As for the rest, I can do no better than the customary proofs. However, one can go one and ask what happens if the map $x \mapsto ax$ is applied numerous times. In some cases, the whole group eventually get mapped to zero. For example, $\mathbf{Z}/p^2\mathbf{Z} \to \mathbf{Z}/p^2\mathbf{Z}$ with the map $x \mapsto px$. In other cases it stabilizes, the Image of a^2 is the same as that of a.

There remain to identify which b have solutions and how solutions are obtained. There is only one subgroup of $\mathbf{Z}/m\mathbf{Z}$ of size m/d and it is the multiples of d. So, for a solution to be possible, $d \mid b$. To find a solution, one might just as well at this point, find s, t such that,

$$d = sa + tm$$

and the result is bs/d. These are the same s and t as satisfy,

$$1 = s(a/d) + t(m/d),$$

hence x is the unique solution to,

$$(a/d)x = (b/d) \pmod{m/d}.$$

5. Remembering that $1 + 2 + \ldots + n = (n+1)n/2$ has always confused me. Now I'll never be confused again because I found this proof:

$$\begin{array}{rccccccc} & 1 & + & 2 & + & \ldots & + & n \\ + & n & + & (n-1) & + & \ldots & + & 1 \\ \\ = & (n+1) & + & (n+1) & + & \ldots & + & (n+1) \end{array}$$

Notes on Congruences

DATE: MAY 18, 1993
BURT ROSENBERG

1. I conjectured in class that having verified that addition is consistant with the equivlance classes of Mod-n, that subtraction follows necessarily. This appears to be false.

2. The development of congruences is via divisibility, rather than homomorphisms. As partial as I am to maps, the earliest foundations of congruences do seem to be faster set in place using divisibility.

3. The proof of Fermat's theorem uses the bijection of the modular ring to itself by multiplication via a unit. This is given by Koblitz. For the sake of variety, he gives a different proof in the case of Euler's extension of Little Fermat. However, the proof works after one sees that multiplication by a unit is a bijection on units.

4. The equation,

$$ax = b \pmod{m}$$

has solutions if and only if $(m,a) \mid b$, and in that case, it has (m,a) solutions given by the reduced equation:

$$(a/d)x = (b/d) \pmod{m/d}, \text{ where } d = (m,a).$$

PROOF: Consider the map $\mathbf{Z}/m\mathbf{Z}$ to itself multiplication by a. The kernal of this map is all y such that $ay = 0 \pmod{m}$. The image is a subgroup of $\mathbf{Z}/m\mathbf{Z}$, from which it stands that for some $d \mid m$, there are m/d cosets and each coset, including the kernel, has d members. Hence, the equation $ax = b \pmod{m}$ has either d or 0 solutions depending where d is the number of annihilators of a. (Note: an annihilator of a is a b such that $ab = 0 \pmod{m}$.)

Now there is some calculation. Let f be the greatest common divisor of a and m, $f = (a,m)$. Write a as $a'f$ and m as $m'f$. Then x annihilates a if and only if $x = im'$ and such x are unique mod m for $i = 0, \ldots, (f-1)$. So there are $d = (a,m)$ annihilators of a in $\mathbf{Z}/m\mathbf{Z}$.

Burt Rosenberg