Introduction to Number Theory

Meeting #5

Justin Hua

McRoberts Math Circle

January 28, 2021

Outline

1. Introduction to Number Theory
   - Warm-Up
2. Floor and Ceiling Functions
3. Primes
4. Division
5. GCD and LCM
6. Number Theory and Combinatorics
   - Counting the number of divisors
7. Resources

Warm-Up

Many problems introduce some new function and ask you to just follow a few rules.

Problem (AMC 12 2016 #3)

The remainder can be defined for all real numbers x and y with $y \neq 0$ by

$$rem(x,y) = x - y\left\lfloor \frac{x}{y} \right\rfloor$$

where $\left\lfloor \frac{x}{y} \right\rfloor$ denotes the greatest integer less than or equal to $\frac{x}{y}$. What is the value of $rem(\frac{3}{8}, -\frac{2}{5})$?

Floor Function

Definition (Floor Function)

We define the **floor** of some real number x, $\lfloor x \rfloor$, as the smallest integer *less than* x.

Example

$\lfloor \pi \rfloor = 3$, $\lfloor 5 \rfloor = 5$, $\lfloor -4.27 \rfloor = -5$

Problem

What is $\left\lfloor \frac{2}{3} \right\rfloor$ *and* $\left\lfloor -\frac{19}{10} \right\rfloor$*?*

Floor Function

Definition (Ceiling Function)

We define the **ceiling** of some real number x, $\lceil x \rceil$, as the smallest integer *greater than* x.

Example

$\lceil \pi \rceil = 4$, $\lceil 5 \rceil = 5$, $\lceil -4.27 \rceil = -4$

Problem (Cookies for Kids)

James has 25 cookies and is babysitting 4 kids. If everyone has to receive the same amount of cookies, what is the maximum amount of cookies does each child receive?

Division

Babies know how to divide. Let us revisit the concept.

Definition (Division)

Let $m, n \in \mathbb{Z}$. Then we say that m divides n, or simply $m|n$, if $\frac{n}{m} = k \in \mathbb{Z}$

Example (3 divides 6)

Does $3|6$? well $\frac{6}{3} = 2$, which **is** an integer, so 3 divides 6!

Example (3 does not divide 7)

Does $3|7$? well $\frac{7}{3} = 2.333333$, which is **not** an integer, so 3 doesn't divide 7!

Primes

Definition (Prime Number)

We call a number p *prime*, if the only positive divisors of p are 1 and p(itself).

For example, the first few primes are:

Example (Primes)

2,3,5,7,11,13,17,...

A nice result on primes is the following:

Theorem (Infinitude of primes (proven by Euclid))

There are an infinite number of primes.

When does $m|n$?

We want to find out when $m|n$, where $m, n \in \mathbb{Z}$

Problem

Why does $4|8$*?*

Problem

Why doesn't $6|8$*?*

So, based on our observations, we can deduce that $m|n$ if and only if the powers of the primes of m are less than or equal to the powers of the *same* primes of n.

Theorem (Criterion for $m|n$)

So, let $m = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_k^{a_k}$ *and* $n = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ldots \cdot p_n^{b_n}$
Then $m|n$ *if and only if* $a_1 \leq b_1, a_2 \leq b_2, \ldots a_k \leq b_k,$

GCD

We begin with a quick review of the *greatest common divisor* (or GCD in short) and the *least common multiple* (LCM in short).

Definition (GCD)

We define the GCD of 2 integers x and y as the largest integer d such that $d|x$ and $d|y$

Example

$$\gcd(4,6)=2, \gcd(7,14)=7, \gcd(14,1)=1$$

We can also extend the GCD idea to more than 2 integers. That is , the GCD of a bunch of numbers is just the greatest positive integer d such that d divides all the numbers.

Finding the GCD

Right now, our only method of finding the GCD of 2 numbers is just guessing. The gcd of m, n must divide both m, n. Then is we break down m, n into its prime factorization, the power of p_k in the gcd must be less than *both* of those of m and n.

