

信息与计算科学导论

Number Theory

221502023 沈硕 第四次作业

Problem 38 [Difficulty Estimate=2.4] Prove Proposition 52 without using induction.

Proposition 52: For any distinct odd numbers $p, q > 1$, suppose f is the permutation on Z_{pq} that maps $aq + b$ to $a + bp$ for every $a \in Z_p, b \in Z_q$. Then, f has the same parity as $\frac{(p-1)(q-1)}{4}$.

Problem 39 [Difficulty Estimate=1.2] Prove Propositions 53 and 54.

Proposition 53: For any positive odd integers n, m and any integers a, b , the Jacobi symbol $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$; the Jacobi symbol $(\frac{a}{nm}) = (\frac{a}{n})(\frac{a}{m})$.

Proposition 54 : For any positive odd integers n , the Jacobi symbol $(\frac{-1}{n}) = 1$ if $n \equiv 1 \pmod{4}$; $(\frac{-1}{n}) = -1$ if $n \equiv 3 \pmod{4}$; the Jacobi symbol $(\frac{2}{n}) = 1$ if $n \equiv \pm 1 \pmod{8}$; $(\frac{2}{n}) = -1$ if $n \equiv \pm 3 \pmod{8}$.

Solution to Proposition 53:

Denote n as $p_1^{k_1} \cdots p_l^{k_l}$, where $p_1 \cdots p_l$ are all odd primes.

$\frac{ab}{n} = (\frac{ab}{p_1})^{k_1} \cdots (\frac{ab}{p_l})^{k_l}$, And as the $(\frac{ab}{p_i})^{k_i}$ can also be a Legendre symbol, so it

can be separated as $((\frac{a}{p_i})(\frac{b}{p_i}))^{k_i}$. Apply this to all $i = 1, 2, \dots, l$ can prove the former one.

For the latter one, denote m as $q_1^{i_1} \cdots q_j^{i_j}$, then by the definition of Jacobi symbol we can similarly reach the proposition.

Solution to Proposition 54:

$(\frac{-1}{n}) = \prod_{i=1}^l (\frac{-1}{x_i})$, $n = x_1 x_2 \cdots x_l \Rightarrow (-1)^{\frac{\prod_{i=1}^l x_i - 1}{2}} = \prod_{i=1}^l (-1)^{\frac{x_i - 1}{2}}$. So $(\frac{-1}{n}) = 1 \Leftrightarrow$ the number of $x_i \equiv 3 \pmod{4}$ is even.

$\Leftrightarrow n \equiv 1 \pmod{4}$. Similar proof to $(\frac{-1}{n}) = -1$ if $n \equiv 3 \pmod{4}$.

If p is a prime, then $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$. Then $(\frac{2}{n}) = (-1)^{\sum_{i=1}^l k_i \frac{p_i^2-1}{8}}$

So $(\frac{2}{n}) = 1 \Leftrightarrow$ the number of $p_i \equiv \pm 3 \pmod{8}$ is even. $\Leftrightarrow n \equiv 1 \pmod{4}$.

Similar proof to $(\frac{2}{n}) = -1$ if $n \equiv \pm 3 \pmod{8}$.

Problem 40 [Difficulty Estimate=1.2] Read another proof of Gauss quadratic reciprocity. For example, you may consider reading the original proof by Gauss, or the famous alternative proof by Einstein.

Solution: I have read it..??

Problem 41 [Difficulty Estimate=1.8] Suppose a is a positive integer but not a perfect square (i.e., not equal to the square of any integer). Prove that there exist infinitely many primes p such that $(\frac{a}{p}) = -1$