ECM3704 NUMBER THEORY **EXERCISE SHEET 1**[1]

This sheet does **not** count towards assessment.

1. Remind yourself of the Sieve of Eratosthenes, or look it up if you are unfamiliar with it. Use it to find all primes up to 200. (If you like programming, write a programme to find all primes up to 1000 or beyond!)

2. For each pair a, b use the Extended Euclidean Algorithm to find $d = \gcd(a, b)$ and integers x, y such that $d = ax + by$:
(i) $a = 34$, $b = 20$;
(ii) $a = 55$, $b = 34$;
(iii) $a = 1105$, $b = 208$.
(Again, if you like programming, write a programme to implement the extended Euclidean algorithm, and try it on some really large numbers.)

3. Let a, $b \in \mathbb{N}$ and let $d = \gcd(a, b)$. Set $l = ab/d$. Show that l is *least common multiple* (lcm) of a and b, denoted by $[a, b]$, in the sense that the following two properties hold:

(i) $a \mid l$ and $b \mid l$; (ii) if $a \mid m$ and $b \mid m$ then $l \mid m$.
(You might find Euclid's Lemma useful.)

Show also that l is the unique positive integer with these properties.

4.
(i) Prove that $4 \nmid (n^2 + 2)$ for any integer n.

(ii) Prove that $a \mid bc$ if and only if $\frac{a}{(a,b)} \mid c$.

5. Find the prime factorisations of the following numbers:
(i) 60 (ii) 105; (iii) 65536.
For each of these numbers n, write down $v_p(n)$ for *all* primes p.
(Recall that $v_p(n)$ means the integer e such that $p^e \mid n$ but $p^{e+1} \nmid n$.)

6. Prove that if a positive integer m is not a perfect square, then $\sqrt{m}$ is irrational.
(Remember that a perfect square is an integer that is the square of an integer)

[1] For simplicity, at some points, we will denote the $\gcd(a, b)$ by (a, b).

7. Prove that there are arbitrarily large gaps in the sequence of primes. Stated otherwise, let $n \in \mathbb{N}$. Show that there exist n consecutive composite numbers.
[Hint: Consider $(n+1)! + k$ for $2 \leq k \leq n+1$.]

8.

(i) Prove that there are infinitely many primes of the form $4x - 1$.
[Hint: Recall the proof of the infinitude of primes given in the lecture notes]

(ii) Prove that the least prime factor p of a composite number n satisfies $p \leq \sqrt{n}$

(iii) *Prove that an odd integer $n > 1$ is a prime if and only if it is not expressible as a sum of three or more consecutive positive integers.