MA 17: HOW TO SOLVE IT
HANDOUT 2: ELEMENTARY NUMBER THEORY

Instructor Lingfu Zhang (lingfuz@caltech) **Office** Linde Hall 358
TA Minghao Pan (mpan2@caltech)

Extremal elements. (left from last time)

Problem 11.
100 soccer teams participate in a tournament, with one match between every two teams (resulting in each team playing 99 games). Suppose that no team wins all 99 games. Prove that there exist three teams A, B, and C, such that A beats B, B beats C, and C beats A.

Problem 12. (IMO 1988)
Let a and b be positive integers such that $ab+1$ divides a^2+b^2. Show that $\frac{a^2+b^2}{ab+1}$ is the square of an integer.

Prime Factorization. *Any positive integer n can be uniquely written as $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are prime numbers, and $a_1, a_2, \ldots, a_k$ are positive integers.*

Modular Arithmetic. *$a \equiv b \pmod{n}$ (a and b are congurent modulo n) if $a-b$ is divisible by n. This divides all integers into n equivalent classes $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. The ring structure of $\mathbb{Z}$ induces a ring structure on $\mathbb{Z}_n$.*

Problem 1. (Putnam 2024, A1)
Determine all positive integers n for which there exist positive integers a, b, and c satisfying

$$2a^n + 3b^n = 4c^n.$$

Problem 2.
The last four digits of a perfect square are equal. Prove that they are all equal to zero.

Problem 3. ***Fermat's Little Theorem***
Let p be a prime number, and n an integer. Then

$$n^p - n \equiv 0 \pmod{p}.$$

Problem 4. (Putnam 2024, A4)
Find all primes $p > 5$ for which there exists an integer a and an integer r satisfying $1 \le r \le p-1$ with the following property: the sequence $1, a, a^2, \ldots, a^{p-5}$ can be rearranged to form a sequence $b_0, b_1, b_2, \ldots, b_{p-5}$ such that $b_n - b_{n-1} - r$ is divisible by p for $1 \le n \le p-5$.

Problem 5.
Let p be a prime number. Show that from any $2p-1$ integers, one can choose p of them, whose sum is divisible by p.

Primitive root. *A positive number g is called a primitive root modulo n if, for every integer a that is coprime to n, there exists an integer k such that*

$$g^k \equiv a \pmod{n}.$$

If p is a prime number, then g is a primitive root modulo p if and only if the multiplicative order of g modulo p is equal to $p-1$.
For every prime number p, there exists at least one primitive root modulo p.

Sketch proof. Consider the multiplicative group $\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$. Note that this is an abelian group, so by the fundamental theorem of finite abelian groups, it can be written as a product of cyclic groups

$$C_{q_1} \oplus C_{q_2} \oplus \cdots \oplus C_{q_k},$$

where $q_1, q_2, \ldots, q_k$ are powers of (not necessarily distinct) primes, and $q_1 q_2 \cdots q_k = p-1$.

Let m be the least common multiple of $q_1, q_2, \ldots, q_k$. Then m divides $p-1$, and $x^m \equiv 1 \pmod{p}$ for each $x \in \mathbb{F}_p^\times$. On the other hand, the polynomial $x^m - 1$ has at most m roots modulo p, so we must have $m \geq p-1$. Thus $m = p-1$, and $q_1, q_2, \ldots, q_k$ are coprime to each other.

This implies that $q_1, q_2, \ldots, q_k$ are powers of distinct primes, and hence the group

$$\mathbb{F}_p^\times = C_{q_1} \oplus C_{q_2} \oplus \cdots \oplus C_{q_k}$$

is isomorphic to $C_{q_1 q_2 \cdots q_k} = C_{p-1}$, whose generator is a primitive root modulo p. □

Problem 6.
Let p be an odd prime number. Show that the equation

$$x^2 \equiv -1 \pmod{p}$$

has a solution if and only if $p \equiv 1 \pmod{4}$.

Problem 7. (Putnam 2021, A5)
Let A be the set of all integers n such that $1 \leq n \leq 2021$ and $\gcd(n, 2021) = 1$. For every nonnegative integer j, let

$$S(j) = \sum_{n \in A} n^j.$$

Determine all values of j such that $S(j)$ is a multiple of 2021.

Base numbers. *For any integer $g > 1$, every positive integer can be uniquely written as*

$$a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0,$$

where each $a_i \in \{0, 1, \ldots, g-1\}$ and $a_n \neq 0$.
(For example, $g = 2$ gives the binary representation, and $g = 10$ gives the decimal representation.)

Problem 8. (Putnam 2020, B1)
For a positive integer n, define $d(n)$ to be the sum of the digits of n when written in binary (for example, $d(13) = 1 + 1 + 0 + 1 = 3$). Let

$$S = \sum_{k=1}^{2020} (-1)^{d(k)} k^3.$$

Determine S modulo 2020.

Reminder PSet 1 is due by the end of Oct 8 (on Canvas). The first problem session (to discuss PSet 1) will be on Oct 9, 7-8 PM, at the same location.