Number Theory

"Number theory" is the study of the integers \( \mathbb{Z} \) and their arithmetic

> "The queen of mathematics"
> - Gauss

- Since primes are the multiplicative building blocks of all integers, they play an important role.

Def'n: Fix \( n \in \mathbb{N}, n > 1 \)

1. \( n \) is prime if its only positive divisors are 1 and \( n \)
2. \( n \) is composite if it is not prime, i.e., if \( \exists a, b \in \mathbb{N}, a, b > 1 \) s.t. \( n = a \cdot b \).

We prove (by strong induction): any \( n \in \mathbb{N} \) can be written as a product of primes.

Once you have proved this, you will prove a unique way to do this:

**Testing Primality is hard!**

Q: How to check a given \( n \in \mathbb{N} \) is prime?

You could just divide by every \( k \in n \) to see if there's a divisor.
or be about smarter.

**Theorem** Fix $n \in \mathbb{N}$. Suppose $n = a \cdot b$.

Then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

**Proof.** Sps $n \neq 1$. Then $a > \sqrt{n}$ and $b > \sqrt{n}$.

But then $ab > \sqrt{n} \cdot \sqrt{n} = n$, contradiction $\checkmark$.

So so to check if $n$ is odd, only need to test for divisors $k \leq \sqrt{n}$.

ex: determine if $a_1$ or $a_7$ are prime.

**Solv.:** observe $9 < \sqrt{91} < \sqrt{97} < 10$.

So only need to test for prime divisors up to 9.

$91 = 2 \times 91, 3 \times 91, 5 \times 91, 7 \times 91$.

So 91 is not prime.

$97 = 2 \times 97, 3 \times 97, 5 \times 97, 7 \times 97$.

So 97 is prime.

**Divisors:** Define $m$ is a divisor of $n$ if $mn \in \mathbb{N}$.

**Note:** For every $n \in \mathbb{Z}$, we have $n$ divides 0 , since $0 = 0 \cdot n$. 
Defn Fix \( m, n \in \mathbb{Z} \) (neither both 0).
The greatest common divisor of \( m, n \) written \( \text{gcd}(m, n) \) is the largest natural number \( d \) dividing both \( m, n \).

Ex 1. What is \( \text{gcd}(42, 60) \)?

Divisors of 42 = \{ \pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42 \}

Divisors of 60 = \{ \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 10, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60 \}

Common divisors = \{ \pm 1, \pm 2, \pm 3, \pm 6 \}

\[ \Rightarrow \text{gcd}(42, 60) = 6. \]

2. \( \text{gcd}(42, 0) = 42 \)

(42 is the greatest divisor of 42 and 42|0)

3. \( \text{gcd}(-42, 60) = 6. \)

If we divide out by gcd, we get numbers w/ no common factors but \( \pm 1. \)

Theorem: Fix \( m, n \in \mathbb{Z} \) and let \( d = \text{gcd}(m, n) \)
Then:
\[ \text{gcd} \left( \frac{m}{d}, \frac{n}{d} \right) = 1 \]
PF: \(-1\leq a = \gcd(\frac{m}{a}, \frac{n}{a})\)
- So \(a \leq 1\) and \(a \mid \frac{m}{a}\) and \(a \mid \frac{n}{a}\)
- i.e. \(\frac{m}{a}, \frac{n}{a} \in \mathbb{Z}\)
  \(\frac{m}{a} = ak\)
  \(\frac{n}{a} = al\)
- So \(m = (kd)k\)
- i.e. \(ad\) is a common divisor of \(mn\)
- but then by defn of \(\gcd\) \(ad \leq d\)
  \(\implies a \leq 1\)
- So \(1 \leq a \leq 1\) \(\implies a = 1\), as claimed

Example: \(\gcd(\frac{a2}{c}, \frac{bc}{c}) = \gcd(7, 10) = 1\) (as expected)

Q: Better way of finding \(\gcd(a, b)\) than writing out all divisors? Page 56
  \(\rightarrow\) Euclidean algorithm will give
  such a way
  \(\rightarrow\) long way to go before we get there.

