Columbia Putnam Seminar

10/27/24

1 Crash Course in Number Theory

- $\gcd(m, n)$: Greatest common divisor of m and n.
- Euclidean Algorithm: Compute $\gcd(m, n)$ by recursively using that $\gcd(m, n) = \gcd(n, n - m)$.
- Bezout's Lemma: There exists $x, y \in \mathbb{Z}$ such that $mx + ny = \gcd(m, n)$.
- Polignac's formula: The exponent of the prime p in $n!$ is $\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.
- $a \equiv b \pmod{m}$ means $m \mid a - b$
- 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 k.
- 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.
- Quadratic residue: a is a quadratic residue mod m if there is a solution to $x^2 \equiv a \pmod{m}$.
- Legendre symbol:
$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue mod } p \\ -1 & a \text{ is not a quadratic residue mod } p \\ 0 & p \mid a \end{cases}$$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
- $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
- Quadratic reciprocity: For $p \neq q$ primes, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

2 Problems

1. Prove that $\gcd(n^a - 1, n^b - 1) = n^{\gcd(a,b)} - 1$.

2. Find all positive integers $n < 10^{100}$ for which simultaneously n divides 2^n, $n-1$ divides $2^n - 1$, and $n-2$ divides $2^n - 2$.

3. Show that for each positive integer n, $n! = \prod_{i=1}^{n} \operatorname{lcm}\{1, 2, \ldots, \lfloor n/i \rfloor\}$.

4. Prove that the expression $\frac{\gcd(m,n)}{n}\binom{n}{m}$ is an integer for all pairs of integers $n \geq m \geq 1$.

5. A *base* 10 *over-expansion* of a positive integer N is an expression of the form

$$N = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_0 10^0$$

with $d_k \neq 0$ and $d_i \in \{0, 1, 2, \ldots, 10\}$ for all i. For instance, the integer $N = 10$ has two base 10 over-expansions: $10 = 10 \cdot 10^0$ and the usual base 10 expansion $10 = 1 \cdot 10^1 + 0 \cdot 10^0$. Which positive integers have a unique base 10 over-expansion?

6. Find the smallest positive integer j such that for every polynomial $p(x)$ with integer coefficients and for every integer k, the integer $p^{(j)}(k) = \frac{\mathrm{d}^j}{\mathrm{d}x^j} p(x)\big|_{x=k}$ is divisible by 2016.

7. Find all ordered pairs (a, b) of positive integers for which $\frac{1}{a} + \frac{1}{b} = \frac{3}{2018}$.

8. If p is a prime number greater than 3 and $k = \lfloor 2p/3 \rfloor$, prove that the sum $\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{k}$ of binomial coefficients is divisible by p^2.

9. 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.

10. Let $F_0, F_1, \ldots$ be the sequence of Fibonacci numbers, with $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. For $m > 2$, let R_m be the remainder when the product $\prod_{k=1}^{F_m - 1} k^k$ is divided by F_m. Prove that R_m is also a Fibonacci number.

11. Prove that for any positive integer n other than 2 or 6, $\varphi(n) \geq \sqrt{n}$.

12. Prove for every positive integer n the identity $\sum_{k=1}^{n} \varphi(k) \lfloor n/k \rfloor = \frac{n(n+1)}{2}$.

13. Prove that for any positive integer k, there exist k consecutive positive integers such that none of them are prime powers.

14. 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.)

15. Is there a sequence of positive integers in which every positive integer occurs exactly once and for every $k = 1, 2, 3, \ldots$ the sum of the first k terms is divisible by k?

16. Let p be an odd prime such that $p \equiv 2 \pmod 3$. Define a permutation π of the residue classes modulo p by $\pi(x) \equiv x^3 \pmod p$. Show that π is an even permutation iff $p \equiv 3 \pmod 4$.

17. Let q be an odd positive integer, and let N_q denote the number of integers a such that $0 < a < q/4$ and $\gcd(a, q) = 1$. Show that N_q is odd if and only if q is of the form p^k with k a positive integer and p a prime congruent to 5 or 7 modulo 8.

18. Let α denote the positive real root of the polynomial $x^2 - 3x - 2$. Compute the remainder when $\lfloor \alpha^{1000} \rfloor$ is divided by the prime number 997.