Elementary Number Theory and Cryptography, Michaelmas 2014

Problem Sheet 2, (Due: Monday Nov 3, at 12:00 in CM116)

Please hand in problems 2, 6, 8, 9(b), 10.
Problems 1, 7, 9(a,c), 11 will be discussed in the tutorials, (depending on time).

1. Show that there are arbitrarily long sequences of *composite* integers. In other words: for any $k \in \mathbb{Z}$, $k > 1$, show that there is an $n \in \mathbb{Z}$ such that *none of* $n+2, n+3, \ldots, n+k$ is prime.

   [Hint: You may want to choose n to have many divisors... (the seemingly strange beginning of the sequence (i.e. $n+2$) may give you another hint)]

2. Prove that a composite number a will always have a prime divisor p satisfying $p \leq \sqrt{a}$.

3. Prove that among any 10 concecutive positive integers at least one is relatively prime to the product of all the others.

4. Let p be a prime number. Prove that $\sqrt{p}$ is not a rational number.

5. Let p_n denote the n^{th} of the prime numbers in their natural order. Show that

   (a) $p_{n+1} \leq p_1 p_2 \ldots p_n + 1$

   (b) $p_{n+1} \leq 2^{2^n}$

   (c) For $n \geq 1$ there are at least $n+1$ primes less than 2^{2^n}.

6. (a) Show that a prime of the form $3n+1$ is necessarily of the form $6n+1$.

   (b) Prove that any positive integer of the form $3n+2$ has a prime factor of that same form. Using this, or otherwise, show that there are infinitely many primes of the form $3n+2$.

7. (a) Find an integer n for which $n/2$ is a square and $n/3$ is a cube.
   [Hint: Characterise a square/cube via its prime factorization exponents.]

   (b) Among the integers n satisfying the conditions of (a), find one for which $n/5$ is a fifth power (of some integer, of course).

8. (The *Sieve of Eratosthenes*)
   Obtain a complete list of all the primes between 1 and n with $n = 100$, by the following method: by a **proper multiple** of the integer k we understand the positive multiples of k except k itself. First write down all numbers from 2 to 100, in a conveniently tabled form. Then cross out all the *proper multiples* of 2, then cross out all the proper multiples of the next prime 3, then the proper multiples of 5, etc. Note that at each stage the next remaining number is a prime (why?). Repeat this process up to the proper multiples of 7.

   (i) What is the next remaining number (> 7) in the list?

(ii) Why are all the remaining numbers in the list primes? (Question 2 may be helpful).

9. (a) Show that $n^4 + 4$ is composite for all $n > 1$.

   (b) Show that if $2^n - 1$ is a prime then necessarily n is prime as well.
   [Primes of the form $2^n - 1$ are called **Mersenne primes**.]

   (c) A number is called **perfect** if it equals the sum of all its (positive) divisors other than itself. For example, the number 6 is perfect (its divisors other than itself are 1, 2 and 3, and $6 = 1 + 2 + 3$).
   Show that $\frac{a(a+1)}{2}$ is a perfect number if a is a Mersenne prime (cf. (b)).
   [Hint: It may help to group its divisors into two suitable sets.]
   Using this, give two other perfect numbers.

10. For two integers a and b we define the least common multiple of a and b as

$$\mathrm{lcm}(a, b) := \min\{d \in \mathbb{N} \ : \ a|d, \ b|d, \}.$$

    Show that for positive integers a and b we have $\gcd(a, b)\mathrm{lcm}(a, b) = ab$.

11. Denote by $\gcd(a, b, c)$ the greatest common divisor of three numbers $a, b, c \in \mathbb{N}$ and by $\mathrm{lcm}(a, b, c)$ their least common multiple:

$$\gcd(a, b, c) := \max\{d \in \mathbb{Z} \ : \ d|a, \ d|b, \ d|c\};$$

$$\mathrm{lcm}(a, b, c) := \min\{d \in \mathbb{N} \ : \ a|d, \ b|d, \ c|d\}.$$

    (a) Prove that $\gcd(a, b, c) = \gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.

    (b) Prove that $\mathrm{lcm}(a, b, c) \cdot \gcd(ab, bc, ca) = abc$.