Modular arithmetic for dummies

Jan Kociniak
Maths Beyond Limits 2017

1 Theory

As the number theory is focused mostly on integers, we consider all of the numbers mentioned in the following theorems being integers, unless stated otherwise.

1.1 Basic theorems

Theorem 1.1.1 Let a, m be integers and $m > 0$. A number $\widetilde{a}$ for which the congruence $a\widetilde{a} \equiv 1 \pmod{m}$ is true is called **the inverse** of a modulo m. There is only one inverse of an element modulo m (in other words, there are no numbers $\widetilde{a_1}$ and $\widetilde{a_2}$ such that $\widetilde{a_1} \equiv \widetilde{a_2} \pmod{m}$ and $a\widetilde{a_1} \equiv a\widetilde{a_2} \equiv 1 \pmod{m}$). The inverse of an element modulo m exists if and only if the element is relatively prime to m.

Theorem 1.1.2 - Euler's theorem
Let $\phi(n)$ be the number of positive integers relatively prime to n. Let a be relatively prime to n. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Theorem 1.1.3 - Fermat's little theorem
Let p be a prime number. Let a be relatively prime to p. Then $a^{p-1} \equiv 1 \pmod{p}$. It's a direct consequence of taking a prime n in Euler's theorem, since $\phi(n) = n - 1$ if and only if n is a prime number.

Theorem 1.1.4 - Wilson's theorem
The number n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

Theorem 1.1.5 - Chinese remainder theorem
Let $m_1, \ldots, m_n$ be positive, different from 1 and pairwise relatively prime. Then for any $a_1, \ldots, a_n$ the system of linear congruences

$$x \equiv a_1 \pmod{m_1}, \quad \ldots, \quad x \equiv a_n \pmod{m_n}$$

has solutions, and any two such solutions are congruent modulo $m = m_1 \cdots m_n$.

1.2 Advanced theory

1.2.1 The order of an element modulo n

Given the numbers a, n such that $n > 1$ and $\gcd(a, n) = 1$, **the order of a modulo n** is the smallest number d for which $a^d \equiv 1 \pmod{n}$ (such a number exists, since from the Euler's theorem $a^{\phi(n)} \equiv 1 \pmod{n}$, but it doesn't have to be the smallest number with that property). If $\gcd(a, n) > 1$, the order of a modulo n doesn't exist. We denote the order of a modulo n as $\mathrm{ord}_n(a)$. The most important and powerful property of $\mathrm{ord}_n(a)$ is the fact that if $a^m \equiv 1 \pmod{n}$ for some m, then $\mathrm{ord}_n(a)$ divides m.

1.2.2 Primitive roots

We call g **a primitive root modulo** n if $\text{ord}_n(g) = \phi(n)$. The primitive roots modulo n exists if and only if $n \in \{2, 4, p^\alpha, 2p^\alpha\}$, where $p \geqslant 3$ is any prime and α is any positive integer. If g is a primitive root modulo p, where p is an odd prime, then the sets $\{g, g^2, \ldots, g^{p-1}\}$ and $\{1, 2, \ldots, p-1\}$ are equal. Additionally, g is a primitive root modulo odd prime p if and only if $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ and $g^k \not\equiv 1 \pmod{p}$ for all $1 \leqslant k \leqslant \frac{p-1}{2}$. Also, given an odd prime p and its primitive root g, g^k is a quadratic residue if and only if k is even.

1.2.3 Quadratic residues

Given relatively prime numbers a and $n > 0$, we call a **a quadratic residue modulo** n if the congruence $x^2 \equiv a \pmod{n}$ has a solution. Otherwise we call a **a quadratic nonresidue modulo** n. For p being an odd prime, there are $\frac{p-1}{2}$ quadratic residues in the set $\{1, 2, \ldots, p-1\}$. Let p be a prime and let a be a positive integer relatively prime to p. The **Legendre symbol** of a with respect to p is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue (mod } p\text{)}, \\ -1 & \text{otherwise.} \end{cases}$$

The most useful properties of the Legendre symbol with respect to an odd prime p are as follows:

- If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- For any numbers $a_1, a_2, \ldots, a_k$ relatively prime to p, $\left(\frac{a_1 a_2 \cdots a_k}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_k}{p}\right)$.
- (**Euler's criterion**) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
- (**The law of quadratic reciprocity**) Let p and q be two odd distinct primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.
- (**The first supplement to the law of quadratic reciprocity**) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
- (**The second supplement to the law of quadratic reciprocity**) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

1.3 Other facts

Theorem 1.3.1 - Bézout's identity
For any numbers $a, b \neq 0$ denote $d = \gcd(a, b)$. Then there exist such numbers x, y that $ax + by = d$. The direct consequence of this is the fact that for every relatively prime numbers a, b there exist such numbers x, y that $ax + by = 1$.

