MATH 371 – Homework assignment 1 – August 29, 2013

1. Prove that if a subset $S \subset \mathbb{Z}$ has a smallest element then it is unique (in other words, if x is a smallest element of S and y is also a smallest element of S then $x = y$).

2. Calculate the remainder of 2^{500} after division by 341 by hand (use repeated squaring).

3. Let r be an integer greater than 1. An r-adic expansion of a number $x \in \mathbb{N}$ is an expression

$$x = a_0 + a_1 r + a_2 r^2 + \cdots + a_k x^k$$

where $k \in \mathbb{N}$, $a_i \in \mathbb{N}$ for all $0 \leqslant i \leqslant k$ and $0 \leqslant a_i < r$ for all $0 \leqslant i \leqslant k$. For instance, the 10-adic expansion of 5129 is

$$5129 = 9 + 2 \cdot 10^1 + 1 \cdot 10^2 + 5 \cdot 10^3$$

and the 8-adic expansion of 156 is

$$156 = 4 + 3 \cdot 8^1 + 2 \cdot 8^2.$$

(a) Compute the 7-adic expansion of 130.

(b) Prove that every $x \in \mathbb{N}$ (with $x > 0$) can be written as $x = ar^k + b$, where $0 \leqslant a < r$, $0 \leqslant b < r^k$ and $k = \max\{i \in \mathbb{N} \mid r^i \leqslant x\}$.

(c) Use (b) to prove (by induction?) that every natural number has a unique r-adic expansion.

4. Let the 10-adic expansion of x be

$$x = a_0 + a_1 10 + a_2 10^2 + \cdots + a_k 10^k$$

(where $0 \leqslant a_i < 10$ for all i).

(a) Prove that $2|x$ if and only if $2|a_0$.
(b) Prove that $4|x$ if and only if $4|(a_0 + 2a_1)$.
(c) Prove that $8|x$ if and only if $8|(a_0 + 2a_1 + 4a_2)$.
(e) Prove that $5|x$ if and only if $5|a_0$.
(f) Prove that $3|x$ if and only if $3|(a_0 + a_1 + \cdots + a_k)$.
(g) Prove that $9|x$ if and only if $9|(a_0 + a_1 + \cdots + a_k)$.
(h) Prove that $11|x$ if and only if $11|(a_0 - a_1 + a_2 - \cdots)$.
(i) What is the rule for divisibility by 7?

5. Find $a, b \in \mathbb{Z}$ such that $89a + 55b = 1$, and use this to find *all* solutions $x \in \mathbb{Z}$ to

$$89x \equiv 17 \pmod{55}.$$

6 (a) Suppose $aM + bN = d$, where $a, b, M, N \in \mathbb{Z}$ and $N > 0$. Prove that you can find $a', b' \in \mathbb{Z}$ such that $a'M + b'N = d$ and $0 \leqslant a' < N$.

(b) Let $m, n \in \mathbb{Z}$ and suppose there exist $a, b \in \mathbb{Z}$ suchs that $am + bn = 1$. Prove that m and n are relatively prime.

7. Define the sequence *Fibonacci numbers* as follows: $F_0 = F_1 = 1$ and for $n > 1$, $F_n = F_{n-1} + F_{n-2}$. So the beginning of the sequence is $1, 1, 2, 3, 5, 8, 13, 21, \ldots$. From the beginning of the sequence it appears that $\gcd(F_n, F_{n-1}) = 1$ for all $n \geqslant 1$. Either prove this or explain why it is not true.

8. Solve the system:

$$x \equiv 19 \pmod{504}$$
$$x \equiv -6 \pmod{35}$$
$$x \equiv 37 \pmod{16}$$

That is, find *all* numbers x that satisfy all three congruences.

9 (a) Let $p > 3$ be a prime number. Prove that for every $a \in \mathbb{N}$ such that $1 < a < p - 1$, there is a unique $b \in \mathbb{N}$ such that $1 < b < p - 1$, $b \neq a$, and $ab \equiv 1 \pmod{p}$.

(b) Let p be a prime number. Prove that $(p - 1)! \equiv -1 \pmod{p}$ (Hint: pair things up and apply part (a)). (This is called *Wilson's theorem.*)

(c) Is the converse of Wilson's theorem true? That is, if $n \geqslant 2$ and $(n - 1)! \equiv -1 \pmod{n}$, is n necessarily a prime number? (Proof or counterexample — think about this first, and try to do it without resorting to the Internet).

10 (a) Let p be a prime number. Prove that

$$p \mid \binom{p}{i} \quad \text{for } 1 \leqslant i \leqslant p - 1.$$

(b) Prove that

$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

for integers a, b and a prime number p.

(c) Suppose

$$n \mid \binom{n}{i} \quad \text{for } 1 \leqslant i \leqslant n - 1.$$

Does this imply that n is a prime number?