Theorem (GCD of m and n)

Let $m = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_n^{a_n}$ *and* $n = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ldots \cdot p_n^{b_n}$
Then,

$$\gcd(m, n) = p_1{}^{min\ (a_1, b_1)} \cdot p_2{}^{min\ (a_2, b_2)} \cdot \ldots \cdot p_n{}^{min\ (a_n, b_n)}$$

Example ($\gcd(40, 700)$)

We begin by breaking down the numbers into their prime factorization.
$40 = 2^3 \cdot 5$ and $700 = 2^2 \cdot 5^2 \cdot 7$
So, $\gcd(m, n) = 2^{\text{ min }(3,2)} \cdot 5^{\text{ min }(1,2)} \cdot 7^{\text{ min }(0,1)} = 2^2 \cdot 5^1 \cdot 7^0 = 20$

As practice, find $\gcd(63, 15)$

Relatively Prime

A term often used in various problems is the following:

Definition (Relatively Prime)

We call two numbers x and y *relatively prime* if the only common factor them is 1. That is, $\gcd(x, y) = 1$

Example

Are 2 and 5 relatively prime? Well, $\gcd(2, 5) = 1$, so they are.

Example

Are 6 and 21 relatively prime? Well, we notice that $3|6$ and $3|21$, so they **aren't**. We don't even need to find their gcd if we can find a common factor other than 1.

LCM

We begin with a quick review of the *greatest common divisor* (or GCD in short) and the *least common multiple* (LCM in short).

Definition (LCM)

We define the LCM of 2 integers x and y as the smallest integer e such that $x|e$ and $y|e$

Example

$$(4,6) = 12, \gcd(7,14) = 14, \gcd(14,1) = 14$$

Similar to the GCD, we can extend the notion of LCM to more than just 2 numbers.

Finding the LCM

Similar to the gcd of 2 numbers, we can also find an efficient way of finding the LCM of two numbers by using prime factorization. Both m, n must divide the LCM, so the powers of p_k in m and n must be less than or equal to the power of p_k in LCM. Since LCM is the *lowest* common multiple, we take the maximum value of the powers.

Theorem

$$lcm\ (m, n) = {p_1}^{max\ (a_1, b_1)} \cdot {p_2}^{max\ (a_2, b_2)} \cdot \ldots \cdot {p_n}^{max\ (a_n, b_n)}$$

Problem

Find $lcm(63, 15)$

LCM or GCD?

Problem (AMC 12A #12 2017)

There are 10 *horses, named Horse 1, Horse 2, . . ., Horse 10. They get their names from how many minutes it takes them to run one lap around a circular race track: Horse k runs one lap in exactly k minutes. At time 0 all the horses are together at the starting point on the track. The horses start running in the same direction, and they keep running around the circular track at their constant speeds. The least time* $S > 0$, *in minutes, at which all* 10 *horses will again simultaneously be at the starting point is* $S = 2520$. *Let* $T > 0$ *be the least time, in minutes, such that at least* 5 *of the horses are again at the starting point. What is the sum of the digits of* T*?*

Number of Divisors

Problem

How many positive divisors does 16 have?

Problem

How many positive divisors does 15 have?

Now,let us extend this notion a bit further.

For an integer n, we want to find how many positive divisors it has. Using primes can be a good idea.

For example, the divisors of 15 are: $1, 3^1, 5^1$ and $3^1 \cdot 5^1$

A Formula for τ

Definition (Number of divisors function (tau))

We define the number of divisors a positive integer n has as $\tau(n)$.

Example

$$\tau(16) = 5, \tau(15) = 4, \tau(1) = 1$$

.

The idea is to break down n into its prime factorization.
Let $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_n^{a_n}$
Then we can construct a divisor of n by picking the power of each of the primes. However, we must remember that the powers of the primes we pick must be less than the ones of n.

Theorem

$$\tau(n) = (a_1 + 1) \cdot (a_2 + 1) \cdot (a_3 + 1) \cdot \ldots (a_n + 1)$$

τ exercises

Problem

Find the number of positive divisors of 900*.*

Problem

Let n be a positive integer with 5 positive divisors. How many positive divisors does n^2 have?

Problem (AMC 12A # 18 2016)

For some positive integer n, the number $110n^3$ has 110 positive integer divisors, including 1 and the number $110n^3$. How many positive integer divisors does the number $81n^4$ have?

Resources

Art of Problem Solving-artofproblemsolving.com

1. Problems
2. Alcumus Game
3. Problem Solving Books
4. Classes