Fundamental Theorem of Arithmetic
Lecture 4b: 2022-02-02

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Multiplicative building blocks

- What kind of building blocks are the primes?

A: Legos, separable and discrete.

B: Paint colors, once mixed, inseparable.

Division of Lego structures

- Suppose I have this Lego structure I built. If I divide it into two substructures, can I separate the yellow part?
- What about the gray part?
- What about the red part?

- Individual Lego pieces can't be split across the two halves, but combinations of Lego pieces can.

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

What is a prime?

- A prime number p is divisible by only 1 and p.
- The set of prime numbers is the smallest set of multiplicative building blocks needed to generate all positive integers > 1.

Another consequence of primes

- When is a product ab of two numbers a and b even?

A: When a is even
B: When b is even
C: When both a and b are even
D: When a or b are even
E: None of the above

- When is a product ab of two numbers a and b divisible by 3?

A: When a is divisible by 3
B: When b is divisible by 3
C: When 3 divides by a and b
D: When 3 divides either a or b
E: None of the above

- When is a product ab of two numbers a and b divisible by 6?

A: When a is divisible by 6
B: When b is divisible by 6
C: When 6 divides by a and b
D: When 6 divides either a or b
E: None of the above

Analogy to legos – punchline

- A prime is a basic building block that you cannot separate further, like this 2x4 yellow building block.

- A composite number, like this 2x4 red structure, can still be used as a building block, but when you divide up the structure, you can separate it.

Divisibility by 3: direct checking

- How can we convince ourselves that in a product ab that is divisible by 3, at least one of a or b is divisible by 3?
- One way is to check every number divisible by 3, but then we have to check every combination of divisors.

Divisibility by 3: checking opposite

- Another easier way is to check every product of a and b where both are NOT divisible. Then we just have to check divisibility by 3 of ab each time.

Proof by Euclidean algorithm

Conclusion to proof

- Assume ab is divisible by 3.
- Case 1: a is not divisible by 3. Then b is divisible by 3.
- Case 2: a is divisible by 3.
- Therefore, if ab is divisible by 3, then at least one of a or b is divisible by 3.
- ---
- Does the argument hold if we replace 3 with 5?
- What about if we replace 3 with 6?
- What goes wrong when we replace 3 with 6?

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

Primes and factoring

- **If a prime number p divides a product of numbers, then it must divide one of the factors.**

- Try it out:
- 1089746112 is divisible by 91 and 97.
- $1089746112 = 436597 \times 2496$

A: At least one of 436597 or 2496 is divisible by 91
B: At least one of 436597 or 2496 is divisible by 97
C: Both A and B are true
D: Neither A nor B is true
E: None of the above

Fundamental Theorem of Arithmetic

- **Any number can be written as a product of primes in one and only one way.**

- General proof uses same logic, that if a prime appears in one decomposition, it has to appear to all decompositions.

Why should we care?

- Writing natural numbers in decimal notation builds up numbers effectively as a combination of summation and multiplication, where the number 10 is special.
- With computers, you might write it in *binary* instead, where we use the base of 2 instead of 10.
- The Fundamental Theorem of Arithmetic gives a different way of writing numbers, based on just multiplication, and without choosing a special number as a base.

Disadvantages to factorization

- What are some disadvantages to writing in factored form?

Respond in chat.

- Harder to know when a number is bigger.
- Converting to factored form can be very difficult, whereas converting from factored form to decimal or binary is easy.
- We have a lot more building blocks that we need to work with (i.e. all primes), rather than just using powers of 10 and 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.