Elementary Number Theory and Cryptography,
Michaelmas 2011, Problem Sheet 3. (Primes and Factorization)

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. (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 $3n+2$.
3. (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).
4. (The *Sieve of Eratosthenes*)
   Obtain a complete list of all the primes between 1 and n with $n = 200$, 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 200 (or let the computer do it for you), 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 13.
   (i) What is the next remaining number (> 13) in the list?
   (ii) Why are all the remaining numbers in the list primes? (A lemma from the lectures may be helpful here.)

5*. (a) Show that $n^4 + 4$ is composite for all $n > 1$. [Look for a "unifying" reason.]
   (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.

6. (*Problems involving computers:*)
   (a) Check that $n^2 - 81n + 1681$ is a prime for $n = 1, 2, \ldots, 60$. Is it always prime? Give a proof or find a counterexample. [Note that this shows again that one needs to be cautious with too rash statements about primes.]
   (b) Using GP-PARI or MAPLE (or otherwise), compare the (number of) primes in the intervals $[10^7 - 100, 10^7]$ and $[10^7, 10^7 + 100]$. How many primes are there below 10^7? What number would you (roughly) expect from the Prime Number Theorem? (Here are some useful commands:)

GP-PARI	MAPLE	functionality
`isprime(n)`	`isprime(n);`	checks if n is prime;
`nextprime(n+1)`	`nextprime(n);`	gives the next prime after n;
`prime(n)`	`ithprime(n);`	gives the nth prime;
`primepi(x)`	`numtheory[pi](x);`	prime counting function $\pi(x)$