Columbia Putnam Seminar

10/7/25

1 Crash Course in Modular Arithmetic

- $a \equiv b \pmod{m}$ means $m \mid a - b$
- You can add, subtract, and multiply numbers modulo m, but not divide.
- If $\gcd(a, m) = 1$, then a^{-1} is an integer mod m such that $a^{-1}a \equiv 1 \pmod{m}$. Can be computed via the Euclidean Algorithm.
- Chinese Remainder Theorem: For pairwise coprime m_i, the system of congruences $x \equiv a_i \pmod{m_i}$ is equivalent to a singular congruence $x \equiv A \pmod{M}$, where $M = \prod_i^n m_i$ and $A = \sum_{i=1}^n (M/m_i)(M/m_i)^{-1}a_i$, where the inverse for each i is taken mod m_i. Can also be interpreted in that any equation mod m is equivalent to solving it modulo the prime factors.
- Fermat's Little Theorem: If p prime and $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$.
- Euler's Totient Function: $\phi(n)$ is the number of positive integers less than n relatively prime to n. If $n = \prod_{i=1}^k p_i^{e_i}$ is the prime factorization of n, then $\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$.
- Euler's Theorem: If $\gcd(a, m) = 1$, $a^{\varphi(m)} \equiv 1 \pmod{m}$.
- Order of a mod m: smallest positive integer k such that $a^k \equiv 1$. If $a^n \equiv 1 \pmod{m}$, the order must divide n.
- Wilson's Theorem: $(p-1)! \equiv -1 \pmod{p}$.
- Primitive root: g such that $g^{\phi(m)} \equiv 1 \pmod{m}$. This exists iff $m = 1, 2, 4$, or of the form p^k and $2p^k$ for odd prime p.

2 Problems

1. For positive integers a, m, and n, show that that $a^m - 1$ divides $a^n - 1$ iff $m \mid n$.
2. Prove there are infinitely many primes equivalent to $3 \pmod{4}$.
3. (2007 B1) Let f be a nonconstant polynomial with positive integer coefficients. Prove that if n is a positive integer, then $f(n)$ divides $f(f(n) + 1)$ if and only if $n = 1$.
4. Find the sum of all positive integers n less than 2030 such that $n^3 + 2n^2 + 2n + 1$ is divisible by 2029.
5. Prove that for any positive integer k, there exist k consecutive positive integers such that none of them are prime powers.
6. (2017 B2) Suppose that a positive integer N can be expressed as the sum of k consecutive positive integers
$$N = a + (a + 1) + (a + 2) + \cdots + (a + k - 1)$$
for $k = 2017$ but for no other values of $k > 1$. Considering all positive integers N with this property, what is the smallest positive integer a that occurs in any of these expressions?
7. Find all integer solutions (a, b, c) for the equation $a^3 + 2b^3 = 7c^3$.

8. (2006 A2) Alice and Bob play a game in which they take turns removing stones from a heap that initially has n stones. The number of stones removed at each turn must be one less than a prime number. The winner is the player who takes the last stone. Alice plays first. Prove that there are infinitely many n such that Bob has a winning strategy. (For example, if $n = 17$, then Alice might take 6 leaving 11; then Bob might take 1 leaving 10; then Alice can take the remaining stones to win.)

9. (2001 A5) Prove that there are unique positive integers a, n such that $a^{n+1} - (a+1)^n = 2001$.

10. (2022 A3) Let p be a prime number greater than 5. Let $f(p)$ denote the number of infinite sequences $a_1, a_2, a_3, \ldots$ such that $a_n \in \{1, 2, \ldots, p-1\}$ and $a_n a_{n+2} \equiv 1 + a_{n+1} \pmod{p}$ for all $n \geq 1$. Prove that $f(p)$ is congruent to 0 or 2 $\pmod 5$.

11. (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.

12. (2024 A4) Find all primes $p > 5$ for which there exists an integer a and an integer r satisfying $1 \leq r \leq p-1$ 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 $1 \leq n \leq p-5$.

13. Prove that for each positive integer n, there are pairwise relatively prime integers $k_0, k_1, \ldots, k_n$, all strictly greater than 1, such that $k_0 k_1 \cdots k_n - 1$ is the product of two consecutive integers.