GCDs and LCMs

Let $a, b \in \mathbb{Z}$ (not both 0)

$\gcd(a,b)$ = greatest common divisor of a and b
= the largest integer that divides a and b
= $\max\{d \in \mathbb{Z} : d \mid a \text{ and } d \mid b\}$
(Used to reduce fractions)

Ex $\gcd(90,100) = 10$
Ex $\gcd(24,48) = 24$
Ex $\gcd(13,14) = 1$

relatively prime $\Leftrightarrow$ gcd = 1

Let $a, b \in \mathbb{Z}^+$.
$\text{lcm}(a,b)$ = least common multiple of a and b
= the smallest positive integer divisible by a and b
= $\min\{m \in \mathbb{Z}^+ : a \mid m \text{ and } b \mid m\}$
(Used to find the LCD.)

Ex $\text{lcm}(8,9) = 72$
If a, b are relatively prime, $\text{lcm}(a,b) = ab$

Ex $\text{lcm}(4,12) = 12$
Ex $\text{lcm}(6,10) = 30$

Finding GCDs and LCMs Using Prime Fac'ns

Ex find gcd(200,1500)

$$200 = 2^3 \qquad \cdot 5^2$$
$$1500 = 2^2 \cdot 3 \cdot 5^3$$

} Prime fac'ns from factor trees.

Put in 0, 1 exponents:

$$200 = 2^3 \cdot 3^0 \cdot 5^2$$
$$1500 = 2^2 \cdot 3^1 \cdot 5^3$$
$$gcd = 2^2 \cdot 3^0 \cdot 5^2$$
$$= \boxed{100}$$

← for each prime, take the smaller exponent

In general, to find gcd(a,b):
Find the prime fac'ns of a and b.
Let $p_1, p_2, \ldots, p_n$ be the primes that appear in the prime fac'n of a or b.

Let $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$
$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ } $a_i, b_i \in \mathbb{Z}^{\geq 0}$

Then, $gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$

Here, $gcd(200,1500) = 2^{\min(3,2)} \cdot 3^{\min(0,1)} \cdot 5^{\min(2,3)}$
$= 2^2 \cdot 3^0 \cdot 5^2$
$= \boxed{100}$

<u>Ex</u> find lcm (200, 1500)

$$\begin{aligned} 200 &= 2^3 \cdot 3^0 \cdot 5^2 \\ 1500 &= 2^2 \cdot 3^1 \cdot 5^3 \\ \hline \text{lcm} &= 2^3 \cdot 3^1 \cdot 5^3 \\ &= \boxed{3000} \end{aligned}$$

← for each prime take the <u>larger</u> exponent

In general, to find lcm(a,b):

same as finding gcd(a,b), except

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

If $a,b \in \mathbb{Z}^+$, then $ab = \gcd(a,b) \cdot \text{lcm}(a,b)$

(HW #33)

<u>Special Case</u>

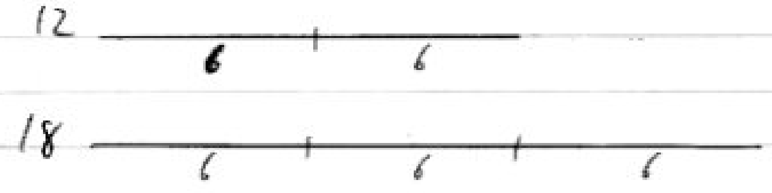
If a,b are relatively prime

$\gcd(a,b) = 1$
$\text{lcm}(a,b) = ab$

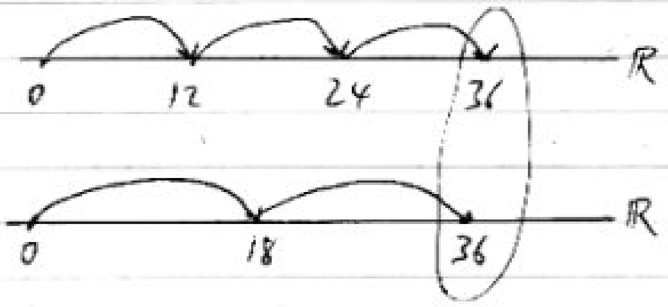
> product = ab

Pictures

$\gcd(12,18)=6$



$\operatorname{lcm}(12,18)=36$



L2-9
2.3

THE DIVISION "ALGORITHM"

