Topic 1 –

Division and Primes

Assumptions for the class

We will assume that the set of <u>integers</u> $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$

exists.

We will assume basic facts about $\mathbb{Z}$:

If $a, b, c \in \mathbb{Z}$, then

- $a+b \in \mathbb{Z}$
- $ab \in \mathbb{Z}$
- $(a+b)+c = a+(b+c)$
- $(ab)c = a(bc)$
- $0+a = a+0 = a$
- $a+(-a) = (-a)+a = 0$
- $a(b+c) = ab+ac$
- $(b+c)a = ba+ca$
- $a+b = b+a$
- $ab = ba$
- $1a = a1 = a$

We will also assume all the other usual basic algebra/arithmetic facts like if $a > b$ then $-a < -b$, ...

Division and Primes (HW 1 topic)

Def: Let x and y be integers with $x \neq 0$. We say that x divides y if there exists an integer k with $xk = y$.

If x divides y, then we say that x is a divisor of y and we write $\underbrace{x \mid y}$.

read: "x divides y"

If x does not divide y, then we say that x is not a divisor of y and we write $\underbrace{x \nmid y}$.

read: "x does not divide y"

Ex:

$\boxed{\begin{array}{l}\underline{\text{divisors of } 12:} \\ \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\end{array}}$

For example, $-3 \mid 12$ because

$$\underbrace{(-3)}_{x}\underbrace{(-4)}_{k}=\underbrace{12}_{y}$$

Or, $2 \mid 12$ because $\underbrace{(2)}_{x}\underbrace{(6)}_{k}=\underbrace{12}_{y}$

$7 \nmid 12$ because there is no integer k with $7k=12$

You need $k=\frac{12}{7}$ which is not an integer.

<u>Def:</u> Let p be an integer, with $p > 1$. We say that p is <u>prime</u> if the only positive divisors of p are 1 and p.

If p is not prime, then we call it <u>composite</u>.

<u>Let's circle the primes</u>

positive divisors are 1, 2, 4

positive divisors are 1, 2, 3, 6

positive divisors are 1, 3, 9

2, 3, 4, 5, 6, 7, 8, 9,

positive divisors are 1, 2, 4, 8

10, 11, 12, 13, 14, 15, 16,

17, 18, 19, 20, 21, 22, 23, ...

Proposition: Let x and y be positive integers. If $x \mid y$, then $1 \le x \le y$.

proof: Suppose that x and y are positive integers and $x \mid y$.

We know $\boxed{1 \le x.}$

Since $x \mid y$ we know that

$$y = xk \text{ where } k \in \mathbb{Z}.$$

We know that x and y are positive, so k is positive.

If $k \le 0$, then $\frac{y}{x} \le 0$ which isn't true because $x, y \ge 1$

Thus, $1 \le k$

Multiply $1 \le k$ by x to get $\boxed{x \le \underbrace{kx}_{y}}$

So, $1 \le x \le y$. ∎

<u>Proposition:</u> Let p and q be prime numbers. If $p \mid q$, then $p = q$.

<u>proof:</u> Suppose p and q are primes and $p \mid q$.

Because q is prime, its only divisors are 1 and q.

So since $p \mid q$, either $p = 1$ or $p = q$.

But $p \neq 1$ because p is prime.

Thus, $p = q$. $\blacksquare$

Proposition: Let $z, a, b, x, y \in \mathbb{Z}$ with $z \neq 0$. If $z \mid a$ and $z \mid b$, then $z \mid (xa + yb)$.

proof: Suppose $z \mid a$ and $z \mid b$. Then, $a = zk$ and $b = zw$ where $k, w \in \mathbb{Z}$.

Ergo,

$$xa + yb = x(zk) + y(zw) \qquad (*)$$
$$= z[xk + yw].$$

Since $x, k, y, w \in \mathbb{Z}$ we know $xk + yw \in \mathbb{Z}$. Thus, from $(*)$ we know $z \mid (xa + yb)$.

$\blacksquare$

Theorem: Let $n \in \mathbb{Z}$, with $n \geq 2$. Then, n can be written as the product of one or more primes.

Ex: $12 = 2 \cdot 2 \cdot 3$ ← product of 3 primes

$5 = 5$ ← product of one prime

proof of theorem: We will prove this statement by strong/complete induction.

Let $S(n)$ be the statement

"n can be written as a product of one or more primes."

When $n=2$, the statement $S(2)$ is true since 2 is the product of one prime.

Let $k \in \mathbb{Z}$ with $k > 2$.

(Induction hypothesis) Assume that $S(n)$ is true for all n with $2 \leq n < k$. That is, each n with $2 \leq n < k$ can be factored into a product of one or more primes

Goal: Show $S(k)$ is true.

case 1: Suppose k is prime.

Then, $S(k)$ is true since k is the product of one prime.

case 2: Suppose k is not prime.

Since k is not prime, it has a divisor a where $1 < a < k$ [i.e. $a \neq 1$, $a \neq k$]

Then, $k = ab$ where b is a positive integer. We can't have $b=1$, because then $k=a$. We can't have $b=k$ because then $a=1$. So, $1 < b < k$.

Since $2 \leq a < k$ and $2 \leq b < k$

we can apply the induction hypothesis.

