Primes - Problem Sheet 3

Quadratic residues and quadratic reciprocity

Q1) Use (the supplements to) Quadratic Reciprocity to find congruence conditions on p such that $\left(\frac{-2}{p}\right) = 1$. This gives an alternate proof of the *Reciprocity* step for $p \mid x^2 + 2y^2$. How does this compare with Problem Sheet 2, Question 6?

Q2) Find congruence conditions on p such that $\left(\frac{a}{p}\right) = 1$ for

i) $a = \pm 5$,

ii) $a = \pm 7$,

iii) $a = \pm 6$,

iv) $a = \pm 10$,

v) $a = \pm 21$.

Hence state the corresponding *Reciprocity* steps for these $x^2 + ny^2$, in these cases.

Q3) (Easy cases of Dirichlet's theorem on primes in arithmetic progressions)

i) By directly imitating Euclid's classical proof that there are infinitely many primes, show that there are infinite many primes $p \equiv 3 \pmod 4$. Hint: consider $N_k = 2^2 p_1 p_2 \dots p_k - 1$, where $p_1 = 3, p_2 = 7, \dots$ are the primes of the form $4n + 3$.

ii) By using Lemma 3.8, with $n = 1$, adapt the above proof, to show there are infinitely many primes $p \equiv 1 \pmod 4$.

iii) Show that there are infinitely many primes $p \equiv 1 \pmod 3$ and infinitely many primes $p \equiv 2 \pmod 3$.

Q4) (Primes of the form $x^2 - 2y^2$)

i) Show directly that the descent step holds for $x^2 - 2y^2$.

ii) Use quadratic reciprocity to determine when $p \mid x^2 - 2y^2$.

iii) Give a condition on when a prime $p = x^2 - 2y^2$.

Q5) In this exercise you will evaluate $\left(\frac{2}{p}\right)$ in a different way, using Euler's criterion. Consider $(\mathbb{Z}/p\mathbb{Z})$, and suppose we extend it to $F = (\mathbb{Z}/p\mathbb{Z})[\zeta_8]$ which includes (the image of) $\zeta_8 = e^{2\pi i/8}$, a primitive 8-th root of 1. Then any element $x \in F$ can be written

$$x \equiv \sum_{i=0}^{7} a_i \zeta_8^i \pmod p,$$

with addition and multiplication given in the 'natural ways' using the rule $\zeta_8^8 = 1$. (Similar to $\mathbb{C} = \mathbb{R}[i]$, where we write element $x \in \mathbb{R}[i]$ as $x = a + bi$, and use the rule $i^2 = 1$.)

i) Write $\tau = \zeta_8 + \zeta_8^{-1} = \zeta_8 + \zeta_8^7$. Show that $\tau^2 = 2$, hence using Euler's criterion, show
$$\tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod p .$$

ii) Using the binomial theorem, show that
$$\tau^p \equiv \zeta_8^p + \zeta_8^{-p} \pmod p$$

iii) For $p \equiv \pm 1, \pm 3 \pmod 8$, evaluate τ^p, and check the result can be written as
$$\tau^p = (-1)^{(p^2-1)/8}\tau \pmod p$$

iv) Conclude that
$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} .$$