Number Theory

- Let $n, d \in \mathbb{Z}, d \neq 0$ we say n is **divisible** by d if $n = dk$ for some $k \in \mathbb{Z}$.
- We write $d|n$ and call d a **divisor** of n, and n a **multiple** of d.
- If d does not divide n, we write $d \nmid n$

Definition - Transitivity of Divisibility:

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

Proof:

$a|b \Rightarrow \exists d \in \mathbb{Z} \ni b = ad$

$b|c \Rightarrow \exists e \in \mathbb{Z} \ni c = be$

$\Rightarrow c = be = (ad)e = a(de), de \in \mathbb{Z}$

$\therefore a|c$

Definition – Divisibility by Primes:

Every $n \in \mathbb{N}\{1\}$ is divisible by some prime number.

Proof: (Strong Induction)

a) $2|2$

b) For $k > 2$, suppose every integer $m \ni 1 < m \leq k$ is divisible by a prime. Show that $k + 1$ is divisible by a prime.

Case 1: $k + 1$ is a prime. Then $(k + 1)|(k + 1)$

Case 2: $k + 1$ is composite. Then $k + 1 = ab$ for some $a, b \in \mathbb{N}\{1\}$,

$a, b < k + 1$

By hypothesis, $\exists c\ Prime \ni c|a$. Since $c|a\ AND\ a|(k + 1)$, by transitivity $c|(k + 1)$

$\therefore$ Every $n \in \mathbb{N}\{1\}$ is divisible by a prime.

Exercise:

Find a prime factor:

a) 693 ← 3, 11

b) 1048

↑ 2

Theorem:
There are infinitely many primes.

Proof: (by contradiction)

Suppose there are finitely many Primes, $p_1, p_2, p_3, \dots, p_n$.
Construct a number p defined by $p = p_1 p_2 \dots p_n + 1$.

Clearly p is larger than all the primes, so p is not equal to any of the primes.
Hence p is divisible by a prime.
Without loss of generality (WLOG), $p_1 | p_2$ ← Can be switched with any other prime

$$\frac{p}{p_1} = \frac{p_1 p_2 \dots p_n + 1}{p_1} = p_2 p_3 \dots p_n + \frac{1}{p_1} \notin \mathbb{Z}$$ ← a contradiction

Not an integer. Strictly less than 1.

∴ There are infinitely many primes.

Quotient-Remainder Theorem

- If $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, then there exists a unique $q, r \in \mathbb{Z}$ such that:

  $n = dq + r \; AND \; 0 \leq r < d$

> *Definition*
>
> $\boldsymbol{n = dq + r \; AND \; 0 \leq r < d}$

Exercise:
Find $q, r \in n = dq + r, 0 \leq r < d$.

a) $n = 54, d = 4$
b) $n = -32, d = 7$
c) $n = 42, d = 70$

a) $54 = 4 \cdot 13 + 2$ ← unique representation
Could also say:
$54 = 4 \cdot 11 + 10$ ← however, doesn't satisfy $r < d$

b) $-32 = 7 \cdot (-5) + 3$ ← what neg. int. that is just below -32.
-5 gives -35, $r = +3$, $n = -32$.

c) $42 = 70 \cdot 0 + 42$

Fundamental Theorem of Arithmetic

- Every $a \in \mathbb{N}\{1\}$ can be factorized uniquely in the form:

  $a = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k}$

  Where $k \in \mathbb{N}, \alpha_i \in \mathbb{N}\ \forall\ i, AND\ P_i\ is\ PRIME\ \forall\ i$

Proof:

The proof requires the following Lemma:

Euclid's Lemma: Let p be prime, $a, b \in \mathbb{N}$. If $p|ab$, then $p|a$ OR $p|b$.

First, we show that every $a \in \mathbb{N}\{1\}$ is either a prime or a product of primes, by strong induction.

a) 2 is prime.
b) Suppose $2, 3, \dots, k$ are all either prime or product of primes.
   Prove that $k+1$ is either prime or product of primes.
   a. If $k+1$ is prime → there is nothing more to prove.
   b. If not, then it is a composite: $\exists\ Integers\ b, c \ni 1 < b \leq c < k+1\ and\ k+1 = bc$

      By hypothesis, $b = p_1 p_2 \dots p_j$ and $c = q_1 q_2 \dots q_m$ are products of primes.
      Then $k+1 = bc = p_1 p_2 \dots p_j q_1 q_2 \dots q_m$ is a product of primes.
      ∴ Ever $a \in \mathbb{N}\backslash\{1\}$ is either prime or a product of primes.

