Number Theory

Eshan M.J

§1 Theory

Definition 1.1. The **order** of $a \pmod{p}$ is defined to be the smallest positive integer e such that

$$a^e \equiv 1 \pmod{p}.$$

Definition 1.2. Let p be a prime. An integer g is called a **primitive root** modulo p if the order of g modulo p is equal to $p-1$.

Theorem 1.3

Primitive root exists for all prime p

Definition 1.4. Let p be an odd prime and a an integer. The **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \text{if } p \mid a, \\ 1, & \text{if there exists an integer } b \text{ not divisible by } p \text{ such that } a \equiv b^2 \pmod{p}, \\ -1, & \text{if there is no integer } b \text{ with } a \equiv b^2 \pmod{p}. \end{cases}$$

Definition 1.5. The Jacobi symbol $\left(\frac{a}{n}\right)$ is defined by extending the Legendre symbol multiplicatively in the bottom.

Theorem 1.6 (Quadratic Reciprocity)

Let m and n be positive odd integers with $\gcd(m,n)=1$. Then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}.$$

> **Remark 1.7.** Often times if you have something like $f(a,b,..) \equiv 0 \pmod{n}$, it is useful to take the smallest prime $p \mid n$ and consider $f(a,b,..) \equiv 0 \pmod{p}$

§2 Problems

Problem 2.1 (Fundamental Theorem of Orders)**.** Suppose $a^N \equiv 1 \pmod{p}$. Then the order of $a \pmod{p}$ divides N.

Problem 2.2. Let p be an odd prime. Then for any integer a, the congruence

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

holds.

Problem 2.3. If p is an odd prime and $p \mid n^2+1$ then $4 \mid p-1$

Problem 2.4. Find all n such that n^2 divides 3^n+1

Problem 2.5. Let a and b be positive integers, and let $p \equiv 3 \pmod 4$ be a prime. If $p \mid (a^2+b^2)$, then $p \mid a$ and $p \mid b$.

Problem 2.6. If p is a prime such that $4 \mid p-1$ then there exists n such that $p|n^2+1$

Problem 2.7. find all integers $n \geq 1$ such that n divides $2^n - 1$

Problem 2.8. Suppose that for some positive integers r and s, the decimal expansion of 2^r is obtained by permuting the digits of the decimal expansion of 2^s, and that 2^r and 2^s have the same number of digits. Prove that $r = s$.

Problem 2.9 (USA TST 2008)**.** Prove that n^7+7 is never a perfect square for positive integers n.

Problem 2.10. Let $m, n \geq 3$ be positive odd integers. Prove that

$$2^m - 1 \nmid 3^n - 1.$$

Problem 2.11 (China TST 2006)**.** Find all positive integers a and n for which

$$n \mid \big((a+1)^n - a^n\big).$$

Problem 2.12. Let n be a positive integer and let $p > n+1$ be a prime. Prove that

$$p \mid 1^n + 2^n + \cdots + (p-1)^n.$$

Problem 2.13. Show that $n!$ is never a square for $n \geq 2$

Problem 2.14 (IMO 2005/4)**.** Determine all positive integers relatively prime to all terms of the infinite sequence

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

Problem 2.15. Counting prime factors without multiplicity, show that for every integer $n \geq 2$ there is some integer n' with $n < n' < 2n$ so that $n$and n' have the same number of prime factors.

§3 Bertrand's Postulate

[1] *Paul Erdős (1913–1996)* published over 1500 mathematical papers in his lifetime, and his first paper was an elementary proof of Bertrand's postulate, namely that for every natural number $n \geq 1$, there exists a prime number p such that

$$n < p \leq 2n.$$

[1]The exposition in this section follows material from a mid-semester examination of the course *Analytic Number Theory*, taught by Prof. Anwesh Ray.

Incidentally, this result was written when he was an undergraduate student, and it was considered an achievement worthy of earning him a PhD from the University of Budapest at the age of 21. Below we discover the proof, step by step.

Problem 3.1. You may assume without loss of generality that $n > 521$, via Landau's trick: the sequence

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 521$$

consists of prime numbers such that each term in the sequence is greater than half of the next term. Explain this step in detail.

Problem 3.2. Prove the inequality

$$\prod_{m+1<p\leq 2m+1} p \;\leq\; \binom{2m+1}{m} \;\leq\; 2^{2m}.$$

Problem 3.3. Use the above to show that

$$\prod_{p\leq n} p \leq 4^{n-1}$$

for all natural numbers $n \geq 2$. *Hint:* You may assume without loss of generality that n is an odd prime; write $n = 2m+1$. Now prove the result by induction.

Problem 3.4. Let e_p be the power of a prime p dividing $\binom{2n}{n}$. Show that

$$e_p = \sum_{k\geq 1}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right) \leq \max\{r \mid p^r \leq 2n\}.$$

Deduce that $e_p \leq 1$ for all primes $p > \sqrt{2n}$.

Problem 3.5. Show that primes p satisfying

$$\frac{2n}{3} < p \leq n$$

do not divide $\binom{2n}{n}$.

Problem 3.6. Prove the inequalities

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq \prod_{p\leq\sqrt{2n}} 2n \times \prod_{\sqrt{2n}<p\leq\frac{2n}{3}} p \times \prod_{n<p\leq 2n} p.$$

Problem 3.7. Let $P(n)$ denote the number of primes between n and $2n$. Show that

$$4^{n/3} < (2n)^{\sqrt{2n}+1+P(n)}.$$

By taking logarithms of both sides, deduce that for $n > 2^9 = 512$ we have $P(n) > 0$.

§4 Problems to Ponder

Problem 4.1. Let $f(n)$ denote the number of pairs of primes (p, q) such that $pq \leq n$. Find

$$\lim_{n\to\infty} \frac{f(n)}{n\log n}.$$

Problem 4.2. You are offered to make bets in favor of integers being squares. Integers n are drawn at random from the interval

$$x - x^{3/4} < n \leq x$$

for some fixed, very large x. Each time n is a square, you win $1.5x^{1/2}$ dollars. Each time it is not, you lose one dollar. Should you accept these bets?

Problem 4.3. let $\zeta(s)$ denote the reiman zeta function then show that coeffecient of $1/n^s$ in $\zeta(s)^k$ equals $d_k(n)$ where $d_k(n)$ denotes the number of ways of writing n as the product of k positive integers (ordering matters)

References

[1] Evan Chen, *OTIS Excerpts*, 2025. Available at https://web.evanchen.cc/textbooks/OTIS-Excerpts.pdf.

[2] Evan Chen, *Orders Modulo A Prime*, 2015. Available at https://web.evanchen.cc/handouts/ORPR/ORPR.pdf.

[3] Mauritz Fasth, Jiachen Mi, Olle Rehnquist, Erik Wettergren, *Quadratic Reciprocity*, 2023. Available at https://static1.squarespace.com/.../Hvitfeldtska_Legendre_symbol.pdf.

[4] M. Overholt, *A Course in Analytic Number Theory*, Graduate Studies in Mathematics, vol. 160, American Mathematical Society, 2015.