Number Theory Basics

\[ \mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \} \]

For \( a, b \in \mathbb{Z} \), we say that \( a \) divides \( b \) if \( az = b \) for some \( z \in \mathbb{Z} \)

Notation: \( a \mid b \)

Fact: for all \( a, b, c \in \mathbb{Z} \):

- \( a \mid a \), \( 1 \mid a \), and \( a \mid 0 \)
- \( 0 \mid a \iff a = 0 \)
- \( a \mid b \) and \( b \mid c \implies a \mid c \)
- \( a \mid b \) and \( a \mid c \implies a \mid (b + c) \)
- \( a \mid b \) and \( b \mid a \iff a = \pm b \)
**Division with remainder property**

Let $a, b \in \mathbb{Z}$ with $b > 0$

There exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$

*Proof: see class notes*

$q = \lfloor a/b \rfloor$

$r = a \mod b$
Greatest Common Divisors

For $a, b \in \mathbb{Z}$, we call $d \in \mathbb{Z}$ a common divisor of $a$ and $b$ if $d \mid a$ and $d \mid b$.

$d$ is called a greatest common divisor if

- $d$ is non-negative, and
- all other common divisors of $a$ and $b$ divide $d$

Fact: greatest common divisors are unique:

- Suppose $d$ and $d'$ are greatest common divisors of $a$ and $b$
- We must have $d \mid d'$ and $d' \mid d$, so $d = \pm d'$
- Since $d$ and $d'$ are non-negative, we must have $d = d'$

Notation: $\gcd(a, b)$

But... we still need to prove that $\gcd(a, b)$ always exists (according to our definition)

We will give an algorithm that computes it
Algorithm Euclid($a, b$): On input $a, b$, where $a$ and $b$ are integers such that $a \geq b \geq 0$, compute gcd($a, b$) as follows:

if $b = 0$
    then return $a$
else return Euclid($b, a \mod b$)

Correctness (induction on $b$):

• $b = 0$: gcd($a, 0$) = $a$
• $b > 0$: write $a = bq + r$

\[ d | a \land d | b \iff d | b \land d | r \]

Example: $a = 100, b = 35$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_i$</td>
<td>100</td>
<td>35</td>
<td>30</td>
<td>5</td>
</tr>
<tr>
<td>$b_i$</td>
<td>35</td>
<td>30</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

gcd(100, 35) = 5
Running Time: On input \((a, b)\) with \(b > 0\):

- algorithm performs one division step
- then calls itself recursively on input \((a', b')\), where \(a' := b\) and \(b' := a \mod b\)
- so \(b > b'\)

It follows that \# of division steps is at most \(b\)

Better bound: \(O(\log b)\) division steps

Proof: if \(b' > 0\), the algorithm performs another division step, and calls itself again on input \((a'', b'')\), where \(a'' := b'\) and \(b'' := b \mod b'\), so that \(b' > b''\)

\[ q' := \lfloor b/b' \rfloor \geq 1 \]

\[ b = b'q' + b'' \geq b' + b'' > 2b'' \]

after two division steps, second argument to Euclid is \(< b/2\)

\# of division steps \(\leq 2\lfloor \log_2 b \rfloor\)
Bezout’s Lemma

Let \( a, b \in \mathbb{Z} \) and \( d := \gcd(a, b) \)

(i) We have \( as + bt = d \) for some \( s, t \in \mathbb{Z} \)

(ii) For every \( d^* \in \mathbb{Z} \), we have

\[
d \mid d^* \iff as^* + bt^* = d^* \quad \text{for some } s^*, t^* \in \mathbb{Z}
\]

Part (ii) follows easily from part (i):

- If \( d \mid d^* \), then \( dz = d^* \), so set \( s^* := sz, t^* := tz \)
- If \( as^* + bt^* = d^* \), then since \( d \mid a \) and \( d \mid b \), it follows that \( d \mid (as^* + bt^*) = d^* \)

For part (i), we can modify the Euclidean Algorithm so that it computes \( s \) and \( t \) together with \( d \)
Algorithm ExtEuclid($a, b$): On input $a, b$, where $a$ and $b$ are integers such that $a \geq b \geq 0$, compute $(d, s, t)$, where $d = \gcd(a, b)$ and $s$ and $t$ are integers such that $as + bt = d$, as follows:

if $b = 0$ then
  $d \leftarrow a$, $s \leftarrow 1$, $t \leftarrow 0$
else
  $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a \mod b$
  $(d, s', t') \leftarrow \text{ExtEuclid}(b, r)$
  $s \leftarrow t'$, $t \leftarrow s' - qt'$
return $(d, s, t)$

