LectureMaterial#4

Information Security

Dr. Abu Nowshed Chy

Department of Computer Science and Engineering

University of Chittagong

Faculty Profile

Division

If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$.

When a divides b we say that a is a factor of b and that b is a multiple of a . The notation a | b denotes that a divides b. We write a ∤ b when a does not divide b.

Division

Let a, b, and c be integers. Then

(*i*) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$;

(*ii*) if $a \mid b$, then $a \mid bc$ for all integers c;

(*iii*) if $a \mid b$ and $b \mid c$, then $a \mid c$.

The Division Algorithm

Let a be an integer and d a positive integer. Then there are unique integers q and r , with $0 \le r < d$, such that $a = dq + r$.

d is called the divisor, a is called the dividend, q is called the quotient, and r is called the remainder. Following notations are used to express the quotient and remainder:

$$q = a \,\mathbf{div}\, d \qquad r = a \,\mathbf{mod}\, d$$

Practice Example

What are the quotient and remainder when 101 is divided by 11?

Solution: We have

$$101 = 11 \cdot 9 + 2.$$

Hence, the quotient when 101 is divided by 11 is $9 = 101$ **div** 11, and the remainder is $2 = 101$ **mod** 11. ◀

Modular Arithmetic

If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$. We use the notation $a \equiv b \ (\mathbf{mod}\ m)$ to indicate that a is congruent to b modulo m. If a and b are not congruent modulo m, we write $a \not\equiv b \ (\mathbf{mod}\ m)$.

Modular Arithmetic

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if

$$a \bmod m = b \bmod m$$

Modular Arithmetic

Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution: Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5 \pmod{6}$. However, because $24 - 14 = 10$ is not divisible by 6, we see that $24 \not\equiv 14 \pmod{6}$. ◀

Modular Arithmetic

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$

Modular Arithmetic

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \qquad \text{and} \qquad ac \equiv bd \pmod{m}.$$

$$7 \equiv 2 \pmod{5} \text{ and } 11 \equiv 1 \pmod{5},$$

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}.$$

Modular Arithmetic (Greatest Common Divisor)

Let a and b be integers, not both zero. The largest integer d such that d | a and d | b is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Modular Arithmetic (Least Common Multiple)

The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by lcm(a , b).

Modular Arithmetic (GCD Linear Combination)

If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

Modular Arithmetic (GCD Linear Combination)

Find the greatest common divisor (GCD) of 414 and 662 using the Euclidean algorithm.

$$662 = 414 \cdot 1 + 248$$
$$414 = 248 \cdot 1 + 166$$
$$248 = 166 \cdot 1 + 82$$
$$166 = 82 \cdot 2 + 2$$
$$82 = 2 \cdot 41.$$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder.

Modular Arithmetic (GCD Linear Combination)

$$\gcd(252, 198) = 18$$

$$\begin{aligned}
252 &= 1 \cdot 198 + 54 \\
198 &= 3 \cdot 54 + 36 \\
54 &= 1 \cdot 36 + 18 \\
36 &= 2 \cdot 18.
\end{aligned}$$

Modular Arithmetic (GCD Linear Combination)

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

$$18 = 54 - 1 \cdot 36$$

$$252 = 1 \cdot 198 + 54$$

$$36 = 198 - 3 \cdot 54$$

$$198 = 3 \cdot 54 + 36$$

$$54 = 1 \cdot 36 + 18$$

$$36 = 2 \cdot 18.$$

$$\begin{aligned} 18 &= 54 - 1 \cdot 36 \\ &= 54 - 1 \cdot (198 - 3 \cdot 54) \\ &= 4 \cdot 54 - 1 \cdot 198 \end{aligned}$$

$$54 = 252 - 1 \cdot 198$$

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = \boxed{4 \cdot 252 - 5 \cdot 198}$$

Modular Arithmetic (GCD Linear Combination)

Example 5. Find $\gcd(41, 12)$ and express it as a linear combination of 41 and 12.

Solution. The algorithm is not needed to find $\gcd(41, 12)$. In fact, 1 and 41 are the only positive divisors of 41, so $\gcd(41, 12) = 1$ because 41 does not divide 12. However, guessing a linear combination $1 = x \cdot 41 + y \cdot 12$ is not easy. The euclidean algorithm gives

$$\begin{aligned} 41 &= 3 \cdot 12 + 5 \\ 12 &= 2 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Hence, $\gcd(41, 12) = 1$ as expected. Elimination of remainders gives

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(12 - 2 \cdot 5) \\ &= 5 \cdot 5 - 2 \cdot 12 \\ &= 5(41 - 3 \cdot 12) - 2 \cdot 12 \\ &= 5 \cdot 41 - 17 \cdot 12 \end{aligned}$$

which is the required linear combination. □

Modular Arithmetic (Practice Problems)

By using Euclidean algorithm, find the *gcd* of the following pairs of integers. Then, express the *gcd* as a linear combination of the pairs of integers.

a. *gcd* (116, 2040)

b. *gcd* (3279, 2073)

Modular Arithmetic

Linear Congruence

A congruence of the form

$$ax \equiv b \ (\text{mod } m)$$

where m is a positive integer, a and b are integers, and x is a variable, is called a *linear congruence*.

- To find all the integers x satisfy this congruence, one method is to find an integer $\bar{a}$ such that $a.\ \bar{a} \equiv 1$ (mod m), if such an integer exists. Such an integer $\bar{a}$ is said to be an *inverse of a modulo m*.

Theorem: If a and ~~b~~ m are relatively prime integers and $m>1$, then an inverse of a modulo m exists. This inverse is unique modulo m.

Proof: Since gcd (a, m) =1, there are integers s and t such that

$$sa + tm = 1$$

this implies that, $\quad sa + tm \equiv 1 \ (\text{mod } m)$

since $tm \equiv 0$ (mod m), it follows that

$$sa \equiv 1 \ (\text{mod } m).$$

Consequently, s is the inverse of a modulo m.

Modular Arithmetic

Solve the congruence equation $33X \equiv 38 \pmod{280}$

$$sa + tm = 1$$

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

3 $33x = 38 \pmod{280}$ ... ... (i)

since gcd (3~~8~~, 280) = 1, the equation has a unique solution. Testing may not be an efficient way to find the solution here. We apply the Euclidean algorithm to find a solution to

$33x \equiv 1 \pmod{280}$ ... ... (ii)

and we find that $33(17) + 280(-2) = 1$

that means that $s = 17$ is a solution for equation (ii). Then

$sb = 17(38) = 646$

is a solution of the original equation (i). Dividing 646 by $m = 280$, we obtain the remainder

$x = 86$

which is the unique solution (i) between 0 and 279.(The general solution is $86 + 280k$ with $k \varepsilon Z$)

Modular Arithmetic

Solve the congruence equation $195X \equiv 23 \pmod{968}$

293


Thank You!