Divisibility and the Euclidean Algorithm Lecture 2c: 2022-01-19

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Abstract definition and examples

- A positive integer a is divisible by another positive integer b if $a \div b = \frac{a}{b} = c$, where c is a positive integer.
- Equivalently, $a \div b$ has no remainder.
- Alternately, there exists a positive integer c such that $bc = a$.

Ex. $24 \div 6 = \frac{24}{6} = 4$ $\quad (4 \times 6 = 24)$ divisible!

Ex. $17 \div 1 = \frac{17}{1} = 17$ $\quad (17 \times 1 = 17)$ divisible!

Ex. $17 \div 2 = \frac{17}{2} = 8\frac{1}{2}$ $\quad$ 8 rem 1 $\quad (8 \times 2 + 1 = 17)$ not divisible!

- Is 51 divisible by 13?
- Is 51 divisible by 17?

$51 \div 13 = 3$ rem 12 $\quad (51 - 39 = 12)$

$51 = 17 \times 3$

A: Yes
B: No
C: Maybe
E: None of the above

Long division

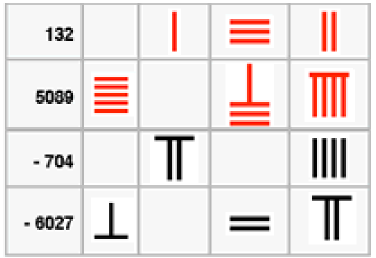
- Division is the opposite of multiplication, but it is somehow "harder" than multiplication and involves lots of multiplications.
- Example:

```
      4526   rem 9
 12 ) 54321
      48
       63
       60
        32
        24
         81
         72
          9
```

- Sometimes, reversing operations is harder.

History of operations

- Negative numbers were invented circa 202 BCE – 220 CE in China.
- Multiplication was invented around 4000 BCE by the Babylonians.
- The Babylonians didn't have direct division, but could multiply by inverses.



Ex. Say we know $\frac{1}{5} = 0.2$

Then $\frac{11}{5} = 11 \times 0.2 = 2.2$

When was direct division invented?

A: Before 1000 BCE
B: 1000 BCE to 1000 CE
C: 1000 CE to 1500 CE
D: 1500 CE to 1800 CE
E: After 1800 CE

Rhind papyrus, British Museum 10057
https://en.wikipedia.org/wiki/Rhind_Mathematical_Papyrus

~1500 BCE, Egypt

When was modern long division invented?

A: Before 1000 BCE
B: 1000 BCE to 1000 CE
C: 1000 CE to 1500 CE
D: 1500 CE to 1800 CE
E: After 1800 CE

$5 \overline{)1513}$

Henry Briggs, 1560-1630

Professor at Oxford University

What numbers are divisible by 4?

- Solution 1: we can just list out numbers and test them.

~~1~~ ~~2~~ ~~3~~ 4 ~~5~~ ~~6~~ ~~7~~ 8 ~~9~~ ~~10~~ ~~11~~ 12

~~13~~ ~~14~~ ~~15~~ 16 ~~17~~ ~~18~~ ~~19~~ 20 ~~21~~ ~~22~~ ~~23~~ 24

- Solution 2: once we know the pattern, we can recognize that it's just all multiples of 4, which we could also prove.

If a is divisible by 4, then $\frac{a}{4} = b$, so $a = 4b$

If $a = 4b$, then $\frac{a}{4} = b$, so a is divisible by 4.

Thus, the numbers divisible by 4 are just all the multiples of 4.

What numbers are divisible by both 4 & 6?

- Obviously, $24 = 4 \times 6$ is divisible by both 4 & 6.
- Also, any multiple of 24 is divisible for the following reason:

If $a = 24b$, then $\frac{a}{4} = \frac{24b}{4} = 6b$, an integer,

so a is divisible by 4.

If $a = 24b$, then $\frac{a}{6} = \frac{24}{6}b = 4b$, an integer,

so a is divisible by 6.

Thus, multiples of 24 are divisible by both 4 & 6.

Are any other numbers divisible by 4 & 6?

- Solution 1: test all numbers for divisibility.
- Solution 2: list out numbers divisible by 4, and list out numbers divisible by 6, and look for any overlapping numbers.

