Topics in Number Theory - 1st exercise sheet

Alex Bartel

October 12, 2012

Always carefully justify your assertions. In particular, "yes" or "no" is never going to be a sufficient answer.

The deadlines for the sheet are Oct 8, Oct 15, and Oct 18.

1. (a) Show that for any positive integer n, $3 \mid (2^{2n} - 1)$.
   (b) For what positive integers n does $15 \mid (2^{2n} - 1)$?
   (c) (optional) You have a checkered board of $2^n \times 2^n$ squares, you have one coin that exactly covers one square, and a large supply of corner pieces that cover three squares each. Can you always tile the whole board with one coin and the corner pieces with no overlaps and nothing sticking out?
   (d) (optional) If not, then for what n is this possible? For those n for which it is possible, can you put the coin onto *any* square and still do it?

2. Prove that for any integer a and any positive integer b, there exist integers q, r such that $a = qb + r$ and $0 \leq r \leq b - 1$. (In the lectures we proved this for positive a, so you only need to consider the case $a \leq 0$.)

3. Let $\mathbb{N}'$ be the set of all positive integers $\equiv \pm 1 \pmod 5$. Call an element of this set *irreducible* if it is not equal to 1 and is not a product of strictly smaller elements of $\mathbb{N}'$.
   (a) Compute the first 10 irreducibles of $\mathbb{N}'$.
   (b) Is every element of $\mathbb{N}'$ other than 1 a product of irreducibles?
   (c) Is the expression of an element as a product of irreducibles unique?

4. Let $a_1, \ldots, a_n$ be n integers. Prove that the sum of some non-empty subset of these is divisible by n.

5. Let a, b be positive coprime integers. Show that if two positive integers x, y satisfy $x^a = y^b$, then there is an integer n such that $x = n^b$, $y = n^a$.

6. Find all solutions of the following equations in positive integers:
   (a) $m^2 + n^2 = 100$;
   (b) $m! + n! + l! = k!$;
   (c) $m! = n^2$; (hint: you might want to google for "Bertrand's Postulate")
   (d) (optional) $m! = (n + 1)n$.

7. (a) Show that there are infinitely many primes $p \equiv 3 \pmod 4$.

   (b) Does your technique also apply to show that there are infinitely many primes $p \equiv 1 \pmod 4$? If yes, do it. If not, what's the problem?

8. (a) Let $\mathbb{Q}[x]$ denote the ring of polynomials in one variable with rational coefficients. The degree of a polynomial $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, denoted by $\deg f$, is the largest integer i for which $a_i \neq 0$. Show that for any $f, g \in \mathbb{Q}[x]$, there exist $r, q \in \mathbb{Q}[x]$ such that $f = qg + r$ and $\deg r < \deg g$.

   (b) Show that every ideal of $\mathbb{Q}[x]$ is principal.

   (c) Show that the ring $\mathbb{Z}[x]$ of polynomials in one variable with integer coefficients has non-principal ideals.