Theorem 1.3.2 Let p be a prime number. Then $\binom{p}{i}$ is divisible by p for $1 \leqslant i \leqslant p-1$.

Theorem 1.3.3 Let $P(x)$ be a polynomial with integer coefficients and let n be positive integer. Let x, y be numbers such that $x \equiv y \pmod{n}$. Then $P(x) \equiv P(y) \pmod{n}$.

Theorem 1.3.4 Let p be a prime number and $P(x)$ be a polynomial of degree n with integer coefficients. Then the congruence

$$P(x) \equiv 0 \pmod{p}$$

has at most n incongruent solutions.

Theorem 1.3.5 - Thue's lemma
Let n be positive integer and a be a number relatively prime to n. Then there exist numbers x, y such that $|x|, |y| < \sqrt{n}$ and $x \equiv ay \pmod{n}$.

Theorem 1.3.6 - Dirichlet's theorem
Given relatively prime a, b, the sequence $an + b$ for $n = 0, 1, 2, \ldots$ contains an infinite number of primes.

Theorem 1.3.7 Let p be an odd prime. Then the congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

where $p \nmid a$ has a solution if and only if $\Delta \equiv 0 \pmod{p}$ or $\left(\frac{\Delta}{p}\right) = 1$ where $\Delta = b^2 - 4ac$. The solutions are given by this formula:

$$x \equiv \widetilde{2a}(-b \pm \sqrt{\Delta}) \pmod{p}$$

where $\sqrt{\Delta}$ is any number for which $(\sqrt{\Delta})^2 \equiv \Delta \pmod{p}$ and $\widetilde{2a}$ is the inverse (modulo p) of $2a$.

Theorem 1.3.8 For any prime $p = 4k + 1$ there exist integers x, y such that $p = x^2 + y^2$.

Theorem 1.3.9 Positive integer n is a sum of two squares of integers if and only if the power of every prime divisor $p \equiv 3 \pmod{4}$ in the factorisation of n is even.

2 Problems I

Problem 2.1 Let $P(x)$ be a polynomial with integer coefficients such that $n \mid P(2^n)$ for every positive integer n. Prove that $P(x) \equiv 0$.

Source: ELMO 2016

Problem 2.2 Let a_0 be a positive integer and $a_n = 5a_{n-1} + 4$ for all $n \geqslant 1$. Can a_0 be chosen so that a_{54} is a multiple of 2013?

Source: Baltic Way 2013

Problem 2.3 Prove that the sequence $\{2^n - 3 \mid n = 2, 3, \dots\}$ contains an infinite subsequence whose members are all relatively prime.

Problem 2.4 Determine all positive integers relatively prime to all the terms of the infinite sequence

$$a_n = 2^n + 3^n + 6^n - 1, \ n \geqslant 1.$$

Source: IMO Shortlist 2005

Problem 2.5 Suppose that $\gcd(a, b) = 1$ and p is a prime. Prove that any prime factor q of $\frac{a^p - b^p}{a-b}$ is either equal to p or of the form $1 + kp$.

Problem 2.6 Find all integer solutions of the following equation:

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

Problem 2.7 Show that if m, n are positive integers, then $4mn - m - n$ cannot be a square of an integer.

Problem 2.8 Given a positive prime number p. Prove that there exist a positive integer α such that $p \mid \alpha(\alpha - 1) + 3$, if and only if there exist a positive integer β such that $p \mid \beta(\beta - 1) + 25$.

Source: Spain 2016

Problem 2.9 Let n be a positive integer with the following property: $2^n - 1$ divides a number of the form $m^2 + 81$, where m is a positive integer. Find all possible n.

Source: Hong Kong TST 2017

Problem 2.10 Let n be a positive integer. Prove that the number $2^n + 1$ has no prime divisor of the form $8k - 1$, where k is a positive integer.

