Number Theory 2013

Problem Sheet 1

1. Prove Lemma 1.3.: The greatest common factor of two integers can be written as an integral combination of the two integers.

2. Adapt Euclid's proof for the fact that there are infinitely many primes to show that there are infinitely many primes of the form $4k-1$.
[Hint: Show that for a prime $p > 2$ either $p \equiv 1 \pmod 4$ or $p \equiv -1 \pmod 4$; and if $a \equiv 1$ and $b \equiv 1$ then $ab \equiv 1 \pmod 4$.]

3. Adapt Euclid's proof for the fact that there are infinitely many primes to show that there are infinitely many primes of the form $6k-1$.
[Hint: Show the corresponding statements as in the hint for Problem 2.]

4. Let a be a positive integer and suppose that in its decimal expansion it has 6 digits: $a = a_0 + 10a_1 + \cdots + 100000a_5$. Show that a is divisible by 7 if and only if $a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5$ is divisible by 7. Can this be generalized?

5. Solve the simultaneous linear congruences
$$x \equiv 3 \pmod 4), \quad 2x \equiv 5 \pmod 9), \quad 7x \equiv 1 \pmod{11}.$$

6. List the elements of $(\mathbb{Z}/30\mathbb{Z})^x$ and compute the multiplicative inverse for each of them.

7. Show that Euler's totient function is multiplicative: If $(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.

8. Let m and n be coprime integers. For any integer a, how are the integer solutions of the equation $x^2 = a \pmod{mn}$ related to the integer solutions of the simultaneous equations
$$x^2 = a \pmod m \quad \text{and} \quad x^2 = a \pmod n?$$

9. Let p be an odd prime and let $a \in \mathbb{Z}$. Use primitive roots to find conditions on p and a which ensure that there exists solutions in $\mathbb{Z}$ for
$$x^3 \equiv a \pmod p.$$
Illustrate your answer with the examples $p = 17$ and $p = 19$.

UT