Number Theory - Problem Sheet 1.

Notation. If x is in $\mathbb{R}$, $[x]$ = largest integer $\leq x$.

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

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

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

3. If x is an integer ≥ 2, use the fundamental theorem of arithmetic to show that

$$x \leq \left(1 + \frac{\log x}{\log 2}\right)^{\pi(x)}.$$

Deduce that, when $x \geq 8$, we have $\pi(x) \geq \dfrac{\log x}{2 \log\log x}$.

4. Let a, n be integers ≥ 2. If $a^n - 1$ is prime, prove that $a = 2$ and n is a prime.

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

6. We say a natural number n is perfect 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 if it can be written in the form $n = 2^{q-1}(2^q - 1)$, where $2^q - 1$ is prime. It is conjectured, but unknown, that there are no odd perfect numbers.

7. By considering numbers of the form

$$n = 2^2 \cdot 3 \cdot 5 \ldots p - 1,$$

prove that there exist infinitely many primes congruent to 3 mod 4.

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

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

9. Find the smallest non-negative integer x satisfying $19x \equiv 103 \bmod 900$, $10x \equiv 511 \bmod 841$.

10. Prove that the classes of both 2 and 3 generate $(\mathbb{Z}/5^n\mathbb{Z})^\times$ for all integers $n \geq 1$. Find a generator of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for all $n \geq 1$ when $p = 11, 13, 17, 19$.

11. 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.

12. Suppose a, n are integers ≥ 2, 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, deduce that there exist infinitely many primes q such that $q \equiv 1 \bmod n$.