Source: Vietnam TST 2003

Problem 2.11 Prove that if $n > 1$ then any prime factor of $2^{2^n} + 1$ is congruent to $1 \pmod{2^{n+2}}$.

Problem 2.12 Let p be a prime number, and let n be a positive integer. Find the number of quadruples (a_1, a_2, a_3, a_4) with $a_i \in \{0, 1, \dots, p^n - 1\}$ for $i = 1, 2, 3, 4$, such that

$$p^n \mid (a_1a_2 + a_3a_4 + 1).$$

Source: Baltic Way 2014

Problem 2.13 Let a, b be positive integers such that $b^n + n$ is a multiple of $a^n + n$ for all positive integers n. Prove that $a = b$.

Source: IMO Shortlist 2005

Problem 2.14 The sequence $\{a_n\}_{n \geqslant 0}$ is defined by $a_0 = 2, a_1 = 4$ and

$$a_{n+1} = \frac{a_n a_{n-1}}{2} + a_n + a_{n-1}$$

for all positive integers n. Determine all prime numbers p for which there exists a positive integer m such that p divides the number $a_m - 1$.

Source: MEMO 2016

Problem 2.15 Find all positive integers n such that for any integer k there exists an integer a for which $a^3 + a - k$ is divisible by n.

Source: APMO 2014

3 Problems II

Problem 3.1 Find all natural numbers m, n such that mn divides $(2^{2^n}+1)(2^{2^m}+1)$.

Source: Bulgaria 2016

Problem 3.2 Let p be an odd prime. Show that

$$1^i + 2^i + \cdots + (p-1)^i \equiv 0 \pmod{p} \quad \text{for} \quad 1 < i < p-1.$$

Problem 3.3 Prove that if $p = 4k+1$ is prime, then $p \mid k^k - 1$.

Problem 3.4 Let $p > 3$ be a prime such that $p \equiv 3 \pmod 4$. Given a positive integer a_0 define the sequence $a_0, a_1, \ldots$ of integers by $a_n = a_{n-1}^{2^n}$ for all $n = 1, 2, \ldots$. Prove that it is possible to choose a_0 such that the subsequence $a_N, a_{N+1}, a_{N+2}, \ldots$ is not constant modulo p for any positive integer N.

Source: Baltic Way 2016

Problem 3.5 Given are integers a, b such that $a \neq 0$ and $6a \mid 3 + a + b^2$. Prove that $a < 0$.

Source: Poland 2013

Problem 3.6 Let p, q be prime numbers (q is odd). Prove that there exists an integer x such that: $q|(x+1)^p - x^p$ if and only if $q \equiv 1 \pmod p$.

Source: Iran 2016

Problem 3.7 Prove that if a is a quadratic residue for every prime, then a is a square of an integer.

Problem 3.8 Prove that $2^{3^n}+1$ has at least n distinct prime divisors in the form $8k+3$.

Problem 3.9 Prove that $2^{2^n}+1$ has a prime divisor greater than $2^{n+2}(n+1)$.

Problem 3.10 Let $a > 1$ be a positive integer. Prove that there exist integer $n \geqslant 0$ such that $2^{2^n} + a$ is not prime.

Problem 3.11 Find all positive integers n such that there exists a unique integer a such that $0 \leqslant a < n!$ with the following property:

$$n! \mid a^n + 1.$$

Source: IMO Shortlist 2005

Problem 3.12 Let k be a fixed integer greater than 1, and let $m = 4k^2 - 5$. Show that there exist positive integers a and b such that the sequence (x_n) defined by

$$x_0 = a, \quad x_1 = b, \quad x_{n+2} = x_{n+1} + x_n \quad \text{for} \quad n = 0, 1, 2, \ldots,$$

has all of its terms relatively prime to m.

Source: IMO Shortlist 2004

Problem 3.13 Determine all integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Source: IMO 1990

Problem 3.14 Let x and y be positive integers. If $x^{2^n} - 1$ is divisible by $2^n y + 1$ for every positive integer n, prove that $x = 1$.

Source: IMO Shortlist 2012

Problem 3.15 Prove that there does not exist positive integers a, b and k such that $4abk - a - b$ is a perfect square.

Source: Olympic Revenge 2017