Background:

Set: collection of objects (often numbers)
can be finite or infinite

$\mathbb{N} = \{1, 2, 3, \dots\}$ set of natural numbers

$\mathbb{Z}$ = set of integers

$\mathbb{Q}$ = set of rational numbers

$\mathbb{R}$ = set of real numbers

$\mathbb{C}$ = set of complex numbers

Remark: $\mathbb{N}$: $n, m \in \mathbb{N} \Rightarrow n+m \in \mathbb{N}$
but if we subtract, the result
is not necessarily in $\mathbb{N}$

MTH 339

$\mathbb{Z}$: We can add and subtract and multiply, but not necessarily divide

$\mathbb{Q}$: · We can divide as well!
· $\sqrt{2} \notin \mathbb{Q}$
· countable

$\mathbb{R}$: · includes all the numbers that are "missing" in $\mathbb{Q}$

(94) $\mathbb{R}$ is <u>not</u> countable.

<u>Proof that $\mathbb{R}$ is uncountable:</u>

Assume we could list all numbers in $(0,1)$.

1. $0.a_1 a_2 a_3 \ldots = r_1$
2. $0.b_1 b_2 b_3 \ldots = r_2$
3. $0.c_1 c_2 c_3 \ldots = r_3$
4. $0.d_1 c_2 d_3 \ldots = r_4$

$\vdots$

Define $\xi = 0.x_1 x_2 x_3 \ldots$

$$x_k = \begin{cases} 1 & \text{if the } k\text{-th digit of } r_k \text{ is not } 1 \\ 2 & \text{if the } k\text{-th digit of } k_k \text{ is } 1 \end{cases}$$

$\Rightarrow$ ξ differs from all r_k on the list in at least one digit. $\square$

Divisibility: (integers)

Def $t \neq 0$ is a divisor of an integer s if there is an integer u such that

$$s = tu$$

we write $t \mid s$ ("t divides s")

When t is not a divisor of s, we write $t \nmid s$.

Def A prime is a positive integer greater than 1 whose only positive divisors are 1 and itself.

Ex: $4 \mid 20$, $13 \mid 169$, $12 \nmid 169$

primes: 2, 3, 5, 7, 11, 13, ...

Finding primes: Sieve of Eratosthenes

(Eratosthenes of Cyrene, 276 B.C - 195 B.C.)

MTH 339

Note: While it is easy to show that there are infinitely many prime numbers, many prime-number related questions are difficult to answer.

(Th) Division algorithm:

Let a and b be integers, $b > 0$. Then there exist unique integers q and r such that $a = bq + r$ where $0 \leq r < b$.

Example: $a = 17$, $b = 5$: $17 = 5 \cdot 3 + 2$

(Def) Greatest Common Divisor: gcd

largest divisor of two nonzero integers

$\gcd(4,15) = 1$, $\gcd(4,10) = 2$

When $\gcd(a,b) = 1$, we say a and b are relatively prime.

<u>Euclids Lemma</u> : $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

(Euclid ~ 300 B.C.) if p is a prime.

We can use this to prove $\sqrt{2} \notin \mathbb{Q}$.

<u>Proof</u>: Assume $\sqrt{2} = \frac{p}{q}$, fully reduced.

$\Rightarrow$ $2q^2 = p^2$ so $2 \mid p^2 \Rightarrow 2 \mid p$ (Euclid's Lemma)

$\Rightarrow$ we can write $p = 2n \Rightarrow 2q^2 = 4n^2$

or $q^2 = 2n^2 \Rightarrow 2 \mid q^2 \Rightarrow 2 \mid q$ (Euclid's Lemma)

$\Rightarrow$ $2 \mid p$ and $2 \mid q$,

so $\frac{p}{q}$ is not fully reduced ↯ $\square$

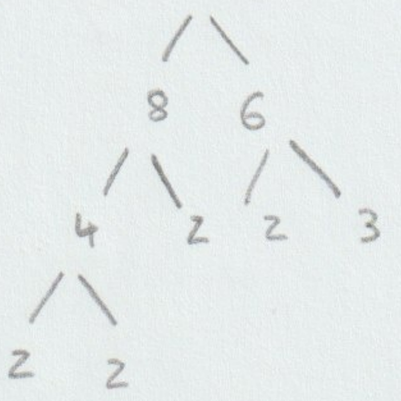
MTH 339

6/8

Th Fundamental Theorem of Arithmetic:

Every integer greater than 1 is a prime or a product of primes. This product is unique (except for order).

