Competitive Programming and Mathematics Society

Mathematics Workshop #5

Extended Number Theory

Cyril and Haibing

Table of contents

Introduction

- Pizza time! Later

Attendance form

Queue Are Code

Exponentials in modular arithmetic

Let p be a prime.

Since multiplication under mod p is invertible, and we have a finite space, there must exist a positive k where $a^k \equiv 1 \pmod{p}$. Why?

Exponentials in modular arithmetic

Let p be a prime.

Since multiplication under mod p is invertible, and we have a finite space, there must exist a positive k where $a^k \equiv 1 \pmod{p}$. Why?

By the pigeonhole principle, there must be two a^m and a^n which are equal for $m \neq n$, and since a^{-1} exists, $a^{m-n} \equiv 1 \pmod{p}$.

Exponentials in modular arithmetic

Let p be a prime.

Since multiplication under mod p is invertible, and we have a finite space, there must exist a positive k where $a^k \equiv 1 \pmod{p}$. Why?

By the pigeonhole principle, there must be two a^m and a^n which are equal for $m \neq n$, and since a^{-1} exists, $a^{m-n} \equiv 1 \pmod{p}$.

$$a^{p-1} \equiv 1 \pmod{p}$$

Exponentials in modular arithmetic

Let p be a prime.

Since multiplication under mod p is invertible, and we have a finite space, there must exist a positive k where $a^k \equiv 1 \pmod p$. Why?

By the pigeonhole principle, there must be two a^m and a^n which are equal for $m \neq n$, and since a^{-1} exists, $a^{m-n} \equiv 1 \pmod p$.

$$a^{p-1} \equiv 1 \pmod p$$

Closed form for smallest length positive integer k? Not trivial! But what can we say about k?

Exponentials in modular arithmetic

Let p be a prime.

Since multiplication under mod p is invertible, and we have a finite space, there must exist a positive k where $a^k \equiv 1 \pmod p$. Why?

By the pigeonhole principle, there must be two a^m and a^n which are equal for $m \neq n$, and since a^{-1} exists, $a^{m-n} \equiv 1 \pmod p$.

$$a^{p-1} \equiv 1 \pmod p$$

Closed form for smallest length positive integer k? Not trivial! But what can we say about k? $p-1$ is divisible by k.

Quadratic Residues

We call a remainder x a "quadratic residue" mod m if there exists a y such that $y^2 \equiv x \pmod{m}$.

This is useful as under the modulus of certain numbers, only very few remainders are quadratic residues. For any prime p, there are exactly $\frac{p+1}{2}$ quadratic residues mod p.

Quadratic Residues

We call a remainder x a "quadratic residue" mod m if there exists a y such that $y^2 \equiv x \pmod{m}$.

This is useful as under the modulus of certain numbers, only very few remainders are quadratic residues. For any prime p, there are exactly $\frac{p+1}{2}$ quadratic residues mod p.

Good numbers to use for equations dealing with squares:
Mod 3: Quadratic residues are $0, 1$
Mod 4: $0, 1$
Mod 5: $0, 1, 4$
Mod 8: $0, 1, 4$
Mod 16: $0, 1, 4, 9$

Example Problems

Show that 60 divides any product of Pythagorean triples.

Example Problems

Show that 60 divides any product of Pythagorean triples.

Consider $\bmod 3, 5$ and 8. Let our Pythagorean triple be a, b, c, and $a^2 + b^2 = c^2$. Squares exist only as $0, 1$ for 3, and $0, 1, 4$ in 5 and 8.

Example Problems

Show that 60 divides any product of Pythagorean triples.

Consider $\mod 3, 5$ and 8. Let our Pythagorean triple be a, b, c, and $a^2 + b^2 = c^2$. Squares exist only as $0, 1$ for 3, and $0, 1, 4$ in 5 and 8.

For 3, at least one of a, b must $0 \pmod 3$ so that c^2 is 0 or 1

Example Problems

Show that 60 divides any product of Pythagorean triples.

Consider $\mod 3, 5$ and 8. Let our Pythagorean triple be a, b, c, and $a^2 + b^2 = c^2$. Squares exist only as $0, 1$ for 3, and $0, 1, 4$ in 5 and 8.

For 3, at least one of a, b must $0 \pmod 3$ so that c^2 is 0 or 1
For 5, 4 cannot be constructed as the sum of two of $0, 1, 4$ under $\pmod 5$, so an argument similar to before is applicable
For 8, for $a^2 + b^2$ to be a quadratic residue either both are $4 \pmod 8$ (so both are even, thus abc is a multiple of 4), or one of a^2, b^2 is divisible by 8 (similar argument to before), thus a is divisible by 4 (this idea does not work under $\pmod 4$).

Cubic Residues

Similarly, we call a remainder x a "cubic residue" mod m if there exists a y such that $y^3 \equiv x$ (mod m). For primes $p \equiv 1 \pmod 3$ there are exactly $\frac{p+2}{3}$ residues, but p for $p \equiv 2 \pmod 3$.

