Elementary Number Theory and Cryptography,
Michaelmas 2011, Problem Sheet 2 (divisibility, Euclidean algo).

1. Show the following statements for integers a, b, c:
   (a) If $\gcd(a,b)=1$ and $\gcd(a,c)=1$ then $\gcd(a,bc)=1$.
   [Hint: write the gcd's explicitly in terms of the input data.]
   (b) If $\gcd(a,b)=1$ then $\gcd(a^2,b^2)=1$.
   [Hint: first determine $\gcd(a,b^2)$.]
   (c) If $a \mid bc$ then $a \mid \gcd(a,b)\gcd(a,c)$.

2. In each of the following, decide whether the statement is true or false for *positive* integers a, b, c, and give either a proof or a counterexample.
   (a) If $ab \mid ac$ then $b \mid c$.
   (b) If $b^2 \mid c^3$ then $b \mid c$.
   (c) $\gcd(a,b)^2 = \gcd(a^2,b^2)$.

3. (a) Show that, for any *odd* number b, one has $8 \mid b^2-1$.
   (b) Is the relation $\nmid$ ("does not divide") transitive? (Justify your answer.)
   (c) The well-known Fibonacci sequence $\{F_n\}_{n\geqslant 0}$ is defined as follows: $F_0=1$, $F_1=1$, and, for any index $n\geqslant 2$, $F_n=F_{n-1}+F_{n-2}$. Prove that the gcd of each pair of *consecutive* Fibonacci numbers equals 1.

4. Devise the following variant of the Euclidean algorithm: given integers a, b, define the *"closest integer"* of a/b to be the number q for which one has $-\frac{1}{2} < \frac{a}{b} - q \leqslant \frac{1}{2}$.
   (a) Show that q is indeed uniquely defined by this.
   (b) Define r as the *remainder* $a-bq$ and determine the interval in which r lies.
   (c) Show that $\gcd(a,b)=\gcd(b,r)$.
   (d) Show also that a successive application of the above process has to terminate and also that it computes the gcd of a and b.

5. For a, b positive integers consider the set $S(a,b) := \{ax+by \mid x,y\in\mathbb{Z}\}$ of all integer linear combinations of a and b.
   (a) Show that $\gcd(a,b)$ is the smallest positive element in this set.
   [Hint: show first that this smallest positive integer *divides* $\gcd(a,b)$, and then show the converse.]
   (b*) Suppose you are given integers x_0 and y_0 satisfying the identity $\gcd(a,b)=ax_0+by_0$ (why can you assume that they exist?).
   i) Give infinitely many (different) pairs (x,y) of integers, in terms of x_0, y_0, a and b, which satisfy $\gcd(a,b)=ax+by$.
   ii) Can you find a complete set of such pairs?

6. Let a, b and n be positive integers.
   (a) Show that we have
   $$\gcd(an,bn) = n\cdot\gcd(a,b).$$
   [Hint: you can use the results of the previous question; or else use induction on the size of $a+b$.]
   (b) Using the above statement, prove that if $n\mid a$ and $n\mid b$ then $n\mid\gcd(a,b)$.

7. (a) Find a factorisation of 4153076928 into primes "by hand".
   (b) Find a factorisation of 1030301 using "pure thought".
   (c) Can you find one for the non-prime 4294049777 ? (A calculator is probably not good enough!)