- $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)} \right) = 1$

- $(a,b) = c \Rightarrow a = c \cdot a_1$ and $b = c \cdot b_1$ such that $(a_1, b_1) = 1$.

<u>Definition:</u> We say a and b are relatively prime (or coprime) if $(a,b) = 1$.

- a, b coprime and $a \mid bc \Rightarrow a \mid c$.

a, b coprime $\Rightarrow ax + by = 1$ for some x and y.
$\Rightarrow acx + bcy = c$

$a \mid acx$ and $a \mid bc \mid bcy \Rightarrow a \mid acx + bcy \Rightarrow a \mid c$.

Can generalize: $a \mid bc \Rightarrow a \mid (a,b) \cdot (a,c)$
(Proof is left as an exercise)

- $(a,b) = 1 \Rightarrow [a,b] = |ab| \quad (a, b \neq 0)$

Let c be a common multiple of a and b, i.e. $a \mid c$ and $b \mid c$.

$b \mid c \Rightarrow c = k \cdot b$ and we have $a \mid k \cdot b \Rightarrow a \mid k$
$\Rightarrow k = \ell \cdot a \Rightarrow c = \ell \cdot ab$
$\Rightarrow$ A common multiple c is at least $|ab|$
positive

Also, clearly $|ab|$ is a common multiple of a and b $\Rightarrow$ $[a,b] = |ab|$.

- $[a,b] = \dfrac{ab}{(a,b)}$

Let $(a,b) = c$ $\Rightarrow$ $a = c \cdot a_1$ and $b = c \cdot b_1$ such that $(a_1, b_1) = 1$

$$[a,b] = [c \cdot a_1, c \cdot b_1] \underset{\text{Exercise}}{=} c \cdot [a_1, b_1] = ca_1 b_1 = \frac{ab}{(a,b)}.$$

Back to the equation $ax + by = c$ one last time.

Suppose $c = k \cdot (a,b)$, otherwise no solution.

We know how to find one solution:

- Euclid's algorithm finds x and y such that $ax + by = (a,b)$
- Then $a \cdot (kx) + b \cdot (ky) = k \cdot (a,b)$

Now using one solution, say (x_0, y_0), we should find all solutions:

$$ax + by = c \iff ax + by = ax_0 + by_0$$

$$\iff a \cdot (x - x_0) = b \cdot (y_0 - y)$$

$$\Longleftrightarrow \frac{a}{(a,b)} \cdot (x - x_0) = \frac{b}{(a,b)} \cdot (y_0 - y)$$

$$\frac{b}{(a,b)} \Bigm| \frac{a}{(a,b)} \cdot (x - x_0) \quad \text{and} \quad \left(\frac{a}{(a,b)} , \frac{b}{(a,b)} \right) = 1$$

$$\Rightarrow \frac{b}{(a,b)} \Bigm| x - x_0 \Rightarrow x - x_0 = m \cdot \frac{b}{(a,b)}$$

$$\Rightarrow y_0 - y = m \cdot \frac{a}{(a,b)}$$

$$\Rightarrow x = x_0 + m \cdot \frac{b}{(a,b)} , \quad y = y_0 - m \cdot \frac{a}{(a,b)} , \quad m \in \mathbb{Z} .$$

are all of the solutions.

<u>Example:</u> Find all integers (x, y) such that

a) $66x + 121y = 100$ b) $14x + 8y = 6$

a) No solution because $(66, 121) = 11 \nmid 100$.

b) $14 = 1 \cdot 8 + 6$ $\quad (14, 8) = 2$ and

$8 = 1 \cdot 6 + 2$ $\quad \Rightarrow$

$6 = 3 \cdot 2 + 0$

$$\begin{aligned} 2 &= 8 - 1 \cdot 6 \\ &= 8 - (14 - 1 \cdot 8) \\ &= 2 \cdot 8 - 14 \end{aligned}$$

$\Rightarrow 6 = 6\cdot 8 - 3\cdot 14 \,.\ \Rightarrow (x_0, y_0) = (-3, 6)$ is solution

All solutions: $x = -3 + m \cdot \frac{8}{(14,8)} = 4m-3$

$y = 6 - m \cdot \frac{14}{(14,8)} = -7m+6$

$\{(4m-3, -7m+6) : m \in \mathbb{Z}\}$: set of solutions

$p \geqslant 2$ is called prime if 1 and p are its only positive divisors.

$n \geqslant 2$ is called composite if it is not prime.