Cubic Residues

Similarly, we call a remainder x a "cubic residue" mod m if there exists a y such that $y^3 \equiv x$ (mod m). For primes $p \equiv 1 \pmod 3$ there are exactly $\frac{p+2}{3}$ residues, but p for $p \equiv 2 \pmod 3$.

Good numbers to use for equations dealing with cubes:
Mod 7: $0, 1, 6$
Mod 9: $0, 1, 8$

Diophantine equations

Definition

A diophantine equation is one with integer coefficients and only integer solutions of interest.

Example: Find the smallest positive integers a, b, c such that $\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = 4$.

- Play around with the equation
- Abuse integer-ness by factoring terms and partioning factors
- Substitute expressions to create simpler equations
- Test cases/find minimum solutions to build from
- Utilise known residues

Another cool technique will be discussed!

Example Questions

Find all integer solutions to $a^3 + b^3 + c^3 = 2001$

Example Questions

Find all integer solutions to $a^3 + b^3 + c^3 = 2001$

Consider mod 9. $2001 \equiv 3 \pmod 9$, $x^3 \in (-1, 0, 1)$. So, $a^3 \equiv b^3 \equiv c^3 \equiv 1$. It can be easily seen from here that the only solutions are such that $\{a, b, c\} = \{10, 10, 1\}$

Example Questions

Prove that for any prime p, there exists a pair of integers a, b such that $a^2 + b^2 + 1$ divisible by p.

Example Questions

Prove that for any prime p, there exists a pair of integers a, b such that $a^2 + b^2 + 1$ divisible by p.

Rewrite the equation as $a^2 \equiv 1 - b^2 \pmod{p}$. How many values can each side take?

Example Questions

Prove that for any prime p, there exists a pair of integers a, b such that $a^2 + b^2 + 1$ divisible by p.

Rewrite the equation as $a^2 \equiv 1 - b^2 \pmod{p}$. How many values can each side take?

There are $\frac{p+1}{2}$ quadratic residues, so the LHS and RHS can take on $p + 1$ values in total. By PHP, at least one value occurs in both sides as there are only p remainders.

Infinite Descent

Assume there exists a smallest solution, and prove the existence of a smaller one.

Famous example is the proof of the irrationality of $\sqrt{2}$.

Infinite Descent - question

Find all integer solutions to $a^3 + 3b^3 = 9c^3$.

Infinite Descent - question

Find all integer solutions to $a^3 + 3b^3 = 9c^3$.Assume there exists non-zero, positive a, b, c satisfying this.

- a is divisible by 3.

Infinite Descent - question

Find all integer solutions to $a^3 + 3b^3 = 9c^3$.Assume there exists non-zero, positive a, b, c satisfying this.

- a is divisible by 3.
- So, b is divisible by 3.

Infinite Descent - question

Find all integer solutions to $a^3 + 3b^3 = 9c^3$.Assume there exists non-zero, positive a, b, c satisfying this.

- a is divisible by 3.
- So, b is divisible by 3.
- So, c is divisible by 3.

By infinite descent, we see a contradiction has been reached, so $a = b = c = 0$ is the only solution.

A harder counting question

Show there is a positive Fibonacci number divisible by 2023.

A harder counting question

Show there is a positive Fibonacci number divisible by 2023.

Hint 1: Divisibility $\to$ Modular arithmetic

Hint 2: Pigeonhole principle, and calculating (F_n, F_{n+1}) is "deterministic" to calculate (forwards and backwards).

An alternate proof of infinite primes

The Fermat numbers are numbers of the form $2^{2^n} + 1$. The first 5 are

$$F_0 = 2^{2^0} + 1 = 3 \tag{1}$$
$$F_1 = 2^{2^1} + 1 = 5 \tag{2}$$
$$F_2 = 2^{2^2} + 1 = 17 \tag{3}$$
$$F_3 = 2^{2^3} + 1 = 257 \tag{4}$$
$$F_4 = 2^{2^4} + 1 = 65537 \tag{5}$$

Fermat thought all such numbers were prime. Unfortunately, F_5 is divisible by 641, so this isn't quite true. However, these numbers do give us another way to show there are infinitely many primes.

An alternate proof of infinite primes

The Fermat numbers are numbers of the form $2^{2^n} + 1$. The first 5 are

$$F_0 = 2^{2^0} + 1 = 3 \tag{1}$$
$$F_1 = 2^{2^1} + 1 = 5 \tag{2}$$
$$F_2 = 2^{2^2} + 1 = 17 \tag{3}$$
$$F_3 = 2^{2^3} + 1 = 257 \tag{4}$$
$$F_4 = 2^{2^4} + 1 = 65537 \tag{5}$$

Fermat thought all such numbers were prime. Unfortunately, F_5 is divisible by 641, so this isn't quite true. However, these numbers do give us another way to show there are infinitely many primes.

Claim: All Fermat numbers are relatively coprime.

A surprise!

4 problems = 1 chocolate

Further events

Please join us for:

- Social session tomorrow!

Attendance form :D