Review and Extension: Primes

Andres Buritica

1 Exam review

2 Quadratic residues

Assume there exists a generator mod n. An element $x \in \mathbb{Z}_n^*$ can be written as y^k for $y \in \mathbb{Z}_n^*$ iff $\text{ord}_n(x)\gcd(\varphi(n), k) \mid \varphi(n)$.

If x can be written as y^2 for $y \in \mathbb{Z}_n^*$, then we say that x is a *quadratic residue (QR)* mod n. Note that 0 is not a QR mod n.

Prove that x is a QR mod n iff both

- $x \equiv 1 \pmod{\gcd(8, n)}$, and
- for each odd prime $p \mid n$, x is a QR mod p.

Hence, we now restrict ourselves to considering QRs mod p. Define the *Jacobi symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \text{ is a QR mod } p \\ -1 & \text{otherwise} \end{cases}.$$

- (Euler's criterion) Prove that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Hence, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
- (Gauss' Lemma) Let $a \in \mathbb{Z}_p^*$, and let $S \subseteq \mathbb{Z}_p^*$ such that $x \in S \iff -x \notin S$. Let $T = \{ay : y \in S\}$. Then $\left(\frac{a}{p}\right) = (-1)^{|T \setminus S|}$.
- Find $\left(\frac{2}{p}\right)$ and $\left(\frac{-1}{p}\right)$.
- Find all completely multiplicative functions $f : \mathbb{N} \to \mathbb{R}$ such that for all $a, b \in \mathbb{N}$, at least two of $f(a), f(b), f(a+b)$ are equal.
- (Quadratic Reciprocity) Let p and q be distinct odd primes. Using Gauss' Lemma, prove that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

3 Problems

1. Let p be an odd prime. Prove that
$$p^2 \mid 1^p + 2^p + \cdots + p^p.$$
2. Let a, b, c be positive integers such that $c \mid a^c - b^c$. Prove that $c(a-b) \mid a^c - b^c$.
3. Prove that for all positive integers n,
$$\binom{2n}{n} \mid \text{lcm}(1, 2, \ldots, 2n).$$
4. Find all pairs of positive integers x, p such that p is prime, $x \leq 2p$, and $x^{p-1} \mid (p-1)^x + 1$.

5. Let a, b, n be positive integers such that $a > b > 1$ and b is odd. If $b^n \mid a^n - 1$, prove that $na^b > 3^n$.

6. Find all natural numbers n such that $n^2 \mid 2^n + 1$.

7. Find all positive integers n such that $n \mid 2^n - 1$.

8. Prove that if $\sigma(n) = 2n + 1$, then n is a perfect square.

9. Find all positive integers n such that $n \mid 2^{n-1} + 1$.

10. Find all primes p, q, r such that $p \mid q^r + 1,\ q \mid r^p + 1,\ r \mid p^q + 1$.

11. Let n and m be nonnegative integers, and let p be prime. Prove that

$$\binom{n}{m} \equiv \prod_{i=0}^{k} \binom{n_i}{m_i} \pmod{p},$$

where $n = \sum n_i p^i$ and $m = \sum m_i p^i$.

12. Find all positive integers n for which there exists a function $g : \mathbb{Z}_n \to \mathbb{Z}_n$ such that all the functions

$$g(x), g(x) + x, \ldots, g(x) + 100x$$

are bijections $\mathbb{Z}_n \to \mathbb{Z}_n$.

13. Let k and n be positive integers such that n is odd. Prove that there is an integer a such that $a^{32} \equiv (n+1)^3 \pmod{n^k}$.

14. Prove that for any prime p and positive integer a with $p \nmid a$ there are at least $p - 1$ solutions in $\mathbb{Z}_p$ to $x^2 + y^2 \equiv a \pmod{p}$.

15. Let p be prime and let a and b be positive integers such that $p \nmid b$. Prove that there exists a positive integer n such that $p^a \mid n^n - b$.

16. If $p > 3$ is a prime such that $\varphi(p-1) > \frac{p-1}{3}$, prove that there are two consecutive generators mod p.

17. Let p be a prime and let n be a positive integer with $p \nmid n$. Find

$$\sum_{i=1}^{p} \left(\frac{i^2 + n}{p} \right).$$

18. Let $p > 3$ be a prime and let a, b, c be integers with $a \neq 0$. Suppose that $ax^2 + bx + c$ is a perfect square for p consecutive integers x. Prove that $p \mid b^2 - 4ac$.

19. Let P be a nonconstant polynomial with integer coefficients. Prove that for any integer m there exist an integer n and a prime p such that $p^m \mid P(n)$.

20. Let $a_1, a_2, a_3, \ldots$ be a sequence of integers, such that for any positive integers n and k, the quantity

$$\frac{a_n + a_{n+1} + \cdots + a_{n+k-1}}{k}$$

is always the square of an integer. Prove that all a_is are equal.

4 Homework

Solve and submit any 3 problems from section 3.