VANDERBILT UNIVERSITY School of Engineering

Discrete Structures

CS 2212

(Fall 2020)

18 – Integers

Chapter - 8

Integers

Integer Division – Review

In integer division, the input and output values must always be integers.

Divisibility:

$\boldsymbol{m \mid n}$ (read m divides n)

if $m \neq 0$ and $n = km$ for some integer k (e.g., $3 \mid 6$).

Important **properties** of divisibility:

- If $d \mid a$ and $a \mid b$ then $d \mid b$
- (Linear combination) If $d \mid a$ and $d \mid b$ then $d \mid (ax + yb)$ for any integers x, y

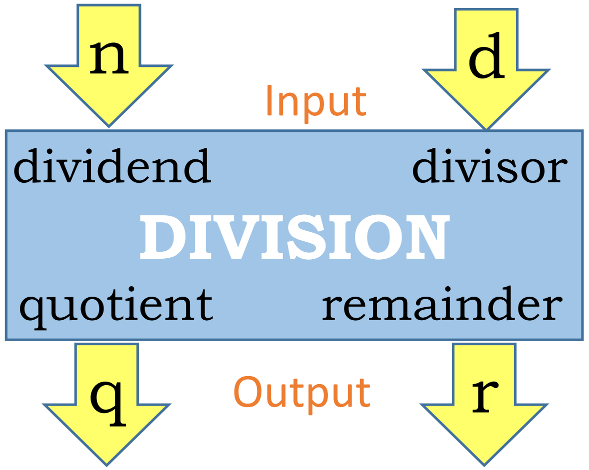
Division Algorithm

Let n be an integer and let d be a positive integer. Then, there are *unique* integers q and r, with $0 \le r < d$, s.t.

$$\boldsymbol{n = qd + r}.$$

q: quotient

r: remainder



div gives quotient: q = n div d

mod gives quotient: r = n mod d

Mod (modulo) Operation

How to calculate the **mod**, that is, n mod d?

For $n, d \in Z$ with $d > 0$, apply the division algorithm

$$n = dq + r, \qquad \text{(here, } 0 \le r < d\text{)}$$

The remainder ***r*** is the value of the mod function applied to n and d.

The mod function is defined as the amount by which a number exceeds the largest integer multiple of the divisor that is **not greater** than that number.

Mod (modulo) Operation

Positive numbers and mod:

- 11 mod 5 = 1
- 14 mod 5 = 4
- 5 mod 11 = 5
- 5 mod 14 = 5

Negative numbers and mod:

- -17 mod 5 = 3
- -99 mod 8 = 5

Modular Arithmetic

Addition mod m

Add two numbers and apply mod m to the result.

Multiplication mod m

Multiply two numbers and apply mod m to the result.

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

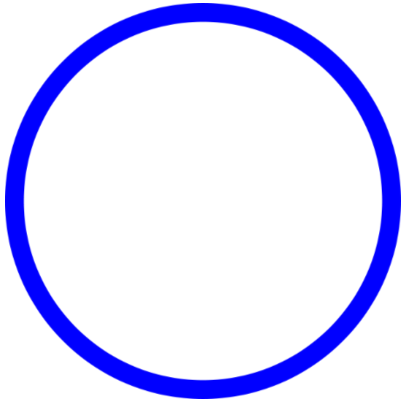
Multiplication and addition **mod 5**.

Ring

Using these *generalized* definitions of addition and multiplication, we define a powerful algebraic structure called a **ring**.

Ring: The set {0, 1, 2,…, m-1} along with addition and multiplication **mod m** defines a closed mathematical system with m elements called a ring.

$\mathbf{Z_m}$ denotes a ring based on the set {0, 1, 2,…, m-1} with addition and multiplication mod m



Modular Arithmetic – Applications

Cryptography

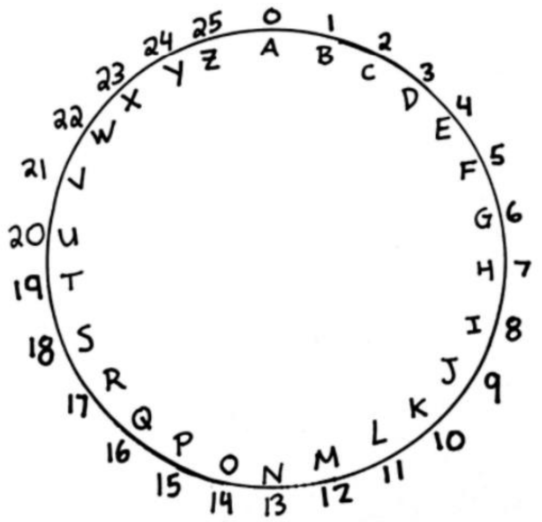
Plain text: **Mods are fun**
Ciphered Code: **Jlsp xob crk**

Shifted each letter to the right by 23 letters.

Is this a **mod** operation?

