Lemma 4.1 says that the relation $|$ is transitive.
(We'll see relations later in the module.)

Lemma 4.2: Suppose $a,b,c \in \mathbb{N}$, and $a|b$, $a|c$ and $b<c$.
Then $a \mid c-b$.

Pf: Since $a|b$ and $a|c$, there are $k,l \in \mathbb{N}$ such that
$b = ak$ and $c = al$. So
$$c-b = a(l-k).$$
$l>k$ because $c>b$, so $l-k \in \mathbb{N}$, so $a \mid c-b$. $\square$

Defn: Suppose $n \in \mathbb{N}$.

- n is prime if $n>1$ and n has no divisors except 1 and n.
- n is composite if $n>1$ and n is not prime.

Note: We do not regard 1 as either prime or composite. This doesn't make much difference, but it's convenient in some situations.

Lemma 4.3: If $n \in \mathbb{N}$ and $n>1$, then n has at least one prime factor.

Pf: We use strong induction. Let $P(n)$ denote the statement "n has a prime factor".

Base case: $P(2)$ is true, because 2 is a prime factor of 2.

Inductive step: Suppose $n \geq 3$, and $P(2), P(3), \dots, P(n-1)$ are all true. We consider two cases.

- First suppose n is prime. Then n is a prime factor of n, so $P(n)$ is true.
- Now suppose n is composite. Then there is $a \in \mathbb{N}$ such that $a|n$ and $1<a<n$. $P(a)$ is true, so there is a prime p such that $p|a$. Then $p|a$ and $a|n$, so $p|n$. So p is a prime factor of n, so $P(n)$ is true.

So $P(n)$ is true for all n. $\square$

In fact, a much stronger statement is true: every $n \in \mathbb{N}$ can be written as a product of primes. This factorisation is called the <u>prime factorisation</u> of n. This factorisation is unique (up to re-ordering the factors). This is called the Fundamental Theorem of Arithmetic.

e.g. The prime factorisation of 660 is

$$660 = 2 \times 2 \times 3 \times 5 \times 11.$$

The next theorem goes back to Euclid (around 300 BC), and has one of the most famous proofs in maths.

Theorem 4.4: There are infinitely many prime numbers.

Pf: We use proof by contradiction. Suppose there are only finitely many prime numbers. Call them

$$p_1, p_2, \dots, p_m.$$

Let $n = p_1 p_2 \cdots p_m + 1$.

By Lemma 4.3, n has a prime factor p. But $p_1, \dots, p_m$ are the only primes, so $p = p_k$ for some k.

This means

$$p \mid p_1 p_2 \cdots p_m, \quad \text{so} \quad p \mid n-1.$$

But also $p \mid n$. So by Lemma 4.2 $p \mid 1$.

But 1 has no prime factors. ↯.

So our assumption was wrong, so there are infinitely many primes. $\square$

4.3 Greatest common divisors

Defn: Suppose $a, b \in \mathbb{N}$. The <u>greatest common divisor</u> of a and b is the largest $d \in \mathbb{N}$ such that $d \mid a$ and $d \mid b$.

We write $\gcd(a,b)$ for the greatest common divisor of a and b.

We say a and b are <u>coprime</u> if $\gcd(a,b) = 1$.

e.g. $\gcd(5,9) = 1$.

$\gcd(15,9) = 3$.

$\gcd(4,30) = 2$.

$\gcd(42,72) = 6$.

$\gcd(42000, 72000) = 6000.$

$\gcd(1,b) = 1$ for every b.

$\gcd(b,b) = b$ for every b.

if $a \mid b$, then $\gcd(a,b) = a$: $a \mid a$ and $a \mid b$, so a is a common divisor of a and b; it's the largest one because it's the largest divisor of a.

if p and q are primes and $p \neq q$, then $\gcd(p,q) = 1$. the only divisors of p are 1 and p, the only divisors of q are 1 and q, so the only common divisor is 1.

