Warmup

Recall that a "proof by induction" is done as follows: for a statement $S(n)$ that depends on an integer n,

1. prove a base (smallest) case; and
2. show that if $S(n)$ is true (the "induction hypothesis"), then so is $S(n+1)$.

You try: Prove the following identities using proof by induction.

(a) $1 + 2 + 3 + \cdots + n = n(n+1)2$

(b) For $a \neq 1$,

$$1 + a + a^2 + \cdots + a^n = \frac{1 - a^{n+1}}{1 - a}.$$

Strong induction: The inductive hypothesis becomes "assume $S(m)$ is true for *all* (base case)$\leqslant m \leqslant n$"; then the inductive step is to show $S(n+1)$ is true using any of those $S(m)$ for smaller m.

Primes and their properties

A prime number is a number $p \geqslant 2$ whose only (positive) divisors are 1 and p.

In $\mathbb{Z}_{>0}$:

Primes: 2, 3, 5, 7, . . . ; Composites: 4, 6, 8, 9, . . . ; Unit: 1.

Lemma

Let p be a prime number, and suppose that p divides the product ab. Then p divides a or b or both.

To prove, recall that there are some integers x and y such that

$$ax + py = \gcd(a, p).$$

Theorem (Prime Divisibility Property)

Let p be a prime number, and suppose that p divides the product $a_1 a_2 \cdots a_r$, where $a_i \in \mathbb{Z}$. Then p divides at least one of the factors a_1, a_2, . . . , a_r.

Today's goal: Every positive integer has a unique prime factorization.

Why is this important/special?? We've been taking this result for granted in doing many examples. But it turns out to be non-trivial.

Let's look at examples where "unique factorization into primes" fails...

Even numbers

Let $2\mathbb{Z}_{>0}$ be the set of positive even integers:

$$2\mathbb{Z}_{>0} = \{2z \mid z \in \mathbb{Z}_{>0}\}.$$

Defining divisibility: We say a divides b *in* $2\mathbb{Z}_{>0}$ if there is some $k \in 2\mathbb{Z}_{>0}$ such that $ak = b$. For example,

$$2 \text{ divides } 4, \quad \text{but not } 6 \qquad (6/2 = 3 \notin 2\mathbb{Z}_{>0}).$$

Defining primes: $2\mathbb{Z}_{>0}$ doesn't have any units, so we define a prime as a number p that has no other divisors in $2\mathbb{Z}_{>0}$. For example,

$$2, 6, 10, 14, 18, 22, 26, 30, \ldots.$$

But now, notice: $6, 8, 10$, and 30 are all prime in $2\mathbb{Z}_{>0}$, but

$$6 * 30 = 180 = 8 * 10.$$

Integers+

Recall $\mathbb{Z}[x]$ is the set of polynomials in x with integer coefficients. Now let

$$\mathbb{Z}[\sqrt{5}] = \{p(\sqrt{5}) \mid p(x) \in \mathbb{Z}[x]\}.$$

Since

$$\sqrt{5}^0, \sqrt{5}^2, \sqrt{5}^4, \dots \in \mathbb{Z}$$

and

$$\sqrt{5}^1, \sqrt{5}^3, \sqrt{5}^5, \dots \in \sqrt{5}\mathbb{Z},$$

we have

$$\mathbb{Z}[\sqrt{5}] = \{n + m\sqrt{5} \mid n, m \in \mathbb{Z}\}.$$

Notice that $\mathbb{Z} \subset \mathbb{Z}[\sqrt{5}]$ (all the numbers where $m = 0$).

Integers+

$$\mathbb{Z}[\sqrt{5}] = \{n + m\sqrt{5} \mid n, m \in \mathbb{Z}\}.$$

Defining divisibility: We say a divides b *in* $\mathbb{Z}[\sqrt{5}]$ if there is some $k \in \mathbb{Z}[\sqrt{5}]$ such that $ak = b$. For example,

2 divides 4 and 6, and also $2 + 2\sqrt{5}$.