- n is composite $\Rightarrow$ it has a divisor $a \mid n$ such that $1 < a < n$
  $\Rightarrow n = a \cdot b$ with $1 < a, b < n$.

- p prime, n integer. What are the possible values of (n,p)?

Since $(n,p) \mid p \Rightarrow (n,p) = 1$ or p

- $(n,p) = 1 \Rightarrow n$ and p are coprime, and $p \nmid n$.
- $(n,p) = p \Rightarrow p \mid n$.

- $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ (or both)

$p \mid ab \Rightarrow p \mid (a,p) \cdot (b,p)$

(a,p)	(b,p)	
1	1	$\longrightarrow$ not possible
1	p	$\longrightarrow p \mid b$
p	1	$\longrightarrow p \mid a$
p	p	$\longrightarrow$ both

Can generalize: $p \mid a_1 a_2 \dots a_k \Rightarrow p \mid a_1$ or $p \mid a_2$ or... $p \mid a_k$.
(Proof is exercise. Hint: induction on k).
A special case: $p \mid a^k \Rightarrow p \mid a$

<u>Fundamental Theorem of Arithmetic</u>: Every $n \geq 2$ has a prime factorisation $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where p_i are distinct primes and α_i are positive integers. This factorisation is unique up to re-ordering.

e.g. $2^2 \cdot 3^5 \cdot 7^2$ same as $3^5 \cdot 7^2 \cdot 2^2$.

<u>Proof</u>: We prove "existence" first, by strong induction on n.

Base case: $n = 2 \longrightarrow n = 2^1$ ✓

Assume $2, 3, \dots, k$ all have prime factorisations.

- Case I: $k+1$ is prime, then $(k+1)^1$ is a prime factorisation

- Case II : $k+1$ is composite, then $k+1 = ab$ such that $2 \leq a, b \leq k$. By assumption a and b have prime factorisations. Combining them, we get a prime factorisation of $k+1$

$$(2^2 \cdot 3^1 \cdot 7^1) \cdot (3^2 \cdot 5^3)$$
$$\parallel$$
$$2^2 \cdot 3^3 \cdot 5^3 \cdot 7^1$$

Next, we show the uniqueness. Suppose not unique for some integers and n be the smallest of such integers.

Write $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = n = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_\ell^{\beta_\ell}$.

$p_1 \mid LHS \Rightarrow p_1 \mid RHS \Rightarrow p_1 \mid q_i$ for some i
$\Rightarrow p_1 = q_i$ for some i

Cancelling out p_1 from both sides, we have two factorisations for $\frac{n}{p_1}$, contradiction because n was the smallest such integer.

$175 = 5^2 \cdot 7^1$, $196 = 2^2 \cdot 7^2$, $1001 = 7^1 \cdot 11^1 \cdot 13^1$

$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$

(They don't have to have same prime factors, but we can write p^0 if p is missing in one of them.

e.g. $196 = 2^2 \cdot 7^2 \cdot 11^0 \cdot 13^0$, $1001 = 2^0 \cdot 7^1 \cdot 11^1 \cdot 13^1$).

- $ab = p_1^{\alpha_1+\beta_1} \cdot p_2^{\alpha_2+\beta_2} \cdot \ldots \cdot p_k^{\alpha_k+\beta_k}$
- $\dfrac{a}{b} = p_1^{\alpha_1-\beta_1} \cdot p_2^{\alpha_2-\beta_2} \cdot \ldots \cdot p_k^{\alpha_k-\beta_k}$
- $a^m = p_1^{m\alpha_1} \cdot p_2^{m\alpha_2} \cdot \ldots \cdot p_k^{m\alpha_k}$

<u>Questions:</u> 1. When does a divide b?

Answer: $\alpha_1 \leq \beta_1, \alpha_2 \leq \beta_2, \ldots, \alpha_k \leq \beta_k$

2. What is $\gcd(a,b)$? What is $\operatorname{lcm}[a,b]$?

Answer: $(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot \ldots \cdot p_k^{\min(\alpha_k,\beta_k)}$

$[a,b] = p_1^{\max(\alpha_1,\beta_1)} \cdot \ldots \cdot p_k^{\max(\alpha_k,\beta_k)}$.

Can generalize to (a,b,c), $[a,b,c]$, etc.

We now have easier proofs for some properties we proved earlier:

- $(a, b) \cdot [a, b] = ab$

$\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$

- $(a, b, c) = ((a, b), c)$

$\min(\alpha, \beta, \theta) = \min(\min(\alpha, \beta), \theta)$.