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 $bc = a$.

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

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

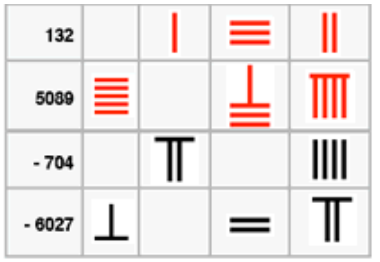
Long division

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

- 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.



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

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

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.

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

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 for the following reason:

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

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

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.

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.

- 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.

Try it out

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

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?

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

- 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.

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.

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

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.

Smarter method (Euclid's algorithm)

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

Continuing $\gcd(30,69)$

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

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.

Try it out

- Find the $\gcd(24,1234)$

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