Elementary Number Theory and Cryptography, Michaelmas 2014

Problem Sheet 1, (Due: Monday Oct 20, at 12:00 in CM116)

Please do problems 1(a), 3, 5(b), 8.

1. Establish the following formulae for any positive integer n, using mathematical induction:

   (a) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$.
   Deduce that each cube is the difference of two squares.

   (b) $1^3 - 2^3 + 3^3 - \ldots - (2n)^3 + (2n+1)^3 = (n+1)^2(4n+1)$.

2. Prove by induction that, for integer $n \geq 1$, one has

   (a) $13 \mid 4^{2n+1} + 3^{n+2}$;

   (b) $5 \mid 3^{3n+1} + 2^{n+1}$.

3. Let a, b, c be integers, where $c \neq 0$. Show that

   (a) if $c \mid a$ and $c \mid b$ then $c \mid ma + nb$ for any integers m, n.

   (b) if $a \mid b$ and $b \mid a$, then $a = \pm b$ (i.e. $a = b$ or $a = -b$).

4. 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) $\gcd(a,b)^2 = \gcd(a^2, b^2)$.

   (d) If $a \nmid b$ and $b \nmid c$ then $a \nmid c$ (recall that $a \nmid b$ means that a does not divide b).

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

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

6. Let a, b and n be positive integers.

   (a) Show that we have
   $$\gcd(an, bn) = n \cdot \gcd(a, b).$$

   (b) Using the above statement, prove that
   if $n \mid a$ and $n \mid b$ then $n \mid \gcd(a, b)$.

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

8. The well-known Fibonacci sequence $\{F_n\}_{n\geq 0}$ is defined as follows: $F_0 = 1$, $F_1 = 1$, and, for any index $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. Prove that the gcd of each pair of *consecutive* Fibonacci numbers equals 1.

   [Hint: Try to use induction.]

9. Show that, for any positive integers $a > 1$ and n one has

   (a)
   $$a - 1 \mid a^n - 1\,,$$

   (b)
   $$\gcd\left(\frac{a^n - 1}{a - 1}, a - 1\right) = \gcd(a - 1, n)$$

   [Hint: It may help to view a first as an indeterminate.]

10. (a) Show that the product of any two consecutive integers is even.
    (b) Show that, for any *odd* number b, one has $8 \mid b^2 - 1$.