Defining primes: $\mathbb{Z}[\sqrt{5}]$ has a unit, so primes are back to what we expect–a prime as a number p whose only divisors in $\mathbb{Z}[\sqrt{5}]$ are ± 1 and $\pm p$. For example,

$\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \dots$ and also $1 + \sqrt{5}$, $1 - \sqrt{5}$, $2 + 3\sqrt{5}$, $\dots$.

(To check: for a supposed prime p, what integers m, n, m', n' satisfy

$$p = (n + m\sqrt{5})(n' + m'\sqrt{5}) = (nn' + 5mm') + (nm' + mn')\sqrt{5}?)$$

But now, notice: ± 2 and $1 \pm \sqrt{5}$ are all prime in $\mathbb{Z}[\sqrt{5}]$, but

$$2(-2) = -4 = (1 + \sqrt{5})(1 - \sqrt{5}).$$

Back to positive integers...

Theorem (The Fundamental Theorem of Arithmetic)
Every integer $n \geqslant 2$ can be factored uniquely as

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

with $p_1 < p_2 < \cdots < p_r$ prime.

To prove, we show

1. Existence: The number n can be factored into a product of primes in some way. (Strong induction)
2. Uniqueness: There is only one such factorization. (Lemma)

Congruences

Recall the division algorithm says for any $a, n \in \mathbb{Z}$ with $n \neq 0$, there are unique integers q and r satisfying

$$a = nq + r \qquad \text{and} \qquad 0 \leqslant r < |b|.$$

Now, for two integers a, b, we say a is congruent to b modulo (mod) n, written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b,$$

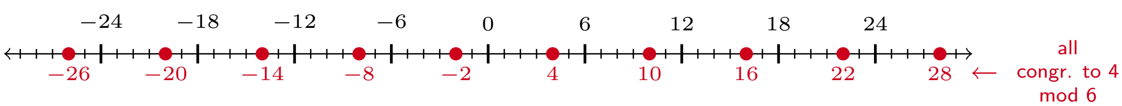
if a and b have the same remainders when divided by n.

Example: Letting $n = 6$, since

$$100 = 16 * 6 + 4 \quad \text{and} \quad 22 = 3 * 6 + 4,$$

we have $100 \equiv 22 \pmod{6}$.

More:



Congruences

For integers a, b, n, with $n \neq 0$, we say a is congruent to b modulo (mod) n, written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b,$$

if a and b have the same remainders when divided by n.

Notice, if a and b both have remainder r, then

$$a = q_a n + r \quad \text{and} \quad b = q_b n + r.$$

So

$$a - b = (q_a n + r) - (q_b n + r) = (q_a - q_b)n.$$

Thus $n | (a - b)$.

Similarly, suppose a and b are integers satisfying $n | (a - b)$, i.e. $nk = a - b$ for some $k \in \mathbb{Z}$. Then writing

$$a = q_a n + r_a \quad \text{and} \quad b = q_b n + r_b, \quad 0 \leqslant r_a, r_b < n,$$

we have

$$nk = a - b = (q_a n + r_a) - (q_b n + r_b) = (q_a - q_b)n + (r_a - r_b).$$

So $r_a - r_b$ is a multiple of n. But $-n < r_a - r_b < n$. So $r_a = r_b$.

Congruences

Theorem

For integers a, b, n, with $n \neq 0$, the following are equivalent:

1. *a and b have the same remainders when divided by n;*
2. *n divides $a - b$.*

Either way, we say that a is congruent to b modulo (mod) n, written

$$a \equiv b \pmod{n} \quad \textit{or} \quad a \equiv_n b.$$

Some properties: Fix $n \geqslant 1$.

1. Congruent is an equivalence relation (reflexive, symmetric, transitive).
2. If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then
   (a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and
   (b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.