MA2316: Introduction to Number Theory
Tutorial problems for February 13, 2014

"Around the quadratic reciprocity"

Let n be an odd number, and let $n = p_1 p_2 \cdots p_k$ be its prime decomposition (possibly with repeated factors). Let us define the *Jacobi symbol* $\left(\frac{a}{n}\right)$ by the formula

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).$$

1. Give an example of a and n for which $\left(\frac{a}{n}\right) = 1$ but a is not congruent to a square modulo n.

2. Show that for Jacobi symbols we have $\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)$ and $\left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right) = \left(\frac{a}{n_1 n_2}\right)$ whenever n, n_1, n_2 are odd.

3. Show that if m and n are odd integers, then $\frac{mn-1}{2} \equiv \frac{m-1}{2} + \frac{n-1}{2} \pmod 2$. Explain why it implies that for each odd n we have $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

4. Show that for any two coprime odd integers m, n we have $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$.

5. Applying previous problem with $m = n + 2$, show that for each odd n we have $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

6. Show that all prime divisors of $9n^2 + 3n + 1$ are of the form $3k + 1$.

7. Let p be an odd prime number.

(**a**) Show that the function $k \mapsto \frac{1-k}{1+k}$ maps the set $(\mathbb{Z}/p\mathbb{Z}) \setminus \{-1\}$ to itself and is a 1-to-1 correspondence.

(**b**) Compute the sum

$$\sum_{k=0}^{p-1} \left(\frac{k}{p}\right).$$

8. Find the number of solutions to the equation $x^2 + y^2 = 1$ in $\mathbb{Z}/p\mathbb{Z}$. (*Hint*: this number is equal to $\sum_{y=0}^{p-1}(1 + \left(\frac{1-y^2}{p}\right))$).