   Now we show uniqueness, by contradiction.
   Assume that $a > 1$ is the product of primes in two different ways:

   $a = p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$

   Since $p_1|a$, Euclid's Lemma says p, divides one of the q_j. Without loss of generality, let $p_1|q_1$. Since q, is prime, its divisors are 1 and q. Hence, $p_1|q_1$, and:

   $$\frac{a}{p_1} = p_2 p_3 \dots p_m = q_2 q_3 \dots q_n$$

   By the same logic, p_2 must divide one of the remaining q_j, WLOQ $p_2|q_2$. Then

   $$\frac{a}{p_1 p_2} = p_3 p_4 \dots p_m = q_3 q_4 \dots q_n$$

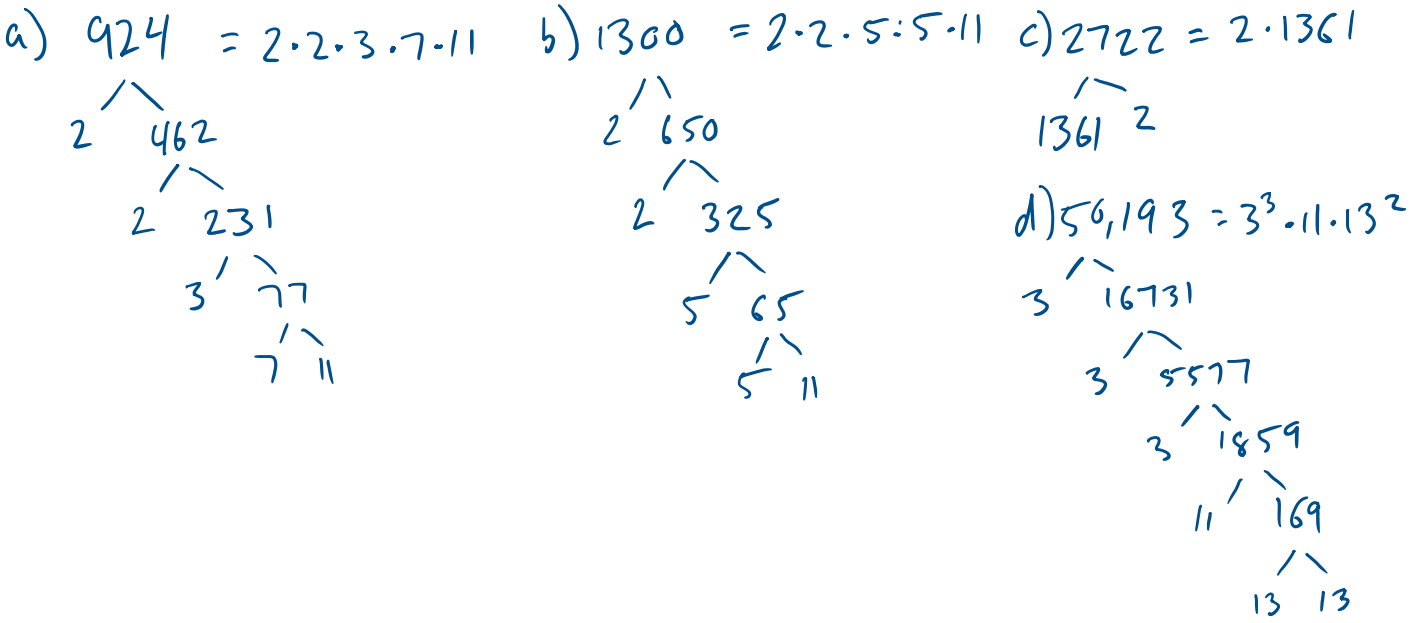
   Continuing like this, we find that $m \leq n$ and $p_i = q_i\ \forall\ i \in \{1, 2, \dots, m\}$.
   The same argument with the p primes and q primes reversed gives us that $n \leq m$ and $q_i = p_i\ \forall\ i \in \{1, 2, \dots, n\}$.
   Therefore, $m = n$ and we have that the two factorizations are the same.

