2.3: \mathbb{Z} and DIVISION

**Ex** 10 \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 \(b\) (\(ab\)) \iff \(b \div a\) (or \(\frac{b}{a}\)) is an integer

\iff \exists c \in \mathbb{Z}: b = ac

\[
\begin{align*}
\text{Ex } 5 & \quad 10 \quad 2 \quad 5 \\
\end{align*}
\]

\[
\begin{align*}
\text{Ex } 4 \mid 12 & \quad \left(\frac{12}{4} = 3 \in \mathbb{Z}\right) \\
\text{Ex } 5 \mid 12 & \quad \left(\frac{12}{5} \notin \mathbb{Z}\right)
\end{align*}
\]

If \(d \in \mathbb{Z}^+\), the multiples of \(d\)

(i.e., the integers divisible by \(d\)):

\[
\begin{align*}
\text{Ex } d = 5 & \\
\end{align*}
\]

\[
\begin{align*}
-15 & \quad -10 & \quad -5 & \quad 0 & \quad 5 & \quad 10 & \quad 15 \\
\end{align*}
\]

\[
\begin{align*}
\text{...} & \quad \uparrow & \quad \uparrow & \quad \uparrow & \quad \uparrow & \quad \uparrow & \quad \uparrow \\
5 \mid -15 & \quad 5 \mid -10 & \quad 5 \mid -5 & \quad 5 \mid 0 & \quad 5 \mid 5 & \quad 5 \mid 10 & \quad 5 \mid 15 \\
\end{align*}
\]

\[
\begin{align*}
-10 = 5 \times (-2) & \quad 15 = 5 \times (3)
\end{align*}
\]
Ex 2 (p. 114)

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

i.e., find \( |\{x \in \mathbb{Z}^+, 1 \leq x \leq n, \ d \mid x\}| \)

Pictures (Optional)

Consider multiples of \( d \)

Case 1 \( (d \| n) \)

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

Case 2 \( (d \nmid n) \)

We have \( m \) integers of interest.  
What's \( m \)?  
It's the highest integer such that \( md \leq n \) (or \( m \leq \frac{n}{d} \)).  
\( m \) is the highest integer \( \leq \frac{n}{d} \).  
So, \( m = \left\lfloor \frac{n}{d} \right\rfloor \)
In either case, our answer is \( \left\lfloor \frac{17}{5} \right\rfloor \).

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

\[
\begin{array}{c}
5 & 10 & 15 & 17 \\
\hline
\end{array}
\]

Answer: 3

\[
\left\lfloor \frac{17}{5} \right\rfloor = \left\lfloor \frac{17}{5} \right\rfloor = \left\lfloor 3.4 \right\rfloor = 3
\]

**Theorem.** Let \( a, b, c \in \mathbb{Z} \).

1. \( a \mid b \) and \( a \mid c \) \( \Rightarrow \) \( a \mid (b+c) \)

\[
\text{Ex. } \frac{3}{6} \text{ and } \frac{3}{9} \Rightarrow \frac{3}{15}
\]

2. \( a \mid b \ \Rightarrow \ \forall c \in \mathbb{Z} \ \ (a \mid bc) \)

For all integers \( c \).

\[
\text{Ex. } \frac{3}{6} \Rightarrow \begin{cases}
3 / 6, & (c=1) \\
3 / 3, & (c=2) \\
& (c=0, 1, -1, 2)
\end{cases}
\]
3. \( a \mid b \) and \( b \mid c \Rightarrow a \mid c \) (transitivity)

\[ \text{Ex: } 3 \mid 6 \text{ and } 6 \mid 24 \Rightarrow 3 \mid 24 \]

Proof of (1): \( a \mid b \) and \( a \mid c \Rightarrow a \mid (b+c) \)

Suppose the condition is true, i.e., assume \( a \mid b \) and \( a \mid c \).

(We will show that \( a \mid (b+c) \) must follow.)

Since \( a \mid b \Rightarrow \exists s \in \mathbb{Z} \ (b=as) \)

Since \( a \mid c \Rightarrow \exists t \in \mathbb{Z} \ (c=at) \)

Use a letter other than \( s \).

\( b \) and \( c \) are not necessarily the same multiples of \( a \).

(We're asking about \( b+c \).)

\( b=as \Rightarrow \text{Add} \)

\( c=at \)

\( b+c=as+at \) \quad \text{Distributive law "in reverse"}

\( b+c=a(s+t) \)

This is some integer \( u \).

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

\[ \Rightarrow a \mid (b+c) \]
Short version:

Assume $ab$ and $ac$.

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

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

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

Proof 2/3 in HW #34

PRIME #s

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

$n$ must be divisible by 1 and itself $(1n, nn)$
1 and $n$ are trivial factors of $n$.

