Number Theory

James Rickards

Canadian Summer Camp 2015

Quadratic Residue Rules

Let a be an integer, and p an odd prime. Define

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p \\ 0, & \text{if } p \mid a \\ -1, & \text{otherwise} \end{cases}$$

For $n = p_1 p_2 \cdots p_r$ an odd positive integer expressed as a product of distinct primes, we define

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)$$

Note that $\left(\frac{a}{n}\right) = 1$ does not necessarily mean a is a quadratic residue modulo n, merely that it is a non-residue modulo an even number of prime factors of n (with multiplicity).

To calculate quadratic residues, the following rules suffice (m, n are coprime odd positive integers):

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right) \text{ if } a \equiv b \pmod{n} \qquad \left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

$$\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4} \\ -1 & \text{if } n \equiv 3 \pmod{4} \end{cases} \qquad \left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{8} \\ -1 & \text{if } n \equiv \pm 3 \pmod{8} \end{cases}$$

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right)$$

Quadratic Residue Problems

1. Let $p \equiv 1 \pmod{4}$. Prove that the sum of the quadratic residues modulo p in $[1, p-1]$ equals the sum of the non-residues in the interval. Does the same hold when $p \equiv 3 \pmod{4}$?

2. Let p be a prime. Find the value of $\displaystyle\sum_{a=1}^{p-1} \left(\frac{a^2+a}{p}\right)$.

3. Let a be a positive integer which is not a square. Prove that there are infinitely many primes p such that $\left(\frac{a}{p}\right) = -1$.

4. Prove that for all $a \in \mathbb{Z}$, the number of solutions (x, y, z) of the congruence

$$x^2 + y^2 + z^2 = 2axyz \pmod{p}$$

equals $\left(p + \left(\frac{-1}{p}\right)\right)^2$.

5. Let a, b, c be positive integers. Prove that $\dfrac{a^2+b^2+c^2}{3(ab+bc+ca)}$ is not an integer.

6. (New Zealand, 2010) Show that there are infinitely many pairs of distinct primes (p, q) such that $p \mid 2^{q-1}-1$ and $q \mid 2^{p-1}-1$.

7. An odd *composite* positive integer n is called a *strong pseudoprime to base* b for an integer $b > 1$, coprime to n, if $b^{\frac{n-1}{2}} \equiv \left(\dfrac{b}{n}\right) \pmod{n}$. Prove that for every odd composite positive integer n, there exists a base $b > 1$ coprime to n such that n is *not* a strong pseudoprime to base b.

8. (China TST 2003) n is a positive integer which is not a multiple of 2 or 3, and there does not exist nonnegative integers a, b such that $|2^a - 3^b| = n$. Find the minimum possible value of n.

Other Generic Number Theory Problems

1. (Romania TST 2015) Given an integer $k \geq 2$, determine the largest number of divisors the binomial coefficient $\dbinom{n}{k}$ may have in the range $n-k+1, \ldots, n$, as n runs through the integers greater than or equal to k.

2. (Jacob's 2008 Summer Camp handout) Define a_n recursively by $\displaystyle\sum_{d \mid n} a_d = 2^n$. Prove that $n \mid a_n$.

3. (China TST 2008) Let $n > 1$ be an integer, and $n \mid 2^{\phi(n)} + 3^{\phi(n)} + \cdots + n^{\phi(n)}$. Let $p_1, p_2, \ldots, p_k$ be the distinct prime factors of n. Prove that $\dfrac{1}{p_1} + \dfrac{1}{p_2} + \cdots + \dfrac{1}{p_k} + \dfrac{1}{p_1 p_2 \cdots p_k}$ is an integer ($\phi(n)$ is Euler's totient funtion, the number of positive integers at most n which are relatively prime to n).

4. (2015 Iran MO) Let $n \geq 50$ be a natural number. Prove that we can express $n = x + y$, as a sum of two natural numbers x, y such that for every prime number p such that $p \mid x$ or $p \mid y$ we have $\sqrt{n} \geq p$. For example, for $n = 94$, we have $x = 80, y = 14$.

5. (2008 All-Russian) Given a finite set P of primes, prove that there exists a positive integer x such that it can be written in the form $a^p + b^p$ (for positive integers a, b) for each $p \in P$, and it *cannot* be written in that form for each $p \notin P$.