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 $x = y$).

We know the integers are linearly ordered (so for every pair $x, y \in \mathbb{Z}$ either $x < y$ or $y < x$ or $x = y$). So suppose x and y are smallest elements of S. We can't have $x < y$ or else y wouldn't be a smallest element, nor can we have $y < x$ or else x wouldn't be a smallest element. Therefore we must have $x = y$.

---

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

First, $500 = 256 + 128 + 64 + 32 + 16 + 4 = 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 2^2$. So we calculate: $2^1 = 1$, $2^2 = 2^{2^1} = 4$, $2^4 = 2^{2^2} = 16$, $2^8 = 2^{2^3} = 256$, $2^{16} = 2^{2^4} = 65536 \equiv 64 \pmod{341}$, $2^{32} = 2^{2^5} \equiv 64^2 \equiv 4096 \equiv 4 \pmod{341}$, $2^{2^6} \equiv 4^2 \equiv 16 \pmod{341}$, $2^{2^7} \equiv 16^2 \equiv 256 \pmod{341}$ and $2^{2^8} \equiv 256^2 \equiv 64 \pmod{341}$. Therefore

$$2^{500} \equiv 2^{2^8} \cdot 2^{2^7} \cdot 2^{2^6} \cdot 2^{2^5} \cdot 2^{2^4} \cdot 2^{2^2} \equiv 64 \cdot 256 \cdot 16 \cdot 4 \cdot 64 \cdot 16 \pmod{341}.$$

We can be clever about calculating this: we already know that $64^2 \equiv 4 \pmod{341}$, $16^2 = 256$ and $256^2 \equiv 64 \pmod{341}$. So we can group the numbers together to get $2^{500} \equiv 16 \cdot 64 \equiv 1024 \equiv 1 \pmod{341}$.

You could simplify the whole calculation by noticing that $341 = 11 \cdot 31$ so we know that $2^{10} \equiv 1 \pmod{11}$ and $2^{30} \equiv 1 \pmod{31}$. Of course, $2^{30} \equiv 1 \pmod{11}$, therefore $2^{30} \equiv 1 \pmod{341}$. Therefore $2^{500} \equiv 2^{480}2^{20} \equiv (2^{30})^{16}2^{20} \equiv 1^{16}2^{20} \equiv 2^{20} \pmod{341}$. But we know that $2^5 = 32 \equiv 1 \pmod{31}$, so $2^{20} \equiv (2^5)^4 \equiv 1 \pmod{31}$; and we already know $2^{20} = (2^{10})^2 \equiv 1 \pmod{11}$, so $2^{500} \equiv 2^{20} \equiv 1 \pmod{341}$.

---

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.

(a) $130 = 2 \cdot 49 + 32 = 2 \cdot 49 + 4 \cdot 7 + 4 = 4 + 4 \cdot 7 + 2 \cdot 7^2$.

(b) Let k be as defined in the problem, and consider the set $S = \{x - ar^k \mid a \in \mathbb{Z} \text{ and } x - ar^k \geqslant 0\}$. We have $S \subset \mathbb{N} \cup \{0\}$ so S has a smallest element, b. We certainly have $b \geqslant 0$ by the definition of S and we have $b < r^k$ since otherwise we could subtract r^k from b and find a smaller element of S. The value of a that produces this b has the property that $0 \leqslant a < r$ since $0 \leqslant ar^k < x < r^{k+1} = r(r^k)$.

(c) This time, let $S \subset \mathbb{N}$ be the set of natural numbers that do *not* have r-adic expansions. We know $1 \notin S$, so the smallest number in S is bigger than 1. If S is non-empty, x be the smallest number in S. We know that x is not a power of r, since the r-adic expansion of r^k is just $1 \cdot r^k$. Since $x > 1$, we know that there are powers of r (i.e., r^k for $k \geqslant 0$) that are less than x. Let r^ℓ be the largest power of r less than x. We know that the number $x - r^\ell$ has an r-adic expansion, say $x - r^\ell = a_0 + a_1 r + a_2 r^2 + \cdots + a_\ell r^\ell$ (where possibly $a_\ell = 0$, but definitely $a_\ell < r - 1$ because x was the smallest number that didn't. But then we'll have

$$x = a_0 + a_1 r + a_2 r^2 + \cdots + (a_\ell + 1) r^\ell,$$

so x has an r-adic expansion. Therefore S is empty and every natural number has an 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 $8|(a_0 + 2a_1 + 4a_2)$.
(d) Prove that $5|x$ if and only if $5|a_0$.
(e) Prove that $3|x$ if and only if $3|(a_0 + a_1 + \cdots + a_k)$.
(f) Prove that $9|x$ if and only if $9|(a_0 + a_1 + \cdots + a_k)$.
(g) Prove that $11|x$ if and only if $11|(a_0 - a_1 + a_2 - \cdots)$.
(h) What is the rule for divisibility by 7?

