COMP 251: Data Structures and Algorithms Fall 2006

Tutorial on Modular Congruences

Lecturer/TA: Ethan Kim *October 20th, 2006*

In this tutorial, we study basic number theory including congruences modulo n.

1 Review of Basic Number Theory

First, we introduce the notation $a \mid b$ (read "*a divides b*"), meaning that $b = ka$ for some integer k. If a does not divide b, we write $a \nmid b$. An integer $p > 1$ whose only divisors are 1 and a itself, we say p is *prime*. All other positive integers can be expressed as a product of prime numbers, and they are called *composite* numbers. Two integers a and b are said to be *relatively prime* if their only common divisor is 1.

2 Introduction to Congruences

Definition. *Let a, b, m be integers with $m > 0$. If $m \mid (a - b)$, we say that a is* congruent to b modulo m*, and we write it as $a \equiv b$ (mod m). This notion can also be characterized as follows.*

Theorem 1. *Let a and b be integers. Then, $a \equiv b$(mod m) if and only if there is an integer k such that $a = b + km$.*

Proof is trivial. You can do this as an exercise..

Theorem 2. Congruence as Equivalence Relation. *Let m be a positive integer. Then, congruences modulo m satisfy the following properties:*

1. Reflexive property*: If a is an integer, then $a \equiv a$ (mod m)*
2. Symmetric property*: If a and b are integers such that $a \equiv b$ (mod m), then $b \equiv a$ (mod m).*
3. Transitive property*: If a, b, and c are integers with $a \equiv b$ (mod m) and $b \equiv c$ (mod m), then $a \equiv c$ (mod m).*

Proof. 1. We see that $a \equiv a \pmod{m}$, since $m \mid (a - a) = 0$.

2. If $a \equiv b \pmod{m}$, then $m \mid (a - b)$. Hence, there is an integer k with $km = a - b$. This shows that $(-k)m = b - a$, so that $m \mid (b - a)$. Consequently, $b \equiv a \pmod{m}$.

3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m \mid (a - b)$ and $m \mid (b - c)$. Hence, there are integers k and l such that $km = a - b$ and $lm = b - c$. Therefore, $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. It follows that $m \mid (a - c)$ and $a \equiv c \pmod{m}$.

□

Theorem 2 suggests that the set of integers is partitioned into m different sets called *congruence classes modulo* m, each containing integers that are mutually congruent modulo m.

Now, we will do arithmetic with congruences.

Theorem 3. *If a, b, c, and m are integers with $m > 0$ such that $a \equiv b \pmod{m}$, then:*

1. $a + c \equiv b + c \pmod{m}$
2. $a - c \equiv b - c \pmod{m}$
3. $ac \equiv bc \pmod{m}$

Proof.

1. From $a \equiv b \pmod{m}$, we have $m \mid (a - b)$. Since $a - b = (a + c) - (b + c)$, we have $m \mid ((a + c) - (b + c))$.
2. Similarly, $a - b = (a - c) - (b - c)$, and hence we have $m \mid ((a - c) - (b - c))$.
3. Note that $ac - bc = c(a - b)$. Since $m \mid (a - b)$, it follows that $m \mid c(a - b)$, and hence $ac \equiv bc \pmod{m}$.

□

Example Since $19 \equiv 3 \pmod{8}$, $26 = 19 + 7 \equiv 3 + 7 = 10 \pmod{8}$, $15 = 19 - 4 \equiv 3 - 4 \equiv -1 \pmod{8}$, and $38 = 19 \cdot 2 \equiv 3 \cdot 2 = 6 \pmod{8}$.

However, it should be noted that the congruence doesn't necessarily hold for divisions.

Example We have $14 = 7 \cdot 2 \equiv 4 \cdot 2 = 8 \pmod{6}$. But we cannot cancel the common factor of 2 since $7 \not\equiv 4 \pmod{6}$.

The congruence does hold for division, however, when the divisor is coprime with the modulo m.

Theorem 1. *If a, b, c and m are integers such that $m > 0$, and c, m are relatively prime, and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$.*

Proof.

$$
\begin{aligned}
& ac \equiv bc (\text{mod} m) \\
\implies & m|(ac - bc) = c(a - b) \\
\implies & km = c(a - b) \\
\implies & \text{Since GCD(m,c)=1,} m \mid (a - b) \\
\implies & a \equiv b (\text{mod} m)
\end{aligned}
$$

□

You can even add/subtract/multiply two distinct but congruent numbers on both sides of the congruence.