So, $S(a)$ and $S(b)$ are true statements.

So, $a = p_1 p_2 \cdots p_r$ and $b = q_1 q_2 \cdots q_t$

where p_i, q_j are primes and $r, t \geqslant 1$.

Then,

$$k = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_t$$

So, k is the product of primes

and $S(k)$ is true.

By induction we know $S(k)$ is true for all $k \geqslant 2$.

$\blacksquare$

Lemma: Let $x, y, z \in \mathbb{Z}$ with $x \neq 0$.
If $x \mid y$ and $x \mid (y+z)$, then $x \mid z$.

proof:
Suppose $x \mid y$ and $x \mid (y+z)$.
Then, $y = xk$ and $y + z = x\ell$ where $k, \ell \in \mathbb{Z}$.

Then,

$$z = x\ell - y = x\ell - xk = x(\ell - k). \quad (*)$$

Since $k, \ell \in \mathbb{Z}$ we know $\ell - k \in \mathbb{Z}$.
Thus, $(*)$ tells us that $x \mid z$. $\blacksquare$

<u>Theorem</u> (Euclid)

There are infinitely many primes.

<u>proof by contradiction:</u>

Suppose there are only finitely many primes.

Call them $p_1, p_2, p_3, \ldots, p_r$.

Let $N = p_1 p_2 p_3 \cdots p_r + 1$

<u>Ex:</u> If only 3 primes existed, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ and $N = 2 \cdot 3 \cdot 5 + 1 = 31$

By the theorem from today, N must be a product of one or more primes.

So, some prime divides N.

Say, $p_i \mid N$ for some $1 \leq i \leq r$.

But then $p_i \mid p_1 p_2 \cdots p_r$ and $p_i \mid (\underbrace{p_1 p_2 \cdots p_r + 1}_{N})$

The lemma tells us that $p_i \mid 1$.

But then $p_i = 1$, which can't happen since p_i is prime.

Contradiction.

Thus, there are infinitely many primes. $\blacksquare$

Another method

This page just for fun.

One can show that

$$\sum_{\substack{2 \le p \le N \\ p \text{ prime}}} \frac{1}{p} > \log(\log(N)) - 1$$

$N = 6$

$\sum \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5}$

An introduction to the theory of numbers
Niven, Zuckerman, Montgomery

So if you let $N \to \infty$ then

$$\lim_{N\to\infty} \sum_{\substack{2 \le p \le N \\ p \text{ prime}}} \frac{1}{p} > \lim_{N\to\infty} \left[\log(\log(N)) - 1\right] = \infty$$

So, there must be an infinite # of primes to make the sum on the left side infinite.

How are the primes spaced out?

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13,
14, 15, 16, 17, 18, 19, 20, 21, 22, 23,
24, 25, 26, 27, 28, 29, 30, 31, 32,
33, 34, 35, 36, 37, 38, 39, 40, 41,
42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59,
60, 61, 62, 63, 64, 65, 66, 67, 68,
69, 70, 71, 72, 73, 74, 75, 76,
77, 78, 79, 80, 81, 82, 83, 84,
85, 86, 87, 88, 89, 90, 91, 92
93, 94, 95, 96, 97, 98, 99, 100, 101,
...

Let $N=4$

$(N+1)!+2$, $(N+1)!+3$, $(N+1)!+4$, $(N+1)!+5$

$\underbrace{5\cdot4\cdot3\cdot2+2}_{\text{2 divides this}}$, $\underbrace{5\cdot4\cdot3\cdot2+3}_{\text{3 divides this}}$, $\underbrace{5\cdot4\cdot3\cdot2+4}_{\text{4 divides this}}$, $\underbrace{5\cdot4\cdot3\cdot2+5}_{\text{5 divides this}}$

122, 123, 124, 125

We just made $N=4$ composite (ie not prime) numbers in a row (in sequence) ie a gap of size 4 in the primes.

Theorem: There are arbitrarily large gaps in the primes. That is, given any positive integer N there exist N consecutive composite integers.

Ex: Last time we showed $N=4$ consecutive composites 122, 123, 124, 125

proof: Let N be a positive integer. Consider the N consecutive integers

$(N+1)!+2,\ (N+1)!+3,\ \ldots,\ (N+1)!+(N+1)$

Given k with $2 \le k \le N+1$, note that

$$(N+1)! + k = \overbrace{(N+1)(N)\cdots(k+1)(k)(k-1)\cdots(2)(1)}^{(N+1)!} + k$$
$$= k\left[(N+1)(N)\cdots(k+1)(k-1)\cdots(2)(1)+1\right]$$

So, $k \mid \left[(N+1)!+k\right]$.

Since $2 \le k \le N+1$

we know $\boxed{k \neq 1}$

Also, since $k < \overbrace{(N+1)!}^{\geq 2} + k$

we know $\boxed{k \neq (N+1)! + k.}$

Thus, since $k \mid [(N+1)! + k]$

we know $(N+1)! + k$ is not

prime for each $2 \le k \le N+1$.

Thus we have made a list

of N consecutive composite

integers. $\blacksquare$

Ex: $N = 8$

k	$(N+1)! + k$
2	362,882
3	362,883
4	362,884
5	362,885
6	362,886
7	362,887
8	362,888
9	362,889