Exercise:

Find the prime factorization.

NOTE: PRIMES = {2 3 5, 7, 11, 13, 17, 19, 23 29 31 37...}

a) 924
b) 1300
c) 2722
d) 50,193



Greatest Common Divisor

- Let $a, b \in \mathbb{Z}$ with at least one of a, b nonzero.
- The **greatest common divisor** of a and b, denoted by $\gcd(a, b)$ is the number c such that:
  - c is a common divisor of a and b: $c|a$ and $c|b$
  - If d is a common divisor of a and b, then $d \leq c$

Definition

$\boldsymbol{a, b \in \mathbb{Z}, a, b \neq 0,} \qquad \boldsymbol{gcd(a, b) = c}$

Exercise:
$\gcd(18, 12) = 6$, since $6|18$ and $6|12$, and there is no bigger integer that divides them both.

Note: $\gcd(18, 12) = \gcd(-18, 12) = \gcd(18, -12) = \gcd(-18, -12)$

- **Prime factorizations** can be used to find $gcd(a, b)$, if:

  $a = P_1^{\alpha_1} \dots P_k^{\alpha_k}$ and $b = P_1^{\beta_1} \dots P_k^{\beta_k}$ (some α_i, β_i can be zero), then

  $\gcd(a, b) = P_1^{\gamma_1} \dots P_k^{\gamma_k}, where\ \gamma_i = \min\{\alpha_i, \beta_i\}$

Exercise:
Given that $3220 = 2^2 \cdot 5 \cdot 7 \cdot 23$ and $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, we have:

$\gcd(3220, 1155) = 5 \cdot 7 = 35$

Least Common Multiples (LCM)

- Let $a, b \in \mathbb{Z}$ with at least one of a, b nonzero.
- The **least common multiple** of a and b, denoted by $lcm(a, b)$, is the number $c \in \mathbb{N}$ such that:
  - c is a common multiple of a and b, i.e., $a|b \; and \; b|c$.
  - If d is a common multiple of a and b, then $c \leq d$.

Exercise:

a) $lcm(12, 4) = 12$
b) $lcm(18, 15) = 90$

- We can use **prime factorization** to calculate $lcm(a, b)$, if:

  $a = P_1^{\alpha_1} \dots P_k^{\alpha_k} \; AND \; b = P_1^{\beta_1} \dots P_k^{\beta_k}$ (some α_i, β_i can be zero), then

  $lcm(a, b) = P_1^{\gamma_1} \dots P_k^{\gamma_k}, where \; \gamma_i = \max\{\alpha_i, \beta_i\}$

Exercise:

Given that $3220 = 2^2 \cdot 5 \cdot 7 \cdot 23$ and $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, we have:

$lcm(3220, 1155) = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 106,260$

Exercise:

a) Find $lcm(35100, 6975)$
b) Find $lcm(268944, \; 198466)$

a) lcm(35100, 6975)

$35100 = 2^2 \cdot 3^3 \cdot 5^2 \cdot 13$

$6975 = 3^2 \cdot 5^2 \cdot 31$

$lcm(35100, 6975) = 2^2 \cdot 3^3 \cdot 5^2 \cdot 13 \cdot 31 = 1,088,100$

b) lcm(268944, 198466)

$268944 = 2^4 \cdot 3 \cdot 13 \cdot 431$

$198466 =$

$2 \; 99233$

The Euclidean Algorithm

- The Euclidean Algorithm is a process for finding the greatest common divisor.
- It works because of the Quotient-Remainder Theorem and the following two lemmas:

Lemma 1: For all $r \in \mathbb{N}, \gcd(r, o) = r$

Proof 1:

Lemma 2: Let $a, b \in \mathbb{Z}, b \neq 0, q, r \in \mathbb{N} \ni a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$

Proof 2:
Let $D = \{d \in \mathbb{Z}: d|a, d|b\}, \overline{D} = \{d \in \mathbb{Z}: d|b, d|r\}$, we will show that $D = \overline{D}$

$(\subseteq)$: *Let* $x \in D$, *then* $x|a$ *and* $x|b$, *we have*

$$a = bq + r$$
$$\Rightarrow a - bq = r$$
$$\Rightarrow \frac{a-bq}{x} = \frac{r}{x}$$
$$\Rightarrow \frac{a}{x} - \frac{bq}{x} = \frac{r}{x}$$

Since $\frac{a}{x}$ and $\frac{bq}{x}$ are integers, we have $\frac{r}{x} \in \mathbb{Z}$, so $x|r$.
Hence, $x \in \overline{D}$, and we have $D \subseteq \overline{D}$.