55 is divisible by 5, because

$$55 = 5\cdot 11$$

57 is <u>not</u>

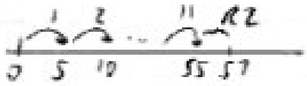
$$\begin{array}{r} 11 \text{ R } 2 \\ 5\,\overline{)\,57} \\ \underline{-5} \\ 07 \\ \underline{-5} \\ 2 \end{array}$$

$$57 = 5\cdot 11 + 2$$

dividend, divisor, quotient, remainder

quotient $= \lfloor \frac{57}{5} \rfloor = \lfloor 11.4 \rfloor$

remainder (must be 0, 1, 2, 3, or 4 when $\div$ by 5) (i.e., $r \in \mathbb{Z}, 0 \le r < 5$)



Let $a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$
Then, there are unique $q, r \in \mathbb{Z}$ $(0 \le r < d)$
such that $a = dq + r$

dividend (given), divisor (given), quotient $= \lfloor \frac{a}{d} \rfloor$, remainder

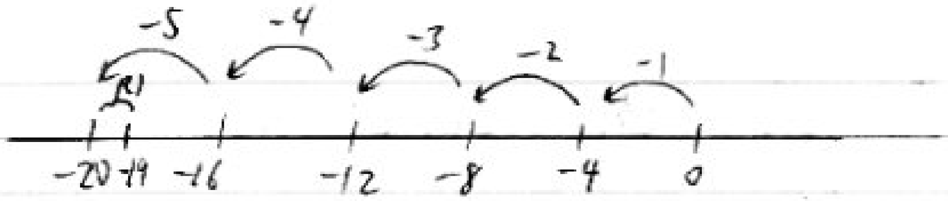
$d \mid a \Leftrightarrow r = 0$

<u>Ex</u> What are the quotient and remainder when -19 is divided by 4?

quotient $= \lfloor \frac{a}{d} \rfloor = \lfloor \frac{-19}{4} \rfloor = \lfloor -4\frac{3}{4} \rfloor = -5$
remainder $= a - dq = -19 - (\quad)$

$$-19 = \underbrace{(4)(-5)}_{-20} + \underbrace{1}_{\text{remainder}}$$

$q = -5$, $r = 1$



Next: Classify integers according to their remainders when you divide by a given divisor.

Ex divisor = "modulus" = 5

Imagine wheel spokes:

R0 $\equiv 0 \pmod 5$

10

5

0

$\equiv 4 \pmod 5$ R4 14 9 4 -1 ◌ -4 1 6 11 R1 $\equiv 1 \pmod 5$

-2 -3

3 2

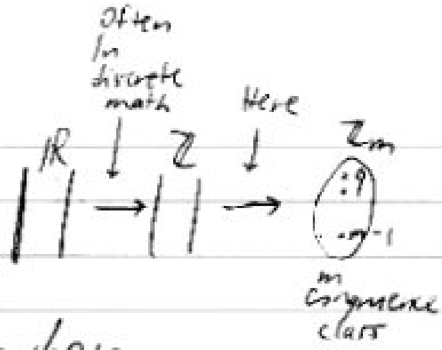
8 7

13 12

R3 R2

$\equiv 3 \pmod 5$ $\equiv 2 \pmod 5$

5 congruence classes



MODULAR ARITHMETIC (Gauss)

$(a)_m$ notation

Let $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$.
Then, a mod m = the remainder when a is divided by m

Ex $11 \bmod 5 = 1$

$$\underset{a}{11} = \underset{d \text{ or } m}{5} \cdot \underset{q}{2} + \underset{r}{1}$$

Ex $-1 \bmod 5 = 4$

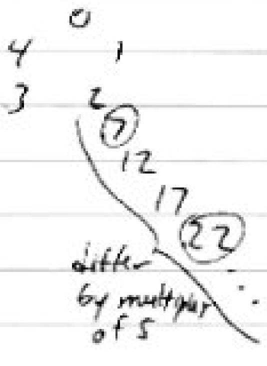
Ex $978 \bmod 7 = ?$ $\quad \lfloor \frac{978}{7} \rfloor = 139 \quad 139 \times 7 = 973$ largest multiple of $7 \le 978$

$r = 978 - 973 = 5$.

