implies a \equiv c$, if a is congruent to b and b to c, then so is a to c.

3. For $a \equiv p$ and $b \equiv q$ show that $a + b \equiv p + q$.
4. For $a \equiv p$ and $b \equiv q$ show that $ab \equiv pq$.

With these properties, we can define an arithmetic structure on the set of integers modulo m.

For $a \in \mathbb{Z}$, define $\overline{a}$ as the set that contains all elements in $\mathbb{Z}$ which are congruent to a, i.e.

$$\overline{a} = \{b \in \mathbb{Z} : b \equiv a \mod m\}.$$

Define $\mathbb{Z}_m = \{\overline{a} : a \in \mathbb{Z}\}$. Can you prove the following statements?

(i) $\overline{a} = \overline{b}$ if and only if $a \equiv b \mod m$

(ii) $\mathbb{Z}_m$ contains m elements which are called *congruence classes* of $\mod m$

(iii) $\overline{a} + \overline{b} := \overline{a+b}$ defines an addition

(iiii) $\overline{a}\overline{b} := \overline{ab}$ defines a multiplication

Numerical answers to the first questions

1. (i) $91 = 7 \cdot 13$ is not a prime; 127 is a prime; $221 = 13 \cdot 17$ is not a prime.

   (ii) $X^4 + 1$ is prime in $Z[X]$ but not in $\mathbb{R}[X]$ as $X^4 + 1 = (X^2 + 2\sqrt{2}X + 1)(X^2 - 2\sqrt{2}X + 1)$

2. (i) $169 = 91 + 78$

   (ii) $4199 = 4 \cdot 1001 + 195$

   (iii) $X^5 - X + 1 = (X - 1)(X^4 - X^3 + X^2 - X) + 1$

3. (i) $-169 + 2 \cdot 91 = 13 = \gcd(169, 91)$

   (ii) $36 \cdot 4199 - 151 \cdot 1001 = 13 = \gcd(1001, 4199)$

   (iii) $-(X^4+X^3+X^2+X)(X^6-X^2-1)+\left(1 + X(X^4 + X^3 + X^2 + X)\right)(X^5-X + 1) = 1 = \gcd(X^6 - X^2 - 1, X^5 - X + 1)$