We can go beyond two numbers: if $a_1, a_2, \ldots, a_m \in \mathbb{N}$, then we can define $\gcd(a_1, a_2, \ldots, a_m)$. We can even consider infinitely many numbers.

e.g. $\gcd(3, 6, 9, 12, 15, \ldots) = 3.$

How do we find $\gcd(a,b)$?

<u>Slow method: write down all the divisors</u>

To find $\gcd(a,b)$, we can just write down all the divisors of a and of b, and find the largest number in both lists.

e.g. What is $\gcd(36, 90)$?

divisors of 36: $1, 2, 3, 4, 6, 9, 12, 18, 36$

divisors of 90: $1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90$

18 is the largest number in both lists, so $\gcd(36,90) = 18$.

This is very slow: finding all the divisors of a number takes a long time.

<u>Better method: use prime factorisations</u>

If we know the prime factorisation of n, then we can find all the divisors of n: every divisor is the product of <u>some of</u> the primes appearing.

e.g. The prime factorisation of 24 is

$$24 = 2 \times 2 \times 2 \times 3.$$

divisors: 2, 3, 2×2, 2×3, 2×2×2, 2×2×3, 2×2×2×3, 1

the product of no primes

So: to work out gcd(a,b), we can find the prime factorisations of a and b, and take the product of the primes appearing in both factorisations.

e.g. gcd(36, 90)

prime factorisation of 36:

$$36 = 2 \times \underline{2 \times 3 \times 3}$$

prime factorisation of 90:

$$90 = \underline{2 \times 3 \times 3} \times 5$$

The product of the primes in both lists is

$$2 \times 3 \times 3 = 18.$$

Unfortunately, finding the prime factorisation of a large integer is very slow.

(Internet security depends on this!)

<u>Fast method: Euclid's algorithm</u>

We'll give a fast method for finding gcd(a,b). First we prove two preparatory results.

The next lemma makes precise the idea of "division with remainder".

Lemma 4.5: Suppose $a, b \in \mathbb{N}$. Then there exist integers q, r such that $0 \le r < b$ and $a = qb + r$.

Pf: Let q be the largest integer such that $qb \le a$, and let $r = a - qb$. Then $a = qb + r$, so we just need to check that $0 \le r < b$.

$r \geq 0$ because $qb \le a$.

But also: q was chosen to be the <u>largest</u> integer such that $qb \le a$.

So $(q+1)b > a$

so $qb + b > a$

so $r = a - qb < b$. $\square$

The next result gives a relationship between gcds and division-with-remainder.

Proposition 4.6. Suppose $a, b, q, r \in \mathbb{Z}$, and $0 < r < b$, and $a = qb + r$. Then $\gcd(a,b) = \gcd(b,r)$.

Pf: We'll prove a stronger statement: the common divisors of a and b are the same as the common divisors of b and r.

So take $d \in \mathbb{N}$. We need to show that d is a common divisor of a and b iff d is a common divisor of b and r.

First suppose $d \mid a$ and $d \mid b$. Then there are $k, l \in \mathbb{N}$ such that $a = dk$ and $b = dl$. Then

$$r = a - qb = d(k - ql),$$

so $d \mid r$. So $d \mid b$ and $d \mid r$, so d is a common divisor of b and r.

Conversely, suppose $d \mid b$ and $d \mid r$. Then there are $l, m \in \mathbb{N}$ such that $b = dl$ and $r = dm$. So

$$a = qb + r = d(ql + m),$$

so $d \mid a$. So $d \mid a$ and $d \mid b$, so d is a common divisor of a and b. $\square$

e.g. Let $a = 32$, $b = 12$. When we divide a by b, we get

$$\underset{\substack{\uparrow \\ q}}{}\; 32 = \underset{\substack{\uparrow \\ q}}{2} \times 12 + \underset{\substack{\uparrow \\ r}}{8}$$

divisors of 32: 1, 2, 4, 8, 16, 32

divisors of 12: 1, 2, 3, 4, 6, 12

divisors of 8: 1, 2, 4, 8.

The common divisors of 32 and 12 are 1, 2, 4.

The common divisors of 12 and 8 are 1, 2, 4.

In particular,

$$\gcd(32, 12) = 4 = \gcd(12, 8).$$