Tuesday, December 1, 2015 4:07 PM

1. Let $n \in \mathbb{Z}^{>1}$. Prove that there is an integer m such that

   (a) digits of m are either 0 or 1.

   (b) $n \mid m$.

(Hint. Consider the remainders $r_1, \dots, r_{n+1}$ of $1, 11, \dots, \underbrace{11\cdots1}_{n+1}$ divided by n. So $\underbrace{r_1, \dots, r_{n+1}}_{\text{pigeons}} \in \{\underbrace{0, 1, \dots, n-1}_{\text{pigeonholes}}\}$.

Using pigeonhole deduce $\exists\, 1 \le i < j \le n+1$:

$$\underbrace{1\cdots1}_{j} \overset{n}{\equiv} \underbrace{1\cdots1}_{i}. \;)$$

2. Prove that there are infinitely many primes of the form $3k-1$ for some integer k.

(Hint. Suppose to the contrary there are only finitely many such primes: $p_1 = 2, p_2, \dots, p_n$. Let $M = 3(p_1 p_2 \cdots p_n) - 1$.

. So $M \overset{p_i}{\equiv} -1 \Rightarrow p_i \nmid M \Rightarrow$ none of the prime factors of M are of the form $3k-1$.

. $3 \nmid M$ as $M \overset{3}{\equiv} -1$.

. So $p \mid M \Rightarrow p \overset{3}{\not\equiv} 0$ and $p \overset{3}{\equiv} -1 \Rightarrow p \overset{3}{\equiv} 1$.

Therefore M can be written as a product of numbers that are $1 \bmod 3$. So $M \overset{3}{\equiv} 1$ which is a contradiction.)

3. (a) Suppose $a_0, a_1, \dots, a_k$ are digits (in base 10) of m. So $m = \overline{a_k a_{k-1} \cdots a_0}$. E.g., for $m = 12037$, $k = 4$, $a_0 = 7$, $a_1 = 3$, $a_2 = 0$, $a_3 = 2$, $a_4 = 1$.

Prove $\overline{a\,a\,\cdots\,a} \overset{11}{=} a - a + a - \cdots (-1)^k a$

Prove $\overline{a_k a_{k-1} \cdots a_0} \overset{11}{\equiv} a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$.

(b) Use part (a) to find the remainder of

$$120345900124687$$ divided by 11.

(Hint. For part (a), use $10 \overset{11}{\equiv} -1$.)

4. (a) Is there $x \in \{0,1,2,\ldots,12\}$ such that

$$5x \overset{13}{\equiv} 1 \quad ?$$ Justify your answer.

(b) Is there $x \in \{0,1,2,\ldots,11\}$ such that

$$2x \overset{12}{\equiv} 1 \quad ?$$ Justify your answer.

5. Suppose p is prime, and $a \in \{1,2,\ldots,p-1\}$.

Let $L_a : \{0,1,2,\ldots,p-1\} \longrightarrow \{0,1,2,\ldots,p-1\}$ be

$L_a(x) = r$ where $ax \overset{p}{\equiv} r$.

Notice that r is the remainder of ax divided by p.

(a) Prove that L_a is surjective.

(b) Prove that L_a is bijective.

(c)* Prove that $a^{p-1} \overset{p}{\equiv} 1$.

(Hint. For part (a) since $\gcd(a,p) = 1$, by Euclid's algorithm

$\exists x_0, y_0 \in \mathbb{Z}$, $ax_0 + py_0 = 1 \Rightarrow ax_0 \overset{p}{\equiv} 1$

$\Rightarrow \forall r \in \{0,1,\ldots,p-1\}$, $ax_0 r \overset{p}{\equiv} r$.

Let x' be the remainder of $x_0 r$ divided by p. So

$xr \overset{p}{\equiv} x'$ and $x' \in \{0,1,\ldots,p-1\}$. Hence $L_a(x') = r$.

For part (b), $L_a(x_1) = L_a(x_2) \Rightarrow ax_1 \overset{p}{\equiv} ax_2$

$\Rightarrow a(x_1 - x_2) \overset{p}{\equiv} 0$

$\Rightarrow a(x_1 - x_2) \overset{p}{\equiv} 0.$

Let x_0 be as in part (a), i.e. $ax_0 \overset{p}{\equiv} 1$.

So $x_1 - x_2 \overset{p}{\equiv} ax_0(x_1 - x_2) \overset{p}{\equiv} 0 \Rightarrow x_1 \overset{p}{\equiv} x_2$ $\Big\}$ $\Rightarrow x_1 = x_2$.
$x_1, x_2 \in \{0, 1, \cdots, p-1\}$

For **part (c)**, since L_a is a bijection and $L_a(0) = 0$,

$$\{L_a(1), L_a(2), \ldots, L_a(p-1)\} = \{1, 2, \ldots, p-1\}.$$

Hence $1 \cdot 2 \cdot \cdots \cdot (p-1) = L_a(1) \cdot L_a(2) \cdot \cdots \cdot L_a(p-1)$

$$\overset{p}{\equiv} (a)(2a) \cdot \cdots \cdot ((p-1)a)$$

$$\Rightarrow (p-1)! \overset{p}{\equiv} a^{p-1}(p-1)!$$

Since p is prime, $p \nmid (p-1)!$ and so $\gcd(p, (p-1)!) = 1$.

Therefore $\exists x' \in \mathbb{Z}$ s.t. $x'(p-1)! \overset{p}{\equiv} 1$

$$\Rightarrow 1 \overset{p}{\equiv} a^{p-1}.$$

Part (c) is NOT easy. It is called Fermat's little theorem.)

6. Find $x, y \in \mathbb{Z}$ such that

$$210x - 121y = 1.$$

(Hint. Use Euclid's algorithm.)