(a) Since $2 \mid 10$, we have $2 \mid a_1 10 + a_2 10^2 + \cdots + a_k 10^k$ and so $2 \mid x$ if and only if $2 \mid a_0$.

(b) Likewise $4 \mid 10^2$ so $4 \mid a_2 10^2 + \cdots + a_k 10^k$ and so $4 \mid x$ if and only if $4 \mid a_0 + 10a_1$. But $10 \equiv 2 \pmod 4$ and so $a_0 + 10a_1 \equiv a_0 + 2a_1 \pmod 4$. Thus $4 \mid x$ if and only if $4 \mid a_0 + 2a_1$.

(c) Likewise $8 \mid 10^3$ and so $8 \mid x$ if ad only if $8 \mid a_0 + 10a_1 + 100a_2$. But $10 \equiv 2 \pmod 8$ and $100 \equiv 4 \pmod 8$, so $8 \mid x$ if and only if $8 \mid a_0 + 2a_1 + 4a_2$.

(d) Since $5 \mid 10$, we have $5 \mid a_1 10 + a_2 10^2 + \cdots + a_k 10^k$ and so $5 \mid x$ if and only if $5 \mid a_0$.

(e) Since $10 \equiv 1 \pmod 3$, and so $1 \equiv 100 \equiv 10^3 \equiv 10^4 \equiv 10^k \pmod 3$ we have

$$x \equiv a_0 + a_1 10 + a_2 10^2 + \cdots + a_k 10^k \equiv a_0 + a_1 + \cdots + a_k \pmod 3$$

and so $3 \mid x$ if and only if $3 \mid a_0 + a_1 + \cdots + a_k$.

(f) Likewise $10 \equiv 1 \pmod 9$, and so $1 \equiv 100 \equiv 10^3 \equiv 10^4 \equiv 10^k \pmod 9$, and we have

$$x \equiv a_0 + a_1 10 + a_2 10^2 + \cdots + a_k 10^k \equiv a_0 + a_1 + \cdots + a_k \pmod 9$$

and so $9 \mid x$ if and only if $9 \mid a_0 + a_1 + \cdots + a_k$.

(g) Since $10 \equiv -1 \pmod{11}$, and so $-10 \equiv 100 \equiv -10^3 \equiv 10^4 \equiv (-1)^k 10^k \equiv 1 \pmod{11}$, and we have

$$x \equiv a_0 - a_1 10 + a_2 10^2 + \cdots + a_k 10^k \equiv a_0 - a_1 + \cdots + (-1)^k a_k \pmod{11}$$

and so $11 \mid x$ if and only if $3 \mid a_0 - a_1 + \cdots + (-1)^k a_k$.

(h) Since $10 \equiv 3 \pmod 7$, so $10^2 \equiv 9 \equiv 2 \pmod 7$, $10^3 \equiv 6 \pmod 7$, $10^4 \equiv 4 \pmod 7$, $10^5 equiv 5 \pmod 7$ and $10^6 \equiv 1 \pmod 7$ and it repeats from there, we have that $7 \mid x$ if and only if

$$7 \mid a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - a_9 - 3a_{10} - 2a_{11} + \cdots .$$

---

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

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

i	-1	0	1	2	3	4	5	6	7	8	9
r_i	89	55	34	21	13	8	5	3	2	1	0
q_i	–	–	1	1	1	1	1	1	1	1	2
λ_i	1	0	1	-1	2	-3	5	-8	13	-21	–
μ_i	0	1	-1	2	-3	5	-8	13	-21	34	–

The result is the next-to-last entry in the r_i row, namely, $\gcd(89, 55) = 1$. We also get that

$$-21 \cdot 89 + 34 \cdot 55 = 1 = \gcd(89, 55).$$

To get solutions to $89x \equiv 17 \pmod{55}$ we just multiply by 17 — so $x = -21 \cdot 17 = -357 \equiv 28 \pmod{55}$. So all the solutions of the equation are for the form $x = 28 + 55n$, for $n \in \mathbb{Z}$.