Theorem 4. *If a, b, c, d, and m are integers such that $m > 0$, $a \equiv b$ (mod m), and $c \equiv d$ (mod m), then:*

1. $a + c \equiv b + d$ *(mod m),*
2. $a - c \equiv b - d$ *(mod m),*
3. $ac \equiv bd$ *(mod m).*

Try this proof on your own.

As a result, we can do mod at any time during computation (and at the end) and still obtain the same result. This is useful if you want to keep the intermediate results of a calculation small.

Example Suppose that you wish to design an algorithm that computes $(a \cdot b) \mod m$, where a and b are as large as 32-bit integers, and m is small. Computing the $ab \mod m$ directly may cause an overflow (as the product of two 32-bit integers can be as large as 64-bit). To resolve this, we can do as follows ($a = 2^{30}, b = 2^{31}, m = 12$):

$$\begin{aligned} ab \mod m &= [(a \mod m)(b \mod m)] \mod m \\ &= [(2^{30} \mod 12)(2^{31} \mod 12)] \mod 12 \\ &= [4 \cdot 8] \mod 12 \\ &= 8 \end{aligned}$$

3 Modular Linear Equations

Suppose you want to solve the following equation, given the value a, b, m:

$$a \cdot x \equiv b \mod m$$

(e.g. If we start at 12:00 and move the hour hand 5 hours each time, how many times does it take to reach 1:00?)

This linear equation sometimes does *not* have solutions. For example, when $a = 2, b = 1, m = 4$, no such value for x exists.

In particular, when $b = 1$, the solution to the equation is called *multiplicative inverse of a*, and we denote it as a^{-1}.

$$a \cdot a^{-1} \equiv 1 \mod m$$

As in the example above, not all values of a and m yield a multiplicative inverse. However, we can say the following.

Theorem 5 (Corollary 31.26 on page 872) . *For any $m > 1$, if $gcd(a, m) = 1$, then the equation $ax \equiv 1$ (mod m) has a unique solution, modulo m. Otherwise it has no solution.*

Therefore, if we let m be some prime number p, all integers in $Z_p \setminus \{0\}$ has a unique multiplicative inverse.

Example Consider Z_5. Then the following holds for each element of $Z_5 \setminus \{0\}$:

$$1 \cdot 1 \equiv 1(\text{mod} 5) \rightarrow 1^{-1} \mod 5 = 1$$
$$2 \cdot 3 \equiv 1(\text{mod} 5) \rightarrow 2^{-1} \mod 5 = 3$$
$$3 \cdot 2 \equiv 1(\text{mod} 5) \rightarrow 3^{-1} \mod 5 = 2$$
$$4 \cdot 4 \equiv 1(\text{mod} 5) \rightarrow 4^{-1} \mod 5 = 4$$

4 Application to Universal Hash Functions

In previous lecture(s), we proved $H_{p,m}$ is universal. During the proof, couple of arguments were possible using these modular arithmetic. Let's look at those arguments again.

Argument 1 First, we let p be a large prime. Since we picked the values a, b for $h_{a,b}$ such that $a \in Z_p^*$ and $b \in Z_p$, both of these values are smaller than p. Now, consider two distinct keys k and l from Z_p. For a given hash function $h_{a,b}$ we let

$$r = (ak + b) \mod p$$
$$s = (al + b) \mod p$$

Then we argued that $r \neq s$. This can be achieved as follows. First, by definition, we have

$$r \equiv ak + b(\mod p)$$
$$s \equiv al + b(\mod p)$$

Subtracting the first congruence by the second congruence, we get

$$r - s \equiv a(k - l)(\mod p)$$

Note that a and $k - l$ are both non-zero. The product $a(k - l)$ cannot be zero modulo p, because p is a prime number. Hence $r - s$ is non-zero, yielding $r \neq s$.

Argument 2 Later in the proof, we solved the above equations for a and b given r and s. We will do this step by step. First of all, since $k - l < p$ and p is a prime, we know that $(k - l)^{-1}$ mod p exists. Hence,

$$\begin{aligned} & r - s \equiv a(k - l) \ (\text{mod} p) \\ \implies & (r - s)(k - l)^{-1} \equiv a(k - l) \cdot (k - l)^{-1} \equiv a \ (\text{mod} p) \\ \implies & a = ((r - s)((k - l)^{-1} \mod p)) \mod p \end{aligned}$$

For b, we can derive similarly:

$$\begin{aligned} & r = (ak + b) \text{mod} p \\ \implies & r \equiv ak + b \ (\text{mod} p) \\ \implies & r - b \equiv ak \ (\text{mod} p) \\ \implies & -b \equiv ak - r \ (\text{mod} p) \\ \implies & b \equiv r - ak \ (\text{mod} p) \\ \implies & b = (r - ak) \mod p \end{aligned}$$