Homework #5. Solutions to selected problems.

For solutions to the remaining problems see Solutions to HW#7 and HW#8 on Spring 2014 webpage.

2. Let p be an odd prime, and consider a congruence $ax^2 + bx + c \equiv 0 \mod p$ where $p \nmid a$. Prove the number of reduced solutions to this congruence is equal to $1 + \left(\frac{b^2-4ac}{p}\right)$.

Solution: Since $p \nmid a$ and p is odd, we have $gcd(p, 4a) = 1$, so by the first cancellation law the given congruence is equivalent to $4a^2x^2 + 4abx + 4ac \equiv 0 \mod p$. Multiplication by $4a$ allows us to complete the square: $4a^2x^2 + 4abx + 4ac \equiv 0 \mod p \iff (2ax + b)^2 + (4ac - b^2) \equiv 0 \mod p \iff (2ax + b)^2 \equiv b^2 - 4ac \mod p$. By definition of Legendre symbol the number of reduced solutions to the congruence $y^2 \equiv b^2 - 4ac \mod p$ is equal to $1 + \left(\frac{b^2-4ac}{p}\right)$. And since $gcd(p, 2a) = 1$, by the theory of linear congruences, for any $y \in \mathbb{Z}$ the congruence $2ax + b \equiv y \mod p$ has unique reduced solution (for x). Thus, the congruence $(2ax + b)^2 \equiv b^2 - 4ac \mod p$ also has $1 + \left(\frac{b^2-4ac}{p}\right)$ reduced solutions.

3. Compute the Legendre symbols $\left(\frac{331}{113}\right)$ and $\left(\frac{319}{107}\right)$.

(a) Since $331 = 113 \cdot 2 + 105$ and $105 = 3 \cdot 5 \cdot 7$, we have $\left(\frac{331}{113}\right) = \left(\frac{105}{113}\right) = \left(\frac{3}{113}\right)\left(\frac{5}{113}\right)\left(\frac{7}{113}\right)$

Using quadratic reciprocity and the formula for $\left(\frac{2}{p}\right)$, we have $\left(\frac{3}{113}\right) = \left(\frac{113}{3}\right) = \left(\frac{2}{3}\right) = -1$, $\left(\frac{5}{113}\right) = \left(\frac{113}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$, $\left(\frac{7}{113}\right) = \left(\frac{113}{7}\right) = \left(\frac{1}{7}\right) = 1$.

Hence $\left(\frac{331}{113}\right) = (-1) \cdot (-1) \cdot 1 = 1$.

(b) Since $319 = 107 \cdot 2 + 105$ and $105 = 3 \cdot 5 \cdot 7$, we have $\left(\frac{319}{107}\right) = \left(\frac{105}{107}\right) = \left(\frac{3}{107}\right)\left(\frac{5}{107}\right)\left(\frac{7}{107}\right)$

Using quadratic reciprocity and the formula for $\left(\frac{2}{p}\right)$, we have $\left(\frac{3}{107}\right) = -\left(\frac{107}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$, $\left(\frac{5}{107}\right) = \left(\frac{107}{5}\right) = \left(\frac{2}{5}\right) = -1$, $\left(\frac{7}{107}\right) = -\left(\frac{107}{7}\right) = -\left(\frac{2}{7}\right) = -1$.

Hence $\left(\frac{331}{113}\right) = 1 \cdot (-1) \cdot (-1)$.