$(\supseteq)$: *Let* $x \in \overline{D}$, *then* $x|b$ *and* $x|r$, *we have*

$$a = bq + r$$
$$\frac{a}{x} = \frac{bq+r}{x}$$
$$\frac{a}{x} = \frac{bq}{x} + \frac{r}{x}$$

Since $\frac{bq}{x}$ and $\frac{r}{x}$ are integers, we have $\frac{a}{x} \in \mathbb{Z}$, so $x|a$.
Hence, $x \in D$, and we have $\overline{D} \subseteq D$.

Therefore, $D = \overline{D}$. So, every common divisor of a and b is also a common divisor of b and r, and vice versa.

$\therefore \gcd(a, b) = \max_{d \in D} d = \max_{d \in \overline{D}} d = \gcd(b, r)$

Euclidean Algorithm

1) Let $a < b \leq 0$
2) Check if $b = 0$. If so, Lemma 1 says $\gcd(a, b) = a$
3) If $b \neq 0$, use Quotient-Remainder Theorem to find q, r with $0 \leq r < b$ such that $a = bq + r$. Lemma 2 says $\gcd(a, b) = \gcd(b, r)$.
4) Set $a = b, b = r$ and go to step 2.

- This algorithm will terminate with $r = 0$, since each remainder is smaller than the previous one.

Exercise:

Find $\gcd(2772, 2310)$.

$\gcd(a,b) = a$

$a = bq + r$

$2772 = 2310 \cdot 1 + 462$

$2310 = 462 \cdot 5 + 0$

$\therefore \gcd(2772, 2310) = 462$

Exercise:

Find $gcd(-243, 223)$.

$243 = 223 \cdot 1 + 20$ (Remember $\gcd(a,b) = \gcd(|a|,|b|)$)

$223 = 20 \cdot 11 + 3$

$11 = 3 \cdot 3 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$\therefore \gcd(-243, 223) = 1$

Definition

Integers a, b are called coprime (relatively prime, mutually prime) if $gcd(a, b) = 1$.

Exercise:

True or false? For all $x \in \mathbb{N}$ there exists $y \in \mathbb{N}$ such that $\gcd(x, y) = 1$.

Bézout's Identity Theorem

- Let $a, b \in \mathbb{Z}\backslash\{0\}$, then $d = \gcd(a, b)$ exists, and there exists $m, n \in \mathbb{Z}$ such that $ma + nb = d$.

Corollary: if a and b are relatively prime, then there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

- How do we find m, n?
  - We use the Euclidean Algorithm in reverse.

Exercise:

Find $m, n \in \mathbb{Z}$ such that $\gcd(303, 156) = 330m + 156n$

① $\gcd(a,b) = a = bq + r$

$\Rightarrow 330 = 156 \cdot 2 + 18$

② $156 = 18 \cdot 8 + 12$

③ $18 = 12 \cdot 1 + 6$

④ $12 = 6 \cdot 2 + 0$

Now starting with the second-last line, isolate the gcd and use each previous line to substitute for other factors.

③ $18 = 12 \cdot 1 + 6 \Rightarrow 6 = 18 - 12$

② $12 = 156 - 18 \cdot 8 \Rightarrow 6 = 18 - (156 - 18 \cdot 8)$

$= -156 + 18 \cdot 9$

① $18 = 330 - 156 \cdot 2 \Rightarrow 6 = -156 + (330 - 156 \cdot 2) \cdot 9$

$= \boxed{330 \cdot 9 - 156 \cdot 19}$

$\therefore m = 9, n = -19$

Exercise:

Find $m, n \in \mathbb{Z}$ such that $243m + 223n = 1$.