$n$ is prime $\iff$ $n$ has no other divisors (factors)

If $n$ is not prime, it is composite

0 and 1 are neither prime nor composite.
<table>
<thead>
<tr>
<th>$n$</th>
<th>Positive divisors (factors) of $n$</th>
<th>$P$ = prime</th>
<th>$C$ = composite</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1, 2</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1, 3</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1, 2, 4</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1, 5</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1, 2, 3, 6</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1, 7</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1, 2, 4, 8</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1, 3, 9</td>
<td>C</td>
<td></td>
</tr>
</tbody>
</table>

odd

2 is the only even prime.

**Fundamental Theorem of Arithmetic (FTA)**

If $n \in \mathbb{Z}^+$, $n \geq 2$, then $n$ is either

1) prime, or

2) expressible as a product of primes.

This prime factorization is unique up to a reordering of the factors.

**Ex**

$12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$

![same factors](underline)

$= 2^2 \cdot 3 \leftarrow$ exponential notation
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

\[
\begin{align*}
24 & \quad 24 \\
12 & \quad 4 \\
6 & \quad 6 \\
3 & \quad 2 \\
4 & \quad 2 \\
2 & \quad 2 \\
2 & \quad 3 \\
\end{align*}
\]

\[
24 = 2^3 \cdot 3 \\
24 = 2^3 \cdot 3
\]

Divisibility Tests (aids)

An integer is divisible by:

- 2 \iff ends in 0, 2, 4, 6, or 8
- 3 \iff digit sum is divisible by 3
  \[
  \text{Ex} \quad 1431 \rightarrow \text{digit sum is 9}
  \]
  \[
  147,000 \rightarrow 12
  \]
- 4 \iff last two digits form a multiple of 4
  \[
  \text{Ex} \quad 35,736
  \]
  \[
  (100 \text{ is divisible by 4})
  \]
- 5 \iff ends in 5 or 0
- 6 \iff divisible by 2 and 3
- 7 \iff no good tricks
8 ⇔ last three digits form a multiple of 8
Ex 13,808
(1000 is divisible by 8)

9 ⇔ digit sum is divisible by 9
Ex 378 → sum digit is 18
9819 → 27
207,000 → 9

10 ⇔ ends in 0

11 ⇔ 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,... are 1 less

12 ⇔ divisible by 3 and 4

m and n are in \( \mathbb{Z}^+ \). m and n are relatively prime if their only common positive factor is 1. Then, \( m \) is test and \( n \) is test.
Key aid:
If \( n \) is a composite integer,
then \( n \) has a prime factor \( \leq \sqrt{n} \).

**Proof**

Let \( n \) be a composite integer.
\( \Rightarrow n \) has a nontrivial factor \( r \) \( (1 < r < n, r \in \mathbb{Z}) \)
\( \Rightarrow n = rs \)

\( r \leq \sqrt{n} \) 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 \( r \leq \sqrt{n} \).

\[ \begin{array}{c}
\sqrt{n} \\
\mathrm{r} \\
\mathrm{s} \\
(r \leq \sqrt{n})
\end{array} \]

**Case 1.** If \( r \) is prime,
then \( r \) is our desired prime factor \( \leq \sqrt{n} \).

\( p \) \( (p \leq \sqrt{n}) \)

**Case 2.** Otherwise, by FTA,
\( r \) has a prime factor \( p \leq \sqrt{n} \).
Contrapositive is true:

If $n$ does not have a prime factor $\leq \sqrt{n}$, then $n$ is not composite.

**Prime**

if $n \neq 0, 1$

Ex Show that $173$ is prime.

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

| Primes $p \leq 13$ | Does $p|173$? |
|-------------------|--------------|
| 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.

Sieve of Eratosthenes

Find the prime #s up to a certain #.

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

Overheads
Ex Find the prime factor of 4575.

\[
4575
\]
\[
\begin{array}{c}
25 \\
\underline{25}
\end{array}
\]
\[
\begin{array}{c}
183 \\
\underline{5}
\end{array}
\]
\[
\begin{array}{c}
361 \\
\underline{11}
\end{array}
\]

Verify that 61 is prime.

\[
\sqrt{61} \approx 7.8
\]

- 2 \not| 61
- 3 \not| 61
- 5 \not| 61
- 7 \not| 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 \(2^p - 1\).

Great Internet Mersenne Prime Search (GIMPS)

More info: pp. 116-7, Rosen’s Web page
Largest prime so far:

611/1999: $2^{38} + 1 < 38^{th}$ Mersenne prime

has 72M digits (2,098,960)

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

19c: $\#\text{prime} \leq n \rightarrow \frac{n}{\log n}$ (Prime Number Thm.)

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