MATH 257: Homework #1

Jesse Farmer

06 October 2004

1. *Prove that* $a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_0 \equiv a_n + a_{n-1} + \cdots + a_0$ *(mod 9).*

   We will show that, in general, if $x \equiv y$ (mod n) then

   $$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0 \equiv a_m y^m + a_{m-1}y^{m-1} + \cdots + a_0 \pmod{n}$$

   This is equivalent to showing that $n \mid a_m(x^m - y^m) + a_{m-1}(x^{m-1} - y^{m-1}) + \cdots + a_1(x - y)$. It is therefore sufficient to show that $n|(x^r - y^r)$ for every $r \in \mathbb{N}$. This is easy to see since, by hypoethesis, we have $n|(x - y)$ and

   $$n \mid (x - y)\sum_{k=1}^{r} x^{k-1}y^{r-k} = x^r - y^r$$

   Therefore $n \mid a_r(x^r - y^r)$ for every $r \in \mathbb{N}$, and the congruence is proven. The problem is a special case where $x = 10$, $y = 1$, and $n = 9$.

2. *Find the remainder of* 37^{100} *when divided by* 29.

   The answer is 23. It is easier to calculate if we use Fermat's Little Theorem since 29 is prime, so

   $$37^{100} \equiv (8^{16})(8^{28})^3 \equiv 8^{16} \equiv (8^2)^8 \equiv 64^8 \equiv 6^8 \equiv (6^2)^4 \equiv 7^4 \equiv 400 \equiv 23 \pmod{29}$$

3. *Define* $\tau_x(a, b) : \mathbb{Z}_n \to \mathbb{Z}_n$ *as* $\overline{x} \mapsto \overline{ax + b}$ *and* $G = \{\tau_x(a, b) \mid a, b \in \mathbb{Z}, (a, n) = 1\}$.

   (a) *Show that each element of* G *is a well-defined permutation on* $\mathbb{Z}_n$.

   Let $x_1, x_2 \in \overline{x}$ so that $x_1 \equiv x_2$ (mod n). By the fact that addition and multiplication are well-defined on $\mathbb{Z}_n$, $ax_1 + b \equiv ax_2 + b$ (mod n), i.e., $\overline{ax_1 + b} = \overline{ax_2 + b}$. The inverse of an arbitrary $\tau_x(a, b)$ is constructed explicitly below, and hence each $\tau_x(a, b) \in G$ is a bijection from $\mathbb{Z}_n$ to $\mathbb{Z}_n$, i.e., a permutation of $\mathbb{Z}_n$.

   (b) *Show that if* $\alpha, \beta \in G$ *then* $\alpha\beta, \alpha^{-1} \in G$.

   Let $\alpha, \beta \in G$ and define $\alpha := \tau_x(a, b)$ and $\beta := \tau_x(c, d)$. Since $(a, n) = 1$, a^{-1} exists. We claim $\alpha^{-1} = \gamma := \tau_x(a^{-1}, -a^{-1}b) \in G$.

   $$x(\gamma\alpha) \equiv a(a^{-1}x - a^{-1}b) + b) \equiv aa^{-1}x - aa^{-1}b + b \equiv x - b + b \equiv x \pmod{n}$$

and

$$x(\alpha\gamma) \equiv a^{-1}(ax+b)-b) \equiv a^{-1}ax + a^{-1}ab - b \equiv x + b - b \equiv x \pmod{\mathrm{n}}$$

Moreover,

$$\alpha\beta = \overline{c(ax+b)+d} = \overline{cax+cb+d} = \tau_x(ca, cb+d) \in G$$

(c) *Find $|G|$ if n is prime.*

Let $\tau_x(a,b) = \tau_x(a',b')$ so that $ax+b \equiv a'x+b' \pmod{\mathrm{n}}$. This implies $x(a-a')+(b-b') \equiv 0 \pmod{\mathrm{n}}$, i.e., $a \equiv a'$ and $b \equiv b' \pmod{\mathrm{n}}$. In general this means there are $\varphi(n)$ ways to choose a, where φ is Euler's totient function, and n ways to choose b, and hence $|G| = n\varphi(n)$. For n prime $\varphi(n) = n-1$ (since all elements of $\mathbb{Z}_n \setminus \{0\}$ are units), so in this case $|G| = n(n-1)$.

4. *Let $G = \{x \in \mathbb{R} \mid x \in [0,1)\}$ and for all $x, y \in G$ define $x \star y = x + y - [x+y]$. Show that $(G, \star)$ is an Abelian group.*

Let $x, y \in G$ be arbitrary. If $0 \le x+y < 1$ then $[x+y] = 0$, so $0 \le x+y-[x+y] < 1$. Otherwise, if $1 \le x+y < 2$ then $[x+y] = 1$, so $0 \le x+y-[x+y] < 1$. Therefore $x \star y \in G$.