Let $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$.
a is congruent to b modulo m, or "$a \equiv b \pmod m$"
$\Leftrightarrow$ a mod m = b mod m (a, b have same r when ÷ by m)
$\Leftrightarrow m \mid (a-b)$
$\Leftrightarrow$ ~~$\exists k \in \mathbb{Z}\ (a = b + km)$~~ (☆) (spokes: ~~a, b can differ by some multiple of m~~)

Ex $7 \equiv 2 \pmod 5$, $22 \equiv 2 \pmod 5$ $\Rightarrow 7 \equiv 22 \pmod 5$

Also: $5 \mid \underbrace{(22-7)}_{15}$



Ex $7 \not\equiv 23 \pmod 5$

Prove $a \equiv b \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z}\ (a = b + km)$ (✱)

$a \equiv b \pmod{m}$
$\Leftrightarrow m \mid (a-b)$
$\Leftrightarrow \exists k \in \mathbb{Z}\ (a - b = km)$
$\Leftrightarrow \exists k \in \mathbb{Z}\ (a = b + km)$

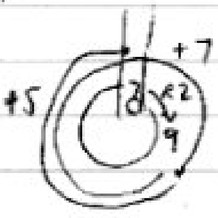
To be on the same spoke, a and b can differ by a multiple of m.

Poss. exam? Math 127 So, $a \equiv b \pmod{m}$ $\Rightarrow a^n \equiv b^n \pmod{m}$ for $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}^{\geq 0}$

If $a \equiv b \pmod{m}$, and
$c \equiv d \pmod{m}$, then

$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$
(Proofs helpful for HW) p.122 Do +

(mod 5) better do Ex 1st

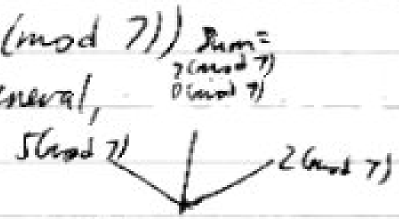


Only the remainders matter as far as spokes go.

Ex $9 \equiv 2 \pmod{7}$
$12 \equiv 5 \pmod{7}$

$\Rightarrow 9 + 12 \equiv 2 + 5 \pmod{7}$
$21 \equiv 7 \pmod{7}$ ✓ (Both $\equiv 0 \pmod{7}$)

In general,



and

$108 \equiv 10 \pmod{7}$ ✓ (Both $\equiv 3 \pmod{7}$) × picture

APPLICATIONS

Hashing functions

Storing records that are uniquely identified by a key "k" (e.g., SSN).

Division Method:

$$\underbrace{h(k)}_{\text{memory location}} = k \pmod{\underset{\uparrow}{m}}$$

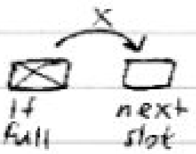
memory locations

"Folding" the list of possible SSNs.

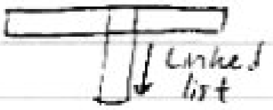
We might get collisions!

Resolutions

① Rosen: Linear probing



② Separate chaining



Requires dynamic memory allocation.

Ex Pseudorandom #s (games, simulations, ...

We want a sequence of "random" #s between 0,1.

Most computers use the linear congruential method.

Seed x_0
Recursive def'n:
$$x_{n+1} = (ax_n + c) \pmod{m}$$

Output: $\frac{x_0}{m}, \frac{x_1}{m}, \frac{x_2}{m}, \ldots$

Ex Cryptology

Do p.122 proofs?