Theorem (Division algorithm)
Fix \(b, c \in \mathbb{Z}\) and \(a \in \mathbb{N}\)
Then there exist unique integers \(q, r \in \mathbb{Z}\) with \(0 \leq r < c\) s.t.
\[b = aq + r\]

\((q, r)\) is quotient \& remainder when \(b\) is divided by \(a\)
Idea: Consider $b = 14, a = 3$

3.1 = 3  
3.2 = 6  
3.3 = 9  
3.4 = 12

and

14 - 3.1 = 11 > 3  
14 - 3.2 = 8 > 3  
14 - 3.3 = 5 > 3  
14 - 3.4 = 2 ≤ 3

PF: Define $S = \{ n \in \mathbb{N} \cup \{0\} | (\exists k \in \mathbb{Z}) \ n = b - ak \}$

Observe: $S \neq \emptyset$

Since $b - ak > 0$

whenever $b > ak$

then $b = ak + r$

- hence by WOP

$S$ has a least element $r$

- Let $q \in \mathbb{Z}$ be s.t.

$b = aq + r$

- then $b = aq + r$

Claim: $r < a$

PF: (If $r > a$)

- so we can write $r = a + r'$

where $0 \leq r' < r$

- then:

$b = aq + r = aq + a + r' = a(q + 1) + r'$

- hence $r \in S$

- contradiction as $r$ was least in $S$

( hence $r < a$ as claimed)

So we've proved existence of $r, q, s$ t. $b = aq + r$ and $0 \leq r < a$
Need to prove uniqueness.

Suppose \( q', r' \in \mathbb{Z} \) with \( 0 \leq r' < a \) and \( b = aq' + r' \).

Un: \( q = q' \) and \( r = r' \).

We have:
\[
    b = aq + r = aq' + r'
\]

Either \( r \geq r' \) or \( r' > r \).
Assume \( r > r' \) since other case is similar.

Then:
\[
    r - r' = a(q' - q' - q') \\
    = r - r' = a(q' - q')
\]

So \( a \mid r - r' \)

But \( 0 \leq r - r' < a \)

So must have \( r - r' = 0 \), i.e. \( r = r' \).

But then:
\[
    b = aq + r = aq' + r'
\]

So \( q = q' \) too. \( \checkmark \).
Ex's ① \( a = 15 \), \( b = 107 \)
Then \( 107 = 15 \cdot 7 + 2 \)
\[ q = \frac{7}{r} = 2 \]

② \( a = 6 \), \( b = -2a \)
Then \( -2a = 6(-5) + 1 \)
\[ q = -5 \quad r = 1 \]

③ \( a = 3 \), \( b = 12 \)
Then \( b = 3 \cdot 4 + 0 \)
\[ q = 4 \quad r = 0 \]

Next theorem is one of the fundamental results about divisibility.

**Bézout's Theorem**

Fix \( a, b \in \mathbb{Z} \) (not both 0) and \(\gcd(a,b) \neq 0\).

Then there exist \( u, v \in \mathbb{Z} \) s.t.

\[ d = au + bv \]

and \( d \) is least natural number that can be written as a linear combination of \( a \) and \( b \).

Example before proof:
Consider \( a = 6 \), \( b = 15 \).

Q: if we +/- 6's and 15's, how small a number could we get?

positive

\[ 15 - 6 = 9 \]
\[ 15 - 6 - 6 = 3 \text{, i.e. } 6(-2) + 15(1) = 3 \]

Can we do better than 3?
Doesn't seem so, but we can get 3 in more than one way e.g.
\[ 6 + 6 + 6 - 15 = 3 \quad \text{i.e.} \quad 6(3) + 15(1) = 3 \]

\underline{Notice:} \quad 3 = \gcd(6, 15)

\underline{Bézout says:} Our discovery above is not accidental.

\[ \exists m, n \in \mathbb{Z} \quad \text{s.t.} \quad 6m + 15n = 3 \]

(e.g. \( m = -2 \quad n = 1 \))

\underline{Here are or} \( m = 3 \quad n = -1 \) \underline{(work)}

\[ \text{no } m, n \quad \text{s.t.} \quad 6m + 15n = 2 \]

or \( c = 1 \)

\underline{Proof of Bézout:}

- Define \( S = \{ c \in \mathbb{N} \mid (6m + 15n) \}

\[ c = am + bn \] is set of positive linear combinations of \( a, b \).