Ex: $48 = 2^4 \cdot 3^1$



Def The least common multiple of two nonzero integers a and b is the smallest positive integer that is a multiple of both a and b.

Ex: $\text{lcm}(10, 12) = 60$

Modular Arithmetic:

Def a mod n

Let n be a fixed positive integer. For any integer a, $a \bmod n$ ("a modulo n") is the remainder upon dividing a by n.

Ex:

$8 \bmod 3 = 2$ $\quad (8 = 3 \cdot 2 + 2)$

$-8 \bmod 3 = 1$ $\quad (-8 = -3 \cdot 3 + 1)$

$23 \bmod 6 = 5$ $\quad (23 = 3 \cdot 6 + 5)$

$-23 \bmod 6 = 1$ $\quad (-23 = -4 \cdot 6 + 1)$

$(7+4) \bmod 3 = 2$ $\quad (11 = 3 \cdot 3 + 2)$

$(10 \cdot 5) \bmod 6 = 2$ $\quad (50 = 8 \cdot 6 + 2)$

Def Modular Equation

If a and b are integers and n is a positive integer, we write $a = b \bmod n$ when n divides $a-b$.

MTH 339

Example: $13 \equiv 3 \mod 5$ $(5 \mid 13-3)$

$22 \equiv 10 \mod 6$ $(6 \mid 22-10)$

$-10 \equiv 4 \mod 7$ $(7 \mid -14)$

Example:

(a) $x \equiv 1 \mod 5$

Solution: $5 \mid x-1 \Rightarrow x-1 = 5k$ for integer k.

$\Rightarrow x-1 = 0, \pm 5, \pm 10 \ldots$

$x \in \{\ldots -9, -4, 1, 6, 11, \ldots\}$

(b) $x \equiv 3 \mod 5$

$\Rightarrow x-3 = 0, \pm 5, \pm 10 \ldots$

$x \in \{\ldots -7, -2, 3, 8, 13, \ldots\}$

(c) $2x \equiv 5 \mod 6$

no solution. If $6 \mid 2x-5$ is means $6k = 2x-5$, but left side is even, right side is odd.

MTH 339 - Do Now

1./ $655 \bmod 3$

$x = 2 \bmod 10$

2./ Find the prime factorization of 480.

3./ Determine $\gcd(2^3 \cdot 5^2 \cdot 11,\ 2^2 \cdot 5 \cdot 7)$
and $\operatorname{lcm}(2^3 \cdot 5^2 \cdot 11,\ 2^2 \cdot 5 \cdot 7)$.

$$\boxed{\text{MTH 339 - HW}}$$

1./ For $n = 25$ find all integers less than n and relatively prime to n.

Solution: $\mathbb{N}^{\leq 24} \setminus \{5, 10, 15\}$

2./(a) Calculate $(15+4) \bmod 7$

Solution: $19 \bmod 7 = 5$

(b) Calculate $(7 \cdot 3) \bmod 5$

Solution $21 \bmod 5 = 1$

3./ Find the prime factorization of 2520.

4./ Prove that $\sqrt{7}$ is irrational

5./ Determine $\gcd(2^4 3^2 5 \cdot 7^2, 2 \cdot 3^3 \cdot 7 \cdot 11)$ and $\operatorname{lcm}(2^3 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7 \cdot 11)$

Solution: $\gcd(,) = 2 \cdot 3^2 \cdot 7$ $\quad \operatorname{lcm}(,) = 2^3 \cdot 3^3 \cdot 7 \cdot 11$

6./ Prove: If n is an odd integer, $n^2 \equiv 1 \bmod 8$

$n^2 - 1 = (n+1)(n-1) = (2k+2)2k = 4k(k+1)$

$\uparrow$

$2k+1$

and $8 \mid 4k(k+1)$

MTH 339 - HW

7./ Prove:

(a) If a number ends in an even number, it is divisible by 2

(b) If the sum of the digits is divisible by 3, the number is divisible by 3.

(c) If the sum of the digits is divisible by 9, the number is divisible by 9.