A: Yes
B: No
C: Maybe
E: None of the above

4b: 4 8 12 16 20 24, 28, 32, $\boxed{36}$

6b: 6 12 18 24 30 $\boxed{36}$ 42 , ...

So 12, 24, 36 are divisible by both

- Hypothesis (guess): all multiples of 12 are divisible by 4 and 6.

Proof of hypothesis

- Claim: the set of all numbers divisible by both 4 and 6 is exactly all multiples of 12.
- Proof step 1: show that all multiples of 12 are divisible by 4 & 6.

If $a = 12b$, (a, b integers), then

$\frac{a}{4} = 3b$ and $\frac{a}{6} = 2b$, so a is divisible by both 4 & 6.

- Proof step 2: show that all numbers divisible by 4 & 6 are multiples of 12.

Suppose $a = 12b + r$, where r is one of $1, 2, \ldots, 11$

Then $\frac{a}{4} = 3b + \frac{r}{4}$ and $\frac{a}{6} = 2b + \frac{r}{6}$. In order to be divisible by both 4 & 6, $\frac{r}{4}$ and $\frac{r}{6}$ must both be integers.

But, no integer b/t 1 & 11 works, so a cannot be divisible by both.

General rule: least common multiples

- Problem: given two numbers a and b, what numbers are divisible by both a and b?
- Solution: the least common multiple $lcm(a, b)$, defined the be the smallest number that is a multiple of both a and b.

Ex. $lcm(6,9) = 18$

The numbers divisible by 6 & 9 are the multiples of 18.

6, 12, 18, 24

9, 18

Ex. $lcm(15,21) = 105$

15 30 45 60 75 90 105

21 42 63 84 105

General proof sketch

- Earlier we proved that the set of numbers divisible by 4 and 6 is exactly the multiples of 12.
- We can prove that the set of numbers divisible by a and b is exactly the multiples of $lcm(a, b)$ using the same ideas.
- First prove that any multiple of $lcm(a, b)$ is divisible by both a and b.

$$\frac{c \cdot lcm(a,b)}{a} = c \cdot \frac{lcm(a,b)}{a}$$

integer b/c $lcm(a,b)$ is a multiple of a

- Then prove that if a number is not a multiple of $lcm(a, b)$, then it will have a remainder when divided by one of a or b.

$c \cdot lcm(a,b) + r$ is divisible by a if $\frac{r}{a}$ is an integer

b if $\frac{r}{b}$ is an integer

But, if r is multiple of both a and b, it cannot be smaller than $lcm(a,b)$

Try it out

- What is the set of numbers divisible by 14 and 21?

14 28 42

21 42

A: All multiples of 14
B: All multiples of 21
C: All multiples of 28
D: All multiples of 42
E: None of the above

- What is the set of numbers divisible by 2 and 10?

2 4 6 8 10

10

A: All multiples of 2
B: All multiples of 10
C: All multiples of 20
D: All multiples of 40
E: None of the above

Can we find the $lcm(a, b)$ faster?

- Sometimes, the $lcm(a, b) = ab$

Ex. $\quad lcm(3,5) = 15 \qquad 3, 6, 9, 12, \underline{15}$

$5, 10, \underline{15}$

- Sometimes, the $lcm(a, b) = a$, where $a > b$.

Ex. $\quad lcm(2,8) = 8 \qquad 2, 4, 6, \underline{8}$

$\underline{8}$

- When $a > b$, $lcm(a, b) \neq b$, because a positive multiple of a cannot be smaller than a itself.
- Can we figure out when the other two cases are true?

Sometimes, the $lcm(a, b) = \max(a, b)$

- When is this true? Let's take a look at a couple of examples.

$lcm(2,4)=4$ $lcm(2,8)=8$

$lcm(2,6)=6$ $lcm(4,8)=8$

$lcm(3,6)=6$ $lcm(8,8)=8$

- Note: it seems to always happen when the bigger number is a multiple of the smaller.
- This makes sense because if the least common multiple is the larger number, that means that the larger number is a multiple of the smaller number.

lowest / least common multiple

Sometimes, the $lcm(a, b) = ab$

- When is this true?

