Elementary Number Theory and Cryptography,
Michaelmas 2011, Problem Sheet 1 (induction, divisibility).

1. Establish the following formulae for any positive integer n, using mathematical induction:
$$1+3+5+\cdots+(2n-1) = n^2\,, \tag{1}$$
$$1^3+2^3+3^3+\cdots+n^3 = \left(\frac{n(n+1)}{2}\right)^2, \tag{2}$$
$$1^3-2^3+3^3-\cdots-(2n)^3+(2n+1)^3 = (n+1)^2(4n+1)\,. \tag{3}$$
Deduce from these that each cube is the difference of two squares.

2. Prove by induction that, for $n \geqslant 1$, one has
   (a) 8 divides $5^{2n}+7$;
   (b) $13 \mid 4^{2n+1}+3^{n+2}$;
   (c) $5 \mid 3^{3n+1}+2^{n+1}$.

3. Recall the *distributive law* for the integers: for any integers a, b, c, we have
$$a(b+c) = ab+ac\,.$$
Use the distributive law to deduce the relation $(-1)\cdot(-1) = +1$.

4. Let a, b, c be integers, where $c \neq 0$. Show that
   (a) if $c \mid a$ then $c \mid a \cdot b$,
   (b) if $c \mid a$ and $c \mid b$ then $c \mid ma+nb$ for any integers m, n.
   (c) if $a \mid b$ and $b \mid a$, then $a = \pm b$ (i.e. $a = b$ or $a = -b$).

5. Show that, for any positive integers a and n one has
   (a) the following divisibility (be careful not to divide by 0)
$$a-1 \mid a^n-1\,,$$
   (b) and, keeping the above in mind, show that for $a > 1$
$$\gcd\left(\frac{a^n-1}{a-1}, a-1\right) = \gcd(a-1, n)\,.$$
[Hint: It may help to view a first as an indeterminate.]

6. (a) Compute the greatest common divisor $d = (455, 1235)$ of the two numbers 455 and 1235 by hand. Find integers x, y such that $d = 455x+1235y$.
   (b) Compute the greatest common divisor $d = (2743, 3587)$ of the two numbers 2743 and 3587 by hand. Find integers x, y such that $d = 2743x+3587y$.

7. For $n \geqslant 0$, let $F_n = 2^{2^n}+1$, the n-th *Fermat number.*
Show that $(F_n, F_{n-1}) = 1$ for *any* n.
[Hint: Try to find factors of the expression $F_n - 2$.]
More generally, show that $(F_n, F_k) = 1$ for *any* k such that $n \neq k$.

8*. (a) Show that, for any integers a, b, c, d, one has that
$$12 \;\Big|\; (a-b)(a-c)(a-d)(b-c)(b-d)(c-d)\,.$$
[Hint: show that both 3 and 4 divide the right hand side.]
   (b) Prove that among any 10 consecutive positive integers at least one is relatively prime to the *product of* all the others.