The identity is clearly 0 since for $x \in G$, $[x] = 0$. $x^{-1} = 1 - x$ since

$$x \star (1-x) = x + (1-x) - [x + (1-x)] = 1 - [1] = 0$$

Commutativity is inherited from $\mathbb{R}$. Let $x, y, z \in G$, then

$$\begin{aligned}
(x \star y) \star z &= (x+y-[x+y]) \star z = x+y+z-[x+y] - \big[x+y+z-[x+y]\big] \\
x \star (y \star z) &= x \star (y+x-[y+z]) = x+y+z-[y+z] - \big[x+y+z-[y+z]\big]
\end{aligned}$$

So it is sufficient to show

$$\big[x+y+z-[x+y]\big] - [y+z] = \big[x+y+z-[y+z]\big] - [x+y] \tag{1}$$

From the definition of G it is clear that $[x+y], [y+z] \in \{0,1\}$. If both are 0 or both are 1 then (1) is obvious, so assume without loss of generality that $[x+y] = 0$ and $[y+z] = 1$. Then, letting $a = x+y+z$,

$$\big[x+y+z-[x+y]\big] - \big[x+y+z-[y+z]\big] = [a] - [a-1] = 1$$

but

$$[y+z] - [x+y] = 1$$

Combining the above two yields (1), and hence $\star$ is associative. Therefore $(G, \star)$ is an Abelian group.

5. *Let $\pi \in S_n$ and define π^i recursively by $\pi^i = \pi^{i-1}\pi$. The order of π is*

$$|\pi| = \min\{i \in \mathbb{N} \mid \pi^i = I\}$$

(a) *Show that $|\pi|$ is the least common multiple of the lengths of the cycles of π.*

Consider π as the product of disjoint cycles $c_1, c_2, \ldots, c_k$, and let the length of the cycle c_i be l_i. If $c_i^n = I$, the identity, then $n \mid l_i$ since, if some element is permuted by c_i it must be permuted some multiple of l_i times for it to return to its original position because of the injective nature of disjoint cycles. Since composition of disjoint cycles is commutative,

$$\pi^n = (c_1 c_2 \cdots c_k)^n = c_1^n c_2^n \cdots c_k^n$$

If $\pi^n = I$ then $c_i^n = I$ and hence $n \mid l_i$ for $i = 1, 2, \ldots, k$. The smallest such n to do this is by definition the least common multiple of the l_i, i.e., the least common multiple of the lengths of the cycles of π.

(b) *Let $N(n,m)$ be the number of permutations in S_n of order m. Determine $N(n,m)$ for $n \leq 5$ and for all m.*

Since $|S_n| = n!$, this provides a way of checking whether the calculated values are correct. Also, in general, there are $\binom{n}{m}(m-1)!$ cycles of length m. We can see this by choosing a subset of size m, calling the first element m_1, and permuting the other $m-1$ elements.

<u>$n = 1$</u>: Since all permutations are the identity, $N(1,1) = 1$.

<u>$n = 2$</u>: $N(2,1) = 1$, and $N(2,2) = 1$.

<u>$n = 3$</u>: $N(3,1) = 1$, $N(3,2) = \binom{3}{2}(2-1)! = 3$, $N(3,3) = \binom{3}{3}(3-1)! = 2$

<u>$n = 4$</u>: $N(4,1) = 1$, $N(4,2) = \binom{4}{2}(2-1)! + \frac{\binom{4}{2}}{2} = 9$, $N(4,3) = \binom{4}{3}(3-1)! = 8$, $N(4,4) = \binom{4}{4}(4-1)! = 6$

<u>$n = 5$</u>: $N(5,1) = 1$, $N(5,2) = \binom{5}{2} + \binom{5}{2}\binom{3}{2}\binom{1}{1} = 25$, $N(5,3) = \binom{5}{3}(3-1)! = 20$, $N(5,4) = \binom{5}{4}(4-1)! = 30$, $N(5,5) = 4! = 24$, $N(5,6) = \binom{5}{3}(3-1)! = 20$.

6. *For what for $n, m \in \mathbb{Z}$ can the map $f : \mathbb{Z} \to \mathbb{Z}$ defined as $f(x) = x^2$ be considered as a map from $\mathbb{Z}_n$ to $\mathbb{Z}_m$?*

The map must be well-defined, so for any two $x, y \in \overline{x}$, $f(x) \equiv f(y) \pmod{m}$. In particular, let $x \in \overline{x}$ be arbitrary and let $y = x + n$.

Simply expanding the required congruence, $x^2 \equiv (x+n)^2 \pmod{m}$ shows that f is well-defined if and only if the following is true:

$$2nx + n^2 \equiv 0 \pmod{m}, \forall x \in \mathbb{Z} \tag{2}$$

We claim that (2) is true if and only if $m \mid 2n$ and $m \mid n^2$. That this condition is sufficient is obvious, so assume (2) is valid for all $x \in \mathbb{Z}$. In particular this means (2) must be valid for $x = 0$, and hence $m \mid n^2$. Similarly, it must be valid for $x = 1$, and hence (since $m \mid n^2$) $m \mid 2n$, which proves our claim. Note that this works even when considering the trivial group $\{0\}$, since $1 \equiv 0 \pmod{1}$ and certainly m will always divide 0.