Respond in chat with hypotheses

a	b	ab	$lcm(a, b)$	$\frac{ab}{lcm(a, b)}$
2	5	10	10	1
4	6	24	12	2
3	7	21	21	1
4	9	36	36	1
9	15	135	45	3
10	21	210	210	1
14	21	294	42	7
15	21	315	105	3
12	22	264	132	2
8	27	216	216	1

Do you notice anything about the right-most column and its relationship to a & b?

Greatest common divisors

- Let $\gcd(a, b)$ be the largest number dividing both a and b.

Ex. $\gcd(4,6) = 2$ $\gcd(5,10) = 5$

$\gcd(9,33) = 3$ $\gcd(1,5) = 1$

- Important Theorem: For any two numbers a and b, $lcm(a, b) = \frac{ab}{\gcd(a,b)}$ or equivalently, $ab = lcm(a, b) \times \gcd(a, b)$

Ex. $\gcd(4,6) = 2$ $lcm(4,6) = 12$

$4 \times 6 = 2 \times 12 = 24$

Can we find the $\gcd(a, b)$ faster?

- If we can find the gcd, we can find the lcm, and vice versa, by just dividing from the product.
- But now we have to ask if we can quickly find the gcd.
- One solution is to write out all the divisors of both.

Ex. Find $\gcd(9, 12) = 3$

Divisors of 9: 1, ~~2~~, $\boxed{3}$, ~~4~~, ~~5~~, ~~6~~, ~~7~~, ~~8~~, 9

Divisors of 12: 1, 2, $\boxed{3}$, 4, ~~5~~, 6, ~~7~~, ~~8~~, ~~9~~, ~~10~~, ~~11~~, 12

- Not much faster than finding lcm directly.

Multiples of 9: 9, 18, 27, $\boxed{36}$

Multiples of 12: 12, 24, $\boxed{36}$

$\mathrm{lcm}(9, 12) = 36$

$9 \times 12 = 3 \times 36$

Smarter method (Euclid's algorithm)

- Find the $d = \gcd(30, 69)$

If $\underbrace{\frac{30}{d}}_{x}$ and $\underbrace{\frac{69}{d}}_{y}$ are integers, then so is $\frac{30}{d} + \frac{69}{d}$

Then $x+y$, $x-y$, $2x+y$, $x-3y$, etc. are integers (might be negative)

Now $69 \div 30 = 2$ remainder 9. $\quad 69 = 30 \cdot 2 + 9$

$$\Rightarrow 69 - 30 \cdot 2 = 9$$

$$\Rightarrow \underbrace{\frac{69}{d}}_{x} - \underbrace{\frac{30}{d}}_{y} \cdot 2 = \frac{9}{d}$$

, so $\frac{9}{d}$ is an integer, so d divides 9.

Conversely, $\gcd(9, 30)$ also divides 69, so

$$\gcd(30, 69) = \gcd(9, 30)$$

Continuing gcd(30,69)

- $\gcd(30,69) = \gcd(9,30)$

Notice $30 = 3 \cdot 9 + 3$, $30 \div 9 = 3$ rem 3

$\gcd(9, 30) = \gcd(3, 9) = 3$

$\Rightarrow \gcd(30, 69) = 3$

The Euclidean Algorithm

- To find the $\gcd(a, b)$, with $b > a$:
- Divide a into b, and let r be the remainder.
  - If $r = 0$, then we're done; a divides b and $\gcd(a, b) = a$.
  - If $r \neq 0$, then we replace (a, b) with (r, a) and repeat.

Ex.

$\gcd(24, 1000) = \gcd(16, 24)$

$= \gcd(8, 16) = \underline{8}$

41 r 16

24) 1000

96

40

24

16

Try it out

- Find the gcd(24,1234) $= \gcd(10, 24) = \gcd(4, 10)$

$$= \gcd(2, 4)$$

$$= 2$$

$$\begin{array}{r} 51 \text{ r } 10 \\ 24\overline{)1234} \\ \underline{120} \\ 34 \\ \underline{24} \\ 10 \end{array}$$

$$\begin{array}{r} 2 \text{ r } 4 \\ 10\overline{)24} \\ \underline{20} \\ 4 \end{array}$$

A: 2
B: 3
C: 4
D: 6
E: None of the above

Try it out

- Find the least common multiple of 36 and 3222?

A: 3222
B: 6444
C: 9333
D: 12888
E: None of the above