CONGRUENCE AND MODULUS: PART 2

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

Congruences such as $a \equiv b \bmod m$ behave a lot like equalities. For example, we saw earlier that reflexive, symmetric, and transitive properties hold. In other words, $\equiv_m$ is an equivalence relation. We will now concentrate on other ways in which congruences behave like equalities. For example, we can add or multiply an integer to both sides of a true congruence and get another true congruence.

We begin with two important rules; all the other rules of congruence we need follow from these two. They can be informally described as follows:

$$\frac{\begin{array}{r} a \equiv b \mod m \\ c \equiv d \mod m \end{array}}{a + c \equiv b + d \mod m} \qquad \frac{\begin{array}{r} a \equiv b \mod m \\ c \equiv d \mod m \end{array}}{ac \equiv bd \mod m}$$

We now formally describe and prove these rules.

Proposition 1 (Additive Compatibility of Congruences)**.** *Let m be a positive integer, and let $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $a + c \equiv b + d \bmod m$.*

Proof. By definition $m \mid (a - b)$ and $m \mid (c - d)$. Thus m divides the sum $(a - b) + (c - d) = (a+c)-(b+d)$. By definition of congruence, $m \mid (a+c)-(b+d)$ yields $a+c \equiv b+d \bmod m$. □

Proposition 2 (Multiplicative Compatibility of Congruences)**.** *Let m be a positive integer, and let $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $ac \equiv bd \bmod m$.*

Proof. By definition $m \mid (a - b)$ and $m \mid (c - d)$. So m divides the linear combination

$$c(a - b) + b(c - d) = ca - cb + bc - bd = ac - bd.$$

From $m|ac - bd$ it follows, by definition, that $ac \equiv bd \bmod m$. □

Example 1. Observe that $5 \equiv 9 \bmod 4$ and $53 \equiv 101 \bmod 4$. We conclude that $5 \cdot 53 \equiv 9 \cdot 101 \bmod 4$. In other words $265 \equiv 909 \bmod 4$.

Example 2. Recall that n is even if and only if $n \equiv 0 \bmod 2$ and n is odd if and only if $n \equiv 1 \bmod 2$. The above rules allow us to conclude that (i) an even plus and even is even, (ii) an odd plus and even is odd, (iii) an odd plus an odd is even, (iv) an even times an even is even, (v) an even times an odd is even, and (vi) an odd times an odd is odd.

For example, to prove (ii) suppose a is odd and b is even. So $a \equiv 1 \bmod 2$ and $b \equiv 0 \bmod 2$. By the additive compatibility, $a + b \equiv 1 + 0 \bmod 2$, so $a + b$ is odd.

In the special case where $c = d$, we have $c \equiv d \bmod m$ by the reflexive law. This give rise to the following

Corollary 1. *Let m be a positive integer, and let $a, b, c \in \mathbb{Z}$. (i) If $a \equiv b \bmod m$ then $a + c \equiv b + c \bmod m$. Likewise, (ii) if $a \equiv b \bmod m$ then $ac \equiv bc \bmod m$.*

Date: Fall 2005. Version of October 1, 2005.

The rules in the above corollary can be written as follows:

$$\frac{a \equiv b \mod m}{a + c \equiv b + c \mod m} \qquad \frac{a \equiv b \mod m}{ac \equiv bc \mod m}$$

In other words, you can add or multiply a true congruence by an integer c and obtain another true congruence. Another way to think of these rules is that it allows you to substitute a congruent term in any given product or sum. Another consequence is the power rule

$$\frac{a \equiv b \mod m}{a^n \equiv b^n \mod m}$$

which we prove below:

Proposition 3. *Let m be a positive integer, let $a, b \in \mathbb{Z}$, and let n be a non-negative integer. If $a \equiv b \bmod m$ then $a^n \equiv b^n \bmod m$.*

Proof. (Induction) The case $n = 0$ is automatic since $1 \equiv 1 \bmod m$.

Assume that the statement holds for a particular $n = k$. We must show that it holds for $n = k + 1$. So assume, $a \equiv b \bmod m$. By the induction hypothesis $a^k \equiv b^k \bmod m$. By Proposition 2 applied to the above two congruences, $aa^k \equiv bb^k \bmod m$. In other words $a^{k+1} \equiv b^{k+1} \bmod m$. □

Remark. There are limitations to what substitutions are allowed. For instance the "rule"

$$\frac{a \equiv b \mod m}{c^a \equiv c^b \mod m}$$

fails. For example, $1 \equiv 4 \bmod 3$ but $2^1 \not\equiv 2^4 \bmod 3$. In fact, we will need theorems such as Fermat's Little Theorem and Euler's Theorem to help reduce powers.

Even though not every possible substitution is allowed, any substitution in a polynomial is allowed:

$$\frac{a \equiv b \mod m}{f(a) \equiv f(b) \mod m}$$

where $f(x)$ is any polynomial with integer coefficients.

Proposition 4. *Let m be a positive integer, let $a, b \in \mathbb{Z}$, and let $f(x)$ be a polynomial with integer coefficients. If $a \equiv b \bmod m$ then $f(a) \equiv f(b) \bmod m$.*

Proof. (Sketch). First assume that $f(x)$ is a monomial: $f(x) = cx^n$. Then $a^n \equiv_m b^n$ by Proposition 3, and $ca^n \equiv_m cb^n$ by Corollary 1. In other words, $f(a) \equiv f(b) \bmod m$.

Prove the general case by induction on the number of terms of $f(x)$ using Proposition 1. □

Dr. Wayne Aitken, Cal. State, San Marcos, CA 92096, USA
E-mail address: waitken@csusm.edu