- Observe: \( S \) is not empty since \( (a_1 + (b_1)c \in S \).

- Hence by WOP, \( S \) has a least element \( d \).

- Fix \( m, n \in \mathbb{Z} \) s.t. \( d = am + bn \)

- \( \gcd \) wts: \( d = \gcd(a, b) \)
Claim 1: \( \ddagger \) \( d \mid a \) and \( \ddagger \) \( d \mid b \) 

By division algorithm we can write
\[ a = q \cdot d + r \quad 0 \leq r < d \]

\( \text{w.r.t.} \quad r = 0 \)

\[ r = a - q \cdot d = a - q \cdot (am + bn) = (1 - qm) a + (-qn) b \]

Hence \( r \) is a linear combo of \( a, b \).

We knew \( r > 0 \). If \( r > 0 \), then would have \( r \leq s \).

But \( r < d \), so thus would contradict the minimality of \( d \).

Hence \( r = 0 \).

(e.g. \( a = q \cdot d \) so \( \ddagger \) \( d \mid a \))

\( \ddagger \) Similar arg proves \( \ddagger \) \( d \mid b \).

Claim 2: \( \ddagger \) \( d \) is great divider \( \ddagger \) \( a, b \).

Pf. Suppose \( t \in \mathbb{N} \) and \( t \mid a \) and \( t \mid b \)

We prove \( t \mid d \), which gives \( t \leq d \)

So we have \( \exists k, \ell \in \mathbb{Z} \) s.t. \( a = \ell t + b = k t \)

\[ d = am + bn = \ell tm + \ell km = (\ell m) t + (\ell k) t = t (\ell m + \ell k) \]

Claim 1 + 2 \( \ddagger \) \( d \) = \text{gcd}(a, b) \)
Def'n  Fix \( a, b, c, d \in \mathbb{Z} \). We say \( a, b \) are relatively prime if \( \gcd(c, d) = 1 \).

Corollary of Bezout: if \( a, b, c, d \in \mathbb{Z} \) are relatively prime then
\[
\exists m, n \in \mathbb{Z} \text{ s.t. } am + bn = 1.
\]

Pf: immediate since \( \gcd(c, d) = 1 \).

Ex 1 \( \gcd(25, 36) = 1 \) so Bezout says \( \exists m, n \in \mathbb{Z} \text{ s.t. } 25m + 36n = 1 \) and indeed:
\[
25(-23) + 36(16) = 1
\]

\( \odot \) Observe: if \( P \) is a prime
then for any \( a \in \mathbb{Z} \) either \( \gcd(a, p) = 1 \) or \( \gcd(a, p) = p \).
So if \( P, Q \) are distinct primes
then of course \( \gcd(P, Q) = 1 \) primes
\( \exists m, n \in \mathbb{Z} \text{ s.t. } pm + qn = 1 \)

e.g. if \( p = 7 \) and \( q = 81 \) then
\[
7(9) + 31(-2) = 1
\]

Here's a useful application of Bezout:
Prop'n (Euclid's Lemma)

Fix $a$, $b$, $c \in \mathbb{Z}$. If $a | bc$ and $\gcd(a, b) = 1$ then actually $a | c$

PF: Sps $a | bc$ and $\gcd(a, b) = 1$
- then $\exists k \in \mathbb{Z}$ s.t. $ak = bc$
- also: by Bezout $\exists m, n \in \mathbb{Z}$ s.t. $am + bn = 1$
- hence:
  $c(am + bn) = c$
  $\Rightarrow a(cm + bn) = 1$
  $\Rightarrow a | c$

Corollary: Fix $a$, $b$, $c \in \mathbb{Z}$ and $p \in \mathbb{N}$ a prime. If $p | ab$ then $p | a$ or $p | b$.

PF:
- IF $p | a$ we are done
- so sps $p | a$
- then it must be $\gcd(p, a) = 1$
  why: $\gcd(p, a) = 1$ or $p$
  since $p$ is prime and we knew $p | a$
- hence by Euclid's Lemma $p | b$