MATH 3070 – THEORY OF NUMBERS

Homework 6

Due: Tuesday, Nov 29, 2022 (in class)

1. Let $p \geq 5$ be an odd prime.

(i). Prove that -3 is a quadratic residue modulo p if $p \equiv 1 \pmod{6}$, and a quadratic non-residue modulo p if $p \equiv 5 \pmod{6}$.

(*Hint: Use the fact that* $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$, *and apply the criteria for* $\left(\frac{-1}{p}\right)$ *and* $\left(\frac{3}{p}\right)$ *in Sects. 6.4 & 7.4.*)

(ii). Prove that if $p \equiv 5 \pmod{6}$, then we **cannot** find integers x and y such that $p = x^2 + 3y^2$.

(*Hint: Prove by contradiction. Assume that there exist* x *and* y *such that* $p = x^2 + 3y^2$. *First prove that* $p \nmid x$ *and* $p \nmid y$. *Then apply Part (i).*)

(iii). Prove that if $p \equiv 1 \pmod{6}$, then there exists an integer x such that

$$x^2 + 3 = mp$$

with $0 < m < p$.

(*Hint: Mimic the proof of Theorem 6.9.*)

(iv). Prove that

$$(x_1^2 + 3y_1^2)(x_2^2 + 3y_2^2) = (x_1x_2 + 3y_1y_2)^2 + 3(x_1y_2 - x_2y_1)^2.$$

(v). Prove that if $p \equiv 1 \pmod{6}$ and x and y are integers such that $x^2 + 3y^2 = mp$ with m an integer, then either m is odd, or m is a multiple of 4. In particular, $m \neq 2$.

(*Hint: Consider the parity of* x *and* y.)

(vi). Prove that if $p \equiv 1 \pmod{6}$, then we **can** find integers x and y such that $p = x^2 + 3y^2$.

(*Hint: First deduce from Part (iii) that there exists an integer* m *with* $0 < m < p$ *such that the equation* $x^2 + 3y^2 = mp$ *has an integer solution* (x, y). *Then consider the two cases: (1).* $(x, y) > 1$; *(2).* $(x, y) = 1$. *For Case (1), prove that* $d^2 \mid m$ *where* $d = (x, y)$. *For Case (2), mimic the* ***first*** *proof of Theorem 8.2.*)