Number Theory – Problem Sheet 1

1. Calculate $d = (a, b)$ and find integers x, y such that $d = ax + by$ when (i) $a = 841, b = 160$, (ii) $a = 2613, b = 2171$, and (iii) $a = 8991, b = 3293$.

2. Let a, b be positive integers with $a > b > 1$. Let $\lambda(a, b)$ denote the number of individual applications of the Euclidean algorithm required to compute $d = (a, b)$. Prove that

$$\lambda(a, b) \leq 2\left[\frac{\log b}{\log 2}\right].$$

N.B. If x is in $\mathbb{R}$, define $[x]$ to be the largest integer $\leq x$.

3. Let a be an integer ≥ 2, and n an integer ≥ 2. If $a^n - 1$ is prime, prove that $a = 2$ and n is a prime.

4. We say a natural number n is <u>perfect</u> if the sum of all positive divisors of n is equal to $2n$. Prove that an even integer $n \geq 2$ is perfect if and only it can be written in the form $n = 2^{q-1}(2^q - 1)$, where $2^q - 1$ is a prime.
(It is conjectured that there are no odd perfect numbers n, and this has been verified numerically for $n \leq 10^{300}$).

5. Find the smallest non-negative integer x satisfying the congruences

$$x \equiv 2 \bmod 3,\ x \equiv 3 \bmod 5,\ x \equiv 4 \bmod 11,\ x \equiv 5 \bmod 16.$$

6. Find the smallest non-negative integer x satisfying

$$19x \equiv 103 \bmod 900, \quad 10x \equiv 511 \bmod 841.$$

7. Prove that the classes of both 2 and 3 generate $(\mathbb{Z}/5^n\mathbb{Z})^\times$ for all integers $n \geqslant 1$. Find a generator of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for all $n \geqslant 1$ when $p = 11, 13, 17$.

8. Suppose a, n are integers with $a \geqslant 2$, $n \geqslant 1$, and put $N = a^n - 1$. Show that the order of $a + N\mathbb{Z}$ in $(\mathbb{Z}/N\mathbb{Z})^\times$ is exactly n, and deduce that n divides $\varphi(N)$. If n is a prime, conclude that there exist infinitely many primes q such that $q \equiv 1 \bmod n$.

9. Let A be the group $(\mathbb{Z}/65520\mathbb{Z})^\times$. Determine the least positive integer n such that $g^n = 1$ for all g in A.

10. Let q be an odd prime. Prove that every prime factor of $2^q - 1$ must be congruent to $1 \bmod q$, and also $\equiv \pm 1 \bmod 8$. Use this general fact to factor $2^{11} - 1 = 2047$.