Correctness (induction):

- $a = bq + r$, $bs' + rt' = d$
- Substitute $r := a - bq$ and re-arrange:
  
  $at' + b(s' - qt') = d$
Example: $a = 100, b = 35$

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_i$</td>
<td>100</td>
<td>35</td>
<td>30</td>
<td>5</td>
</tr>
<tr>
<td>$b_i$</td>
<td>35</td>
<td>30</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>$s_i$</td>
<td>−1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$t_i$</td>
<td>3</td>
<td>−1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$q_i$</td>
<td>2</td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

$s_i := t_{i+1}$ and $t_i := s_{i+1} - q_it_{i+1}$

d = 5, $s = s_0 = -1$, $t = t_0 = 3$

$as + bt = 100 \cdot (-1) + 35 \cdot (3) = 5 = d$
Relatively prime numbers

Let $a, b \in \mathbb{Z}$

We say $a, b$ are **relatively prime** if $\gcd(a, b) = 1$

• In other words, $\pm 1$ are the only common divisors of $a$ and $b$

**Special case of Bezout’s Lemma:**

• $a$ and $b$ are relatively prime $\iff as + bt = 1$ for some $s, t \in \mathbb{Z}$

**Theorem 1:** Let $a, b, c \in \mathbb{Z}$ such that $c$ divides $ab$, and $a$ and $c$ are relatively prime. Then $c \mid b$

**Proof:** Assume $c \mid ab$, $\gcd(a, c) = 1$. Want to show: $c \mid b$

$\gcd(a, c) = 1 \implies as + ct = 1$ for some $s, t \in \mathbb{Z}$ (Bezout)

Multiply by $b$: $abs + cht = b$

$c \mid cht$, $c \mid abs$, $\therefore c \mid b$
Primes and composites

Let $n$ be a positive integer

$n$ is prime if $n > 1$ and the only positive integers that divide $n$ are 1 and $n$

$n$ is composite if $n > 1$ and is not prime

- $n$ is composite $\iff n = ab$ for some integers $a, b$ with $1 < a < n$ and $1 < b < n$

$n = 1$ is neither prime nor composite
Fundamental theorem of arithmetic: Every non-zero integer $n$ can be expressed as

$$n = \pm p_1^{e_1} \cdots p_r^{e_r},$$

where $p_1, \ldots, p_r$ are distinct primes and $e_1, \ldots, e_r$ are positive integers. Moreover, this expression is unique, up to a reordering of the primes.
Proof (existence): Assume $n$ positive

Induction on $n$

$n = 1 \checkmark$

$n > 1$. Induction hypothesis: every number smaller than $n$ can be expressed as a product of primes

If $n$ is prime, then we’re done

Otherwise, $n = ab$, where $1 < a < n$ and $1 < b < n$

By induction, both $a$ and $b$ can be expressed as a product of primes

$\therefore n$ can also be expressed as a product of primes

Proof (uniqueness): that’s the hard part . . .
**Theorem 2:** Let $p$ be a prime. For all $a, b \in \mathbb{Z}$, if $p | ab$, then $p | a$ or $p | b$

**Proof:** Suppose $p | ab$. Want to show: $p | a$ or $p | b$

If $p | a$, we are done

So assume $p \nmid a$. Want to show $p | b$

As the only divisors of $p$ are $\pm 1$ and $\pm p$, the only common divisors of $p$ and $a$ are $\pm 1$

So we have $\gcd(p, a) = 1$

By Theorem 1 (with $c := p$), we have $p | b$

**Generalization:** if $p$ is prime and $p | a_1 \cdots a_k$, then $p | a_i$ for some $i = 1, \ldots, k$

**Proof:** easy induction on $k$
Finishing proof of Fundamental Theorem (uniqueness)

Suppose

\[ p_1 \cdots p_r = q_1 \cdots q_s, \quad (\ast) \]

where the \( p_i \)'s and \( q_j \)'s are primes

Want to show that \( (p_1, \ldots, p_r) \) is a re-ordering of \( (q_1, \ldots, q_s) \)

Induction on \( r \):

- \( r = 0 \vee \)
- \( r > 0: \)
  - Since \( p_1 \) prime, we have \( p_1 \mid q_j \) for some \( j \)
  - Since \( q_j \) prime, we have \( p_1 = q_j \)
  - Cancel \( p_1 \) from LHS of \( (\ast) \) and \( q_j \) from RHS of \( (\ast) \), and apply induction hypothesis