Math 358 – Foundations of Mathematics **Fall 2008**
11-6-08 Class Notes

Section 4.5
4.5: 64, 70, 72, 77, 81

Modular Arithmetic

Example 1: If it is currently 10:00, what time will it be in
(a) 5 hours?
(b) 29 hours?
(c) 80 hours?
(d) 24,000 hours?

(a) 3:00, (b) 3:00, (c) 6:00, (d) 10:00.

This is an example of modular arithmetic. Even though $10+5=15$, we all knew that $10:00+5 \text{ hours} = 3:00$. Also, adding 29 hours to a time is the same as adding 5 hours to it, so we were able to answer part (b) with little trouble. Similarly, adding 24 hours to a time is equivalent to adding 0 hours to a time, so we were able to compute the other two answers easily as well. This notion of equivalence is the focus of this section.

Definition: Let $m \in \mathbb{N}$. For $a, b \in \mathbb{Z}$, we say that ***a is congruent to b modulo m*** if $a-b$ is divisible by m. The number m is called the ***modulus***. This is denoted by $a \equiv b \pmod{m}$. Stated another way:

$$a \equiv b \pmod{m} \iff a = b + km \text{ (for some integer } k\text{)}$$

Example 2: $26 \equiv 1 \pmod{5}$, $54 \equiv 14 \pmod{4}$, and $-130 \equiv 2 \pmod{3}$. But $20 \not\equiv 1 \pmod{5}$. In fact, $20 \not\equiv 1 \pmod{m}$ for any $m \neq 1 \text{ or } 19$.

Theorem 1: For $m \in \mathbb{N}$, congruence modulo m is an equivalence relation on $\mathbb{Z}$.

Proof:

(Reflexivity) $a \equiv a \pmod{m}$ for all a, since 0 is divisible by any m.

(Symmetry) If $a \equiv b \pmod{m}$, then $a = b + km$ for some integer k. So $b = a + (-k)m$ and therefore $b \equiv a \pmod{m}$.

(Transitivity) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a = b + km$ for some integer k and $b = c + lm$ for some integer l. So $a = b + km = (c + lm) + km = c + (k + l)m$. Therefore, $a \equiv c \pmod{m}$.

Note: The equivalence classes for this equivalence relation are usually called the ***congruence classes*** modulo m.

As we learned, the set of all congruence classes forms a partition of $\mathbb{Z}$. Let's examine this partition for several values of m.

$\boxed{m = 1}$ This isn't a very interesting partition. In this case, every integer is congruent to every other integer since 1 (the modulus) divides everything. So we only have one congruence class, the whole set $\mathbb{Z}$.

$\boxed{m = 2}$ For 2 to divide the difference of two integers, they have to have the same parity. In other words, the two numbers have to both be even or both be odd. So we have two congruence classes, the evens and the odds.

$\boxed{m = 3}$ Clearly, 0, 1, and 2 are not congruent. So we have at least three congruent classes. In fact, we can easily see that there are exactly three congruence classes, namely:

$$\{\ldots, -6, -3, 0, 3, 6, \ldots\},$$
$$\{\ldots -5, -2, 1, 4, 7, \ldots\}, \text{ and}$$
$$\{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

Theorem 2: If $m \in \mathbb{N}$, then every integer is congruent modulo m to exactly one of the integers $0, 1, 2, \ldots, m - 1$.

Proof: This is true by the Division Algorithm. Recall that when we divide an integer a by m, the Division Algorithm tells us that there are unique integers q (the quotient) and r (the remainder) with $0 \le r < m$ such that $a = mq + r$. Therefore, a is congruent to r.

What this theorem tells us is that when we partition $\mathbb{Z}$ into it's congruence classes modulo m, we get $\{[0],[1],[2],\ldots,[m-1]\}$.

Theorem 3: Let $m \in \mathbb{N}$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

(a) $a + c \equiv b + d \pmod{m}$, and

(b) $ac \equiv bd \pmod{m}$.

Since $a \equiv b \pmod{m}$ are integers, this theorem shows that addition, subtraction and multiplication all preserve congruence. What about division? Nope.

Example 3: $20 \equiv 10 \pmod{10}$ but clearly $2 \not\equiv 1 \pmod{10}$.

Theorem 4: Let $m \in \mathbb{N}$ and let $a,b,c \in \mathbb{Z}$. Suppose that $ac \equiv bc \pmod{m}$. If $\gcd(c,m) = 1$, then $a \equiv b \pmod{m}$. In general, if $\gcd(c,m) = d$, then $a \equiv b \pmod{\frac{m}{d}}$.

Theorem 5: Let $m \in \mathbb{N}$, $a,b \in \mathbb{Z}$, and $d = \gcd(a,m)$. If $d \mid b$, then $ax \equiv b \pmod{m}$ has exactly d distinct (i.e. incongruent) solutions. Otherwise, $ax \equiv b \pmod{m}$ has no solutions.

Example 4: (a) How many distinct solutions does $3x \equiv 12 \pmod{15}$ have?

(b) How many distinct solutions does $3x \equiv 12 \pmod{10}$ have?

(c) How many distinct solutions does $3x \equiv 10 \pmod{15}$ have?

(a) Since $\gcd(3,15) = 3$ and $3 \mid 12$, we have 3 distinct solutions. They are: 4, 9, and 14. Notice that $3 \cdot 19 = 57 \equiv 12 \pmod{15}$, but 19 is congruent to 4 modulo 15, so it is not a *distinct* solution.

(b) Since $\gcd(3,10) = 1$ and $1 \mid 12$, we have a unique solution, 4.

(c) The $\gcd(3,15) = 3$, but 3 does not divide 10, so there are no solutions.

Finally we come to a useful little theorem.

Theorem 6 (Fermat's Little Theorem): Let p be a prime and let $a \in \mathbb{N}$ such that p does not divide a. Then $a^{p-1} \equiv 1 \pmod{p}$.

This is a very powerful theorem, because:

(1) It allows us to calculate congruence classes of large numbers Easily. For example, $18^{28} \equiv 1 \pmod{29}$.

(2) It allows us to easily simplify even larger expressions. For example, $3^{2241} \equiv (3^6)^{373} \cdot 3^3 \equiv 27 \equiv 6 \pmod{7}$.

(3) It actually allows us to check large number for primality. For example, since $2^{85812} \not\equiv 1 \pmod{85813}$, 85813 is not prime.