MATH 3070 – THEORY OF NUMBERS

Homework 4

Due: Thursday, Oct 20, 2022 (in class)

1. Let $p \geq 3$ be a prime.

(i). Prove that for any integers a and b such that $a \equiv b \pmod{p}$,

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

(ii). Prove that

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

Further, if $\{a_1, \ldots, a_{p-1}\}$ is a reduced system modulo p, prove that

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

(iii). Let $R := \{1 \leq a \leq p-1 : a \text{ is a quadratic residue modulo } p\}$ and $N := \{1 \leq a \leq p-1 : a \text{ is a quadratic non-residue modulo } p\}$. Determine R and N when $p = 13$. (*Give your answer directly. No need to present detailed calculations.*)

(iv). Define

$$\begin{aligned} RR &:= \{1 \leq a \leq p-\mathbf{2} : a \in R \text{ and } a+1 \in R\}, \\ RN &:= \{1 \leq a \leq p-\mathbf{2} : a \in R \text{ and } a+1 \in N\}, \\ NR &:= \{1 \leq a \leq p-\mathbf{2} : a \in N \text{ and } a+1 \in R\}, \\ NN &:= \{1 \leq a \leq p-\mathbf{2} : a \in N \text{ and } a+1 \in N\}. \end{aligned}$$

Determine RR, RN, NR and NN when $p = 13$. (*Give your answer directly. No need to present detailed calculations.*)

(v). Prove that for $1 \leq a \leq p-2$,

$$\left(\left(\frac{a}{p}\right)+1\right)\left(\left(\frac{a+1}{p}\right)+1\right) = \begin{cases} 4 & \text{if } a \in RR, \\ 0 & \text{if } a \notin RR. \end{cases}$$

(vi). Prove that the cardinality of RR is given by

$$|RR| = \frac{1}{4}\left(p - 3 - \left(\frac{-1}{p}\right) + \sum_{a=1}^{p-2}\left(\frac{a^2+a}{p}\right)\right).$$

(vii). Prove that

$$\sum_{a=1}^{p-2}\left(\frac{a^2+a}{p}\right) = -1$$

and conclude that

$$|RR| = \frac{p - 4 - \left(\frac{-1}{p}\right)}{4}.$$

(*Hint: Prove first that for* $1 \leq a \leq p-2$, $\left(\frac{a^2+a}{p}\right) = \left(\frac{1+a^{-1}}{p}\right)$ *where* a^{-1} *is the modular inverse of* $a \bmod p$.)