$243 = 223 \cdot 1 + 20$

$223 = 20 \cdot 11 + 3$

$20 = 3 \cdot 6 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$\Rightarrow (3 = 2 \cdot 1 + 1) \Rightarrow 1 = 3 - 2$

$(2 = 20 - 3 \cdot 6) \Rightarrow 1 = 3 - (20 - 3 \cdot 6)$

$= -20 + 3 \cdot 7$

$(3 = 223 - 20 \cdot 11) \Rightarrow 1 = -20 + (223 - 20 \cdot 11) \cdot 7$

$= 223 \cdot 7 - 20 \cdot 78$

$(20 = 243 - 223 \cdot 1) \Rightarrow 1 = 223 \cdot 7 - (243 - 223 \cdot 1) \cdot 78$

$= \boxed{-243 \cdot 78 + 223 \cdot 85}$

$\therefore m = -78, n = 85$

The Pigeonhole Principle

- Let $k, n \in \mathbb{N}, k < n$.
- If n pigeons fly into k pigeonholes, then some pigeonhole contains at least two pigeons.

Proof:

Suppose that each pigeonhole contains at most one pigeon.
Then the total number of pigeons is at most

$\sum_{i=1}^{k} 1 = k < n$ ← a contradiction

Therefore, there exists a pigeonhole that contains more than one pigeon.

Examples:

a) You have a drawer full of socks, of 3 different colours. How many socks must you pick at random to be sure you have a matching pair?
A: 4. The first 3 could possibly be all 3 different colours, but the fourth will match one or those (or else there's a previous pair).

b) In a room of 367 people (allowing for leap year), at least 2 of them share a birthday.

c) Humans have a maximum of about 500,000 hairs. Is it guaranteed that 2 residents of Wollongong have exactly the same number of hairs? How about 2 residents of Sydney?

- Some formal equivalent statements to the pigeonhole principle:
  1) Let A be a set of n elements. If A is partitioned into k pairwise disjoint subsets, where k, n, then at least one subset contains more than one element.
  2) A function from one finite set to a smaller set cannot be one-to-one. There must be at least two elements that map to the same point.

Exercise:
In a group of 700 people, must there be two whose first names have the same first and last letters?

A: At most 26 people can have different first letters, and at most 26 people can have different last letters.
So at most $26 \cdot 26 = 676$ people can have different either first or last names.
$\therefore$ A group of 700 people meets this condition.

- Problems of this sort involve figuring out how to form the pigeonholes properly (how to partition the set).

Exercise:
5 different numbers are selected from the set $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Show that 2 of the selected numbers sum to 9.

A: Partition into pairs that sum to 9
$S = \{1, 8\} \cup \{2, 7\} \cup \{3, 6\} \cup \{4, 2\}$
There are 4 subsets, so its possible to select 4 numbers from S such that only one of them belongs to each subset. Choosing 5 numbers by the pigeonhole principle, results in 2 numbers chosen belonging to the same subset.

Exercise:
A restaurant serves 3 different salads, 6 different mains and 4 different desserts. How many people must eat there to ensure that at least 2 of them have the same meal.

A: There are $3 \cdot 6 \cdot 4$ different combinations of meals.
$\therefore$ 73 people

Generalised Pigeonhole Principle

- If n pigeons fly into k pigeonholes, and $n > km$ for some $m \in \mathbb{N}$, then some pigeonhole contains at least $m + 1$ pigeons.

Exercise:

Show that in a group of 85 people, the first name of at least 4 of them must start with the same letter.

A: 85 pigeons, 26 pigeonholes

$85 = 26 \cdot 3 + 7$

So $85 > 26 \cdot 3 \Rightarrow m = 3$, and some pigeonholes contain at least $m + 1 = 4$ pigeons.

Exercise:

We want to assign 70 students to 11 classes so that no class has more than 15 people. Show that there must be at least 3 classes with 5 or more people.

A: Assume only 2 classes have 5 or more people, and show a contradiction.

The best case is that those 2 classes are full (leaving the fewest possible people for the other classes), 15 student each.

Then 40 people remain, for 9 classes.

Since $40 = 9 \cdot 4 + 4$, $m = 4$ and the principle says at least one of the 9 classes has 5 or more people in it. □