2.3: $\mathbb{Z}$ and DIVISION

<u>Ex</u> $10 \underset{(\frac{10}{2})}{\div} 2$ is an integer (namely, 5), because $10=(2)(5)$

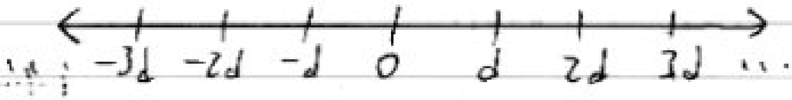
Write: $2 \mid 10$
2 divides 10
2 is a factor of 10
10 is a multiple of 2
10 is divisible by 2

Assume $a, b \in \mathbb{Z}$ and $a \neq 0$
a divides b $(a \mid b)$ $\Leftrightarrow$ $b \div a$ (or $\frac{b}{a}$) is an integer
$\Leftrightarrow \exists c \in \mathbb{Z} : b = ac$

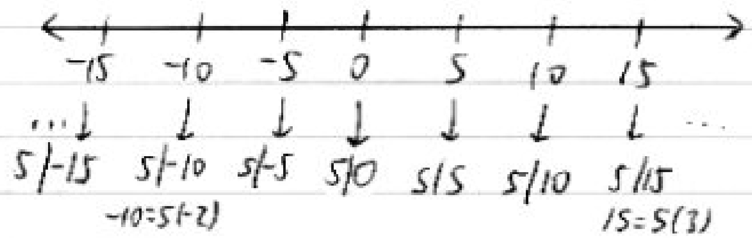
<u>Ex</u> 5 10 2 5

<u>Ex</u> $4 \mid 12$ $\quad (\frac{12}{4} = 3 \in \mathbb{Z})$
<u>Ex</u> $5 \nmid 12$ $\quad (\frac{12}{5} \notin \mathbb{Z})$

If $d \in \mathbb{Z}^+$, the multiples of d
(i.e., the integers divisible by d):



<u>Ex</u> $d = 5$:



(Skip / Too technical)

Ex 2 (p. 114)

$n, d \in \mathbb{Z}^+$.

How many positive integers not exceeding n are divisible by d?

i.e., find $\left| \{ x \mid \underbrace{x \in \mathbb{Z}^+}_{}, \underbrace{1 \le x}_{\text{redundant}} \le n,\ d \mid x \} \right|$

Pictures (Optional)

Consider multiples of d

Case 1 ($d \mid n$)

We have $m \ (= \frac{n}{d})$ integers of interest.

Case 2 ($d \nmid n$)

We have m integers of interest.

What's m?

It's the highest integer such that

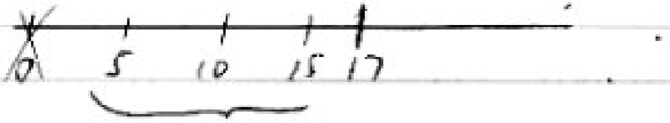
$md \le n$ (or $m \le \frac{n}{d}$)

m is the highest integer $\le \frac{n}{d}$

So, $m = \lfloor \frac{n}{d} \rfloor$

In either case, our answer is $\lfloor \frac{n}{d} \rfloor$.

Ex How many positive integers not exceeding 17 are divisible by 5?



Answer: 3

$$\lfloor \tfrac{n}{d} \rfloor = \lfloor \tfrac{17}{5} \rfloor = \lfloor 3.4 \rfloor = 3$$

Thm 1 Let $a, b, c \in \mathbb{Z}$.

① $a | b$ and $a | c \Rightarrow a | (b+c)$

Ex $\underset{a}{3} | \underset{b}{6}$ and $\underset{a}{3} | \underset{c}{9} \Rightarrow \underset{a}{3} | \underset{(b+c)}{15}$

② $a | b \Rightarrow \underbrace{\forall c \in \mathbb{Z}}_{\text{for all integers "c"}} (a | bc)$

Ex $\underset{a}{3} | \underset{b}{6} \Rightarrow \begin{cases} \underset{(c=1)}{3|6}, \underset{(c=2)}{3|12}, \underset{(c=3)}{3|18}, \ldots \\ \underset{(c=0)}{3|0}, \underset{(c=-1)}{3|-6}, \underset{(c=-2)}{3|-12}, \ldots \end{cases}$

③ $a|b$ and $b|c \Rightarrow a|c$ (transitivity)

<u>Ex</u> $3|6$ and $6|24 \Rightarrow 3|24$

<u>Proof of ①</u>: $\underbrace{a|b \text{ and } a|c}$ $\Rightarrow a|(b+c)$

Suppose the condition is true.
i.e., assume $a|b$ and $a|c$.

