Number Theory 2013

Problem Sheet 2

1. Verify that 5 is the least positive primitive root of 73, and 3 is the least positive primitive root of 199.
2. If n has a primitive root then it has $\phi(\phi(n))$ of them.
3. Compute the order of all elements in $(\mathbb{Z}/13\mathbb{Z})^\times$ and check that your answer agrees with Lemma 4.2 and Question 2 above.
4. Let p be a prime. Show that every element in $\mathbb{Z}/p\mathbb{Z}$ can be written as the sum of two squares.
   [Hint: Do the non-zero sums of two squares in $\mathbb{Z}/p\mathbb{Z}$ form a multiplicative group?]
5. Prove that there exists solutions for the equation

$$x^2 \equiv 251 \quad (\mod 779).$$

   [*Note that* $779 = 19 \cdot 41$.]
6. Does the equation $x^2 + 10x + 15 \equiv 0 \quad (\mod 45083)$ have any solutions?
7. Prove that there are infinitely many primes of the form $p = 8k - 1$.
8. Use the Fermat Method to factorize 119143.
   [Hint: $345^2 < 119143 < 346^2$ *and* $4761 = 69^2$*.]*
9. Suppose that the cipher-text message produced by RSA encryption, with exponent $e = 5$ and modulus $n = 2881$, is

0504 1874 0347 0515 2088 2356 0736 0468.

   What is the plain-text message?

UT