M: 12
M shifted to right by 23: J = 9
But: $(12 + 23) \bmod 26 = 9$

o: 14
o shifted to right by 23: l = 11
But: $(14 + 23) \bmod 26 = 11$



Cipher: $(x + s) \bmod 26$

- x: Number corresponding to the actual letter
- s: Shift
- 26: Total number of letters

Also known as **Ceaser cipher.**

Mod Properties

Let m be an integer larger than 1. Let x and y be any integers. Then

$$[(x \bmod m) + (y \bmod m)] \bmod m = (x + y) \bmod m$$

$$[(x \bmod m)(y \bmod m)] \bmod m = (x \cdot y) \bmod m$$

Mod Properties

$$[(x \bmod m) + (y \bmod m)] \bmod m = (x + y) \bmod m$$

L.H.S $[(x \bmod m) + (y \bmod m)] \bmod m$

$= [(x - km) + (y - jm)] \bmod m$

$= [(x + y) - (k + j)m] \bmod m.$

$= (x + y) \bmod m$

(Since $[(x + y) - (k + j)m]$ and $(x+y)$ differ only by a multiple of m.)

Similarly, we can show

$$[(x \bmod m)(y \bmod m)] \bmod m = (x \cdot y) \bmod m$$

Mod Properties

Question: What is $(651^{23} + 17) \bmod 10$?

$$(651^{23} + 17) \bmod 10 = [(651^{23} \bmod 10) + (17 \bmod 10)] \bmod 10$$

Lets compute first:

$$(651^{23} \bmod 10) = (651 \bmod 10)^{23} \bmod 10$$

$$= (1)^{23} \bmod 10 = 1$$

So, we get,

$$(651^{23} + 17) \bmod 10 = [1 + (17 \bmod 10)] \bmod 10$$

$$= [1 + 7] \bmod 10 = 8$$

Mod Properties

$$A^B \text{ mod } C = ((A \text{ mod } C)^B) \text{ mod } C$$

Example: $A^2 \text{ mod } C = (A*A) \text{ mod } C$

$= ((A \text{ mod } C) * (A \text{ mod } C)) \text{ mod } C$

$= (A \text{ mod } C)^2 \text{ mod } C$

What is $2^{90} \text{ mod } 13$?

How to approach this?

- Use a calculator?
- Could cause an overflow.

Mod Properties

$2^{90} = (2^{40} * 2^{40} * 2^{10}) \bmod 13$

$= ((2^{40} \bmod 13) * (2^{40} \bmod 13) * (2^{10} \bmod 13)) \bmod 13$

Lets compute (2^{40} mod 13) first.

$2^{40} \bmod 13 = ((2^{20} \bmod 13) * (2^{20} \bmod 13)) \bmod 13$

$= (9 * 9) \bmod 13 = 3$

$2^{90} = (2^{40} * 2^{40} * 2^{10}) \bmod 13$

$= (3 * 3 * 10) \bmod 13$

$= 12$

Congruence

Let m be an integer > 1. Let x and y be any two integers. Then **x is congruent to y mod m** if x mod m = y mod m.

The fact that x is congruent to y mod m is denoted as

$$x \equiv y \pmod{m}.$$

Alternatively, let m be an integer > 1. Let x and y be any two integers. Then,

$x \equiv y \pmod{m}$ if and only if $m \mid (x - y)$.

Congruence

Alternatively, let m be an integer > 1. Let x and y be any two integers. Then,

$$x \equiv y \pmod{m} \text{ if and only if } m \mid (x - y).$$

First, we show: $x \equiv y \pmod{m} \rightarrow m \mid (x - y)$.

$x \equiv y \pmod{m} \quad \rightarrow \quad x \bmod m = y \bmod m$

Therefore, $x = k_1 m + r$ for some integer k_1, and
$y = k_2 m + r$ for some integer k_2.

Now, $(x - y) = (k_1 - k_2)\, m$

Since $(k_1 - k_2)$ is an integer, which means $m \mid (x - y)$.

Congruence

Alternatively, let m be an integer > 1. Let x and y be any two integers. Then,

$x \equiv y \pmod{m}$ if and only if $m \mid (x - y)$.

Next, we show: **$m \mid (x - y) \rightarrow x \equiv y \pmod{m}$.**

$m \mid (x - y) \rightarrow (x - y) = tm$ for some integer t.

Let $(x \bmod m) = r \rightarrow x = km + r$, for some integer k.

Note $y = x - (x - y)$

$= (km + r) - tm = (k - t)m + r$,

which means $r = (y \bmod m)$

Hence, $x \equiv y \pmod{m}$.

Greatest Common Divisor (GCD)

If x and y are integers, not both zero, then **gcd(x, y)** is the largest integer that divides both x and y.

Examples:

- gcd(12, 15) = 3
- gcd(–12, –8) = 4

Euclid’s Algorithm for Finding GCD

Example: Rachel has

6 cans of Pepsi

15 water bottles

She wants to create identical refreshment tables that will operate during their high school football game. She was told she must put all beverages out on the table initially.

Question: What is the greatest number of refreshment tables that Rachel can stock?