(We will show that $a|(b+c)$ must follow.)

Since $a|b \Rightarrow \exists s \in \mathbb{Z}\ (b = as)$
Since $a|c \Rightarrow \exists t \in \mathbb{Z}\ (c = at)$

Use a letter other than s.
b and c are not
necessarily the same
multiples of a.

(We're asking about b+c.)

$b = as$ > Add
$c = at$

$b+c = as + at$ ↓ Distributive law "in reverse"
$b+c = a\underbrace{(s+t)}$

This is some integer "u"!

$\Rightarrow \exists u \in \mathbb{Z}\ (b+c = au)$

$\Rightarrow a|(b+c)$

Short version:

Assume $a|b$ and $a|c$.

$$\Rightarrow \begin{cases} \exists s \in \mathbb{Z}\ (b = as) \\ \exists t \in \mathbb{Z}\ (c = at) \end{cases}$$

$$\Rightarrow b + c = as + at$$
$$\Rightarrow b + c = a\underbrace{(s+t)}_{\in \mathbb{Z}}$$

$$\Rightarrow a | (b+c)$$

Prove ② ③ in HW #3, 4

<u>PRIME #s</u>

Assume $n \in \mathbb{Z}^+$, $n > 1$.

n must be divisible by 1 and itself $(1|n, n|n)$
1 and n are trivial factors of n.
n is <u>prime</u> $\Leftrightarrow$ n has no other divisors (factors)

If n is not prime, it is <u>composite</u>

0 and 1 are neither prime nor composite.

n	Positive divisors (factors) of n	P = prime, C = Composite
2	1, 2	P
3	1, 3	P
4	1, 2, 4	C
5	1, 5	P
6	1, 2, 3, 6	C
7	1, 7	P
8	1, 2, 4, 8	C
largest odd C → 9	1, 3, 9	C

2 is the only even prime.

<u>Fundamental Theorem of Arithmetic</u> (FTA)

If $n \in \mathbb{Z}^+$, $n \geq 2$,
then n is either
1) prime, or
2) expressable as a product of primes.
This <u>prime factorization</u> is unique up to a reordering of the factors.

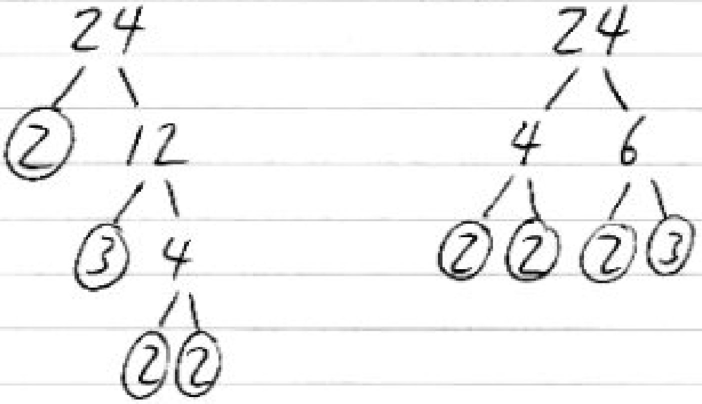
<u>Ex</u> $12 = \underbrace{2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2}_{\text{same fac'n}}$

$= 2^2 \cdot 3$ ← <u>exponential notation</u>

Factor Tree Method for Finding Prime Fac'ns

Keep splitting factors into smaller factors until all the "leaves" are primes.
Then, the leaves give you the prime fac'n.

Ex



$24 = 2^3 \cdot 3$ $\qquad$ $24 = 2^3 \cdot 3$

Divisibility Tests (aids)

An integer is divisible by...

2 $\Leftrightarrow$ ends in 0, 2, 4, 6, or 8
3 $\Leftrightarrow$ digit sum is divisible by 3
Ex 1431 → digit sum is 9
147,000 → 12

These are div'e by 3. What's the trick - take a look at the digits...