---

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 $a, b \in \mathbb{Z}$ such that $am + bn = 1$. Prove that m and n are relatively prime.

(a) For any integer k we will have $(a + kN)M + (b - kM)N = d$. Now let $S = \{a + kN \mid k \in \mathbb{Z} \text{ and } a + kN \geqslant 0\}$. This set has a smallest element, call it k'. It must be that $0 \leqslant a + k'N < N$ or else we'd have $a + (k' - 1)N \in S$ and $0 \leqslant a + (k' - 1)N < a + k'N$, which would be a contradiction. So $a' = a + k'N$ and $b' = b - k'M$ have the desired properties.

(b) Suppose $\gcd(m, n) = d > 1$. Then $d \mid m$ and $d \mid n$, but then $d \mid am + bn$ which contradicts $am + bn = 1$.

---

7. Define the sequence of *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.

It is true that $\gcd(F_n, F_{n-1}) = 1$. We can prove this by induction. It's clearly true for $n = 1$, so suppose $\gcd(F_{n-1}, F_{n-2}) = 1$. Then there are numbers λ and μ such that $\lambda F_{n-1} + \mu F_{n-2} = 1$. But then

$$1 = \lambda F_{n-1} - \mu F_{n-1} + \mu F_{n-1} + \mu F_{n-2} = (\lambda - \mu)F_{n-1} + \mu(F_{n-1} + F_{n-2}) = (\lambda - \mu)F_{n-1} + \mu F_n,$$

which shows that $\gcd(F_{n-1}, F_n) = 1$ by 6(b) above.

---

8. Solve the system:

$$\begin{aligned} x &\equiv 19 \pmod{504} \\ x &\equiv -6 \pmod{35} \\ x &\equiv 37 \pmod{16} \end{aligned}$$

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

There are no solutions — if $x \equiv 37 \equiv 5 \pmod{16}$ then $x = 16a + 5 = 4(4a + 1) + 1$, so $x \equiv 1 \pmod 4$. But $504 = 4 \cdot 126$, so if $x \equiv 19 \pmod{504}$ then $x = 504b + 19 = 4(126b + 4) + 3$, so $x \equiv 3 \pmod 4$, a contradiction.

---

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).

(a) Since every number in $1 < a < p - 1$ is relatively prime to p, we can find b and μ such that $ba + \mu p = 1$. By problem 6(a) we can choose b and μ so that $0 \leqslant b < p$ so we have $ba \equiv 1 \pmod p$. We can't have $b = a$ since then we'd have $a^2 \equiv 1 \pmod p$ but then a would have to be either 1 or $p - 1$, which it isn't. b is unique, since if there were another such number b' between 1 and $p - 1$, then (assuming b is the larger of the two) $b - b'$ would have the property that $(b - b')a \equiv 0 \pmod p$, i.e., $p \mid (b - b')a$. But p divides neither $b - b'$ nor a since they're both less than $p - 1$, contradicting the fact that p is prime.

(b) Since $(p-1)!$ is the product of all the numbers up to $p-1$, it contains every pair of numbers a, b as we found in part (a), and every number is part of such a pair except for 1 and $p - 1$. So $(p-1)! \equiv 1 \cdot 1 \cdots 1 \cdot (p-1) \equiv p - 1 \equiv -1 \pmod p$.

(c) The converse is true — if p is composite, then we can write $p = ab$ for two numbers a and b between 2 and $p - 1$. But both these numbers will be factors of $(p-1)!$ so we'll have $p \mid (p-1)!$, i.e., $(p-1)! \equiv 0 \pmod p$.

---

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?

(a) Because $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$, we have that $p! = \binom{p}{i}[i!(p-i)!]$. Now certainly $p \mid p!$, but p does not divide $i!(p-i)!$, since all the factors of $i!(p-i)!$ are less than p (this uses the basic fact that p divides a product if and only if p divides at least one of the factors). Using that same fact, we deduce that $p \mid \binom{p}{i}$.

(b) This follows easily from the binomial theorem and part (a), since p divides the binomial coefficients in all the terms except the initial and final terms.

(c) Yes. Let p be the smallest prime factor of n. Then n cannot divide $\displaystyle\binom{n}{p}$, because the p in the $p!$ in the denominator of the binomial coefficient will cancel a power of p from the n in the $n!$ in the numerator, and the $(n-p)!$ in the denominator will cancel all of the other factors in the numerator that have any powers of p as divisors. So $\displaystyle\binom{n}{p}$ will be a factor of p short of being divisible by n.