Euclid's Algorithm for Finding GCD

gcd(189,33) = ?

y	x	r = y mod x
189	33	24
33	24	9
24	9	6
9	6	3
6	3	0

gcd(189,33) = **3**

Euclid's Algorithm for Finding GCD

Input:

Two positive integers, x and y.

Output:

gcd(x, y).

```
If ( y < x )
    Swap x and y.
r = y mod x.

While ( r ≠ 0 )
    y := x
    x := r.
    r := y mod x.
End-while


Return( x )
```

Greatest Common Divisor (GCD)

GCD Theorem:

Let x and y be two positive integers. Then

$$\textbf{Gcd}\,(x\,,\,y) = \textbf{Gcd}\,(y \bmod x\,,\,x).$$

We show that:

k is a factor of both x and y

if and only if

k is a factor of both x and $(y \bmod x)$

Greatest Common Divisor (GCD)

(→) Assume k is a factor of both x and y

- Then, k is a factor of any linear combination of x and y.
- So, we just need to show that (y mod x) is a linear combination of x and y.
- Let y mod $x = r$
- $y = xq + r$
- $r = y - qx$ (linear combination of x and y)

Greatest Common Divisor (GCD)

($\leftarrow$) Assume k is a factor of both x and (y mod x).

We need to show that k is also a factor of y

- Let y mod $x = r$
- $y = xq + r$
- We know that k is a factor of x, and k is a factor of r. So, k is also a factor of their linear combination.
- Since y is indeed a linear combination of x and r, so k is also a factor of y. QED.

Some Properties of GCD

$$\gcd(x, y) = \gcd(y \bmod x, x).$$

$$\gcd(a, b) = \gcd(b, a) = \gcd(a, -b)$$

$$\gcd(a, b) = \gcd(b, a - bq) \text{ for } \textit{any} \text{ integer } q$$

$$\gcd(a, b) = ma + nb \text{ for some } m, n \in Z$$

If $d \mid ab$ and $\gcd(d, a) = 1$, then $d \mid b$

Extended Euclid Algorithm

The extended Euclidean algorithm says that:

The gcd of a and b can be expressed as a linear combination of a and b.

In other words, $\gcd(a, b) = ma + nb$ for some integers m, n.

Bezout's Identity

Extended Euclid Algorithm

Prove: gcd(a, b) = ma + nb for some m, n $\in$ **Z**

Proof:

Let g be any positive linear combination of a and b.

$$g = xa + yb > 0$$

Since gcd(a, b) divides a and b (by definition), so gcd(a, b) also divides g. Thus,

$$g = c \gcd(a, b) \qquad \text{for some integer } c$$

Thus,

$$\gcd(a, b) \le g.$$

Recall WOP

In particular, if g' = ma + nb is the *smallest* positive linear combination of a and b, then

$$\mathbf{gcd(a, b) \le g'}$$

Extended Euclid Algorithm

Proof (continued):

Now, $g' = ma + nb$

Dividing a by g', we get

$$a = sg' + r \qquad \text{with } 0 \leq r < g'$$

$$r = a - sg' = a - s(ma + nb)$$

$$r = a(1 - sm) - snb$$

So r is a positive linear combination of a and b and is less than g'.

But we said g' is the smallest positive linear combination. So

$$r = 0.$$

Extended Euclid Algorithm

Proof (continued):

So, g' divides a.

Similarly, g' divides b. Thus, g' is a factor of a and b.

Since gcd(a, b) is the greatest common factor, so

$$g' \leq \gcd(a, b)$$

Previously, showed $g' \geq \gcd(a, b)$.

Hence,

$$\gcd(a, b) = g'$$
$$= ma + nb; \quad \text{for some integers } m \text{ and } n.$$

QED.

Extended Euclid Algorithm

Extended Euclidean Algorithm:

The algorithm used to find the coefficients, x and y, such that

$$\gcd(a, b) = ma + nb,$$

is called the Extended Euclidean Algorithm.

Example:

We know that: gcd (252, 198) = 18.

Express 18 as a linear combination of 252 and 198.

18 = (4) 252 + (-5) 198

Extended Euclid Algorithm

gcd(675,210) = (?) 675 + (?) 210

y	x	r = y mod x
675	210	45
210	45	30
45	30	15
30	15	0

= y – (k x)

45 = 675 – (3) 210

30 = 210 – (4) 45

15 = 45 – (1) 30

Use these expressions to solve:

15 = (?) 675 + (?) 210

Extended Euclid Algorithm

gcd(675, 210) = (5) 675 + (-16) 210

r = y – k x

45 = 675 – (3) 210

30 = 210 – (4) 45

15 = 45 – (1) 30

15 = (5) 675 + (-16) 210

15 = 5 (675 – (3)210) – 210

15 = (5) 45 – 210

15 = 45 – (210 – (4) 45)

15 = 45 – 30

Back substitution

Extended Euclid Algorithm

1. Find the **gcd(252, 198).**
2. Also express it as a linear combination of 252 and 198.

Solution:

1. gcd(252, 198) = 18
2. 18 = (4) 252 – (5) 198