4 $\Leftrightarrow$ last two digits form a multiple of 4
Ex 35,736
(100 is div'e by 4)
5 $\Leftrightarrow$ ends in 5 or 0
6 $\Leftrightarrow$ div'e by 2 and 3
7 (no good tricks)

$8 \Leftrightarrow$ last three digits form a multiple of 8

Ex 13,808

(1000 is div'e by 8)

$9 \Leftrightarrow$ digit sum is divisible by 9

Ex 378 $\rightarrow$ sum digit is 18

9819 $\rightarrow$ 27

207,000 $\rightarrow$ 9

$10 \Leftrightarrow$ ends in 0

$11 \Leftrightarrow$ alternating sum of digits is divisible by 11

Ex 5467

$+5-4+6-7=0$

Ex 90,904

$+9-0+9-0+4=22$

Think place value:

1, 100, 10000, ... are 1 more than multiples of 11

10, 1000, ... less

$12 \Leftrightarrow$ div'e by 3 and 4

~~If m and n are in~~

$m, n \in \mathbb{Z}^+$. m and n are relatively prime if their only common positive factor is 1. Then, mn-test $\Leftrightarrow$ m-test and n-test

Key aid:

If n is a composite integer, then n has a prime factor $\leq \sqrt{n}$.

<u>Proof</u>

Let n be a composite integer.

$\Rightarrow n$ has a nontrivial factor "r" $\quad (1 < r < n,\ r \in \mathbb{Z})$

$\Rightarrow n = rs \quad (1 < s < n,\ s \in \mathbb{Z})$

$r \leq \sqrt{n}$ or $s \leq \sqrt{n}$

Otherwise, $r > \sqrt{n}$ and $s > \sqrt{n}$.

Then, $rs > (\sqrt{n})(\sqrt{n}) = n$

$\Rightarrow rs > n$

This contradicts $n = rs$, so this can't happen!

Without loss of generality (w.l.o.g.), let's say $r \leq \sqrt{n}$.

$$\begin{tikzcd}
 & n \arrow[dl, dash] \arrow[dr, dash] & \\
r \ (r \leq \sqrt{n}) \arrow[d, dotted, dash, "\text{FTA}"'] & & s \\
p \ (p \leq \sqrt{n}) & &
\end{tikzcd}$$

<u>Case 1</u> If r is prime, then r is our desired prime factor $\leq \sqrt{n}$.

<u>Case 2</u> Otherwise, by FTA, r has a prime factor $p \leq \sqrt{n}$.

Contrapositive is true:

If n does not have a prime factor $\le \sqrt{n}$, then n is $\underbrace{\text{not composite}}_{\substack{\text{prime} \\ \text{if } n \neq 0,1}}$.

<u>Ex</u> Show that 173 is prime.

Sufficient to show that 173 does not have a prime factor $\le \sqrt{173} \approx 13.2$.

<u>Primes $p \le 13$</u>	<u>Does $p \mid 173$?</u>	
2	N	
3	N	
5	N	
7	N	(calculator: $\frac{173}{7} \notin \mathbb{Z}$)
11	N	
13	N	(calculator $\frac{173}{13} \notin \mathbb{Z}$)

So, 173 is prime.

<u>Sieve of Eratosthenes</u>

Find the prime #s up to a certain #.

<u>Ex</u> for #s up to 40, run through the multiples of 2, 3, and 5 and eliminate them (except 2, 3, and 5, themselves)

<u>Overheads</u>

Ex Find the prime fac'n of 4575.

4575

25 183

5 5 3 61

Verify that 61 is prime

$\sqrt{61} \approx 7.8$

$2 \nmid 61$

$3 \nmid 61$

$5 \nmid 61$

$7 \nmid 61$

$$4575 = 3 \cdot 5 \cdot 5 \cdot 61$$
$$= 3 \cdot 5^2 \cdot 61$$

Cryptography – primality testing, factoring

Mersenne primes – primes of the form $2^p - 1$. (p prime)

Great Internet Mersenne Prime Search (GIMPS)

More info: pp. 116-7, Rosen's Web page

p.116 web
Chris Caldwell

Largest prime so far:

6/1/1999: $2^{6,972,593}-1$ ← 38^{th} Mersenne prime

has ≈2M digits (2,098,960)

Previous one only had 909,526 digits. (1998)

19c: # primes $\le n \to \frac{n}{\log n}$ (Prime Number Thm.)
1792 - stated by Gauss
1896 - proven

So, n^{th} prime $\approx n \log n$