Due Wednesday. From page 47, exercises 3–8, 10.

Due Friday. From page 54: 1–5, 8, 10; and from page 63: 1, 4–6, 8, 9, 13, 19–21.

First test. Wednesday, Feb. 22.

For next time. Read through section 3.3.

Last meeting. Introduction to congruence modulo $n$.

Today. As we’ve seen, congruence modulo $n$ has a lot of the same properties as equality. Equality has a very strong property of substitution. If $a = b$, then given any algebraic expression $f(a)$ that involves $a$, if you substitute one or more of the instances of $a$ by $b$, then the resulting expression $f(b)$ is equal to the original expression $f(a)$. Congruence modulo $n$ doesn’t have as strong a property of substitution. But, since congruence modulo $n$ works well with addition, subtraction, and multiplication, if $f(a)$ is any algebraic expression built from addition, subtraction, and multiplication, that is, if $f(a)$ is a polynomial, and one or more of the instances of $a$ in $f(a)$ is replaced by $b$, then the resulting polynomial $f(b)$ is congruent to $f(a)$ modulo $n$.

For example, if $f(a) = 7xa^2 + 5axy - 13$, and $a \equiv b \pmod{n}$, then $f(a) \equiv b \pmod{n}$, that is, $7xa^2 + 5axy - 13 \equiv 7xb^2 + 5bxy - 13 \pmod{n}$.

We saw last time that division doesn’t always work so well with congruence modulo $n$, but it does sometimes, and that’s when you’re dividing by a number relatively prime to $n$. Here’s the theorem.

Theorem. If $(a, n) = 1$ and $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.

Proof: Since $ab \equiv ac \pmod{n}$, therefore $ab = ac + kn$ for some integer $n$. Therefore, $a|kn$, but $(a, n) = 1$, so $a|k$. Let $k = ak_1$. Now divide the equation $ab = ac + kn$ by $a$ to get $b = c + k_1n$. Therefore, $b \equiv c \pmod{n}$. Q.E.D.

There is a generalization of this theorem, namely, if $(a, n) = d$ and $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n/d}$.

Residue systems. It is clear that every integer $a$ is congruent modulo $n$ to one of the integers $0, 1, 2, \ldots, n - 1$. Just take the remainder when you divide $a$ by $n$. (There’s a little more to do if $a$ is negative, but not much.) The set of numbers

$$\{0, 1, 2, \ldots, n - 1\}$$

is called a complete system of residues modulo $n$ because every integer is congruent to exactly one of the integers in that set. There are other complete systems of residues modulo $n$, but this is the one usually taken.

We’ll look at addition and multiplication tables modulo $n$. 