Beginning of Jan.22, 2021

0.1 Mathematical Inductions

Induction

Let $\varphi(n)$ be a statement with respect to $n \in \mathbb{N}$. If

(1) $\varphi(x)$ holds for some $x \in \mathbb{N}$, and

(2) (*weak induction*) $\varphi(k) \implies \varphi(k+1)$ for all $k \geqslant x$ or (*strong induction*) $\varphi(x) \wedge \cdots \wedge \varphi(k) \implies \varphi(k+1)$ then

$\varphi(n)$ holds for all $n \in \mathbb{N}$ greater or equal to x.

0.2 Divisibility, Primes, and Factorization

Some "dumb" definitions first — these will become useful later on when we examine more general cases.

Definition 0.2.1

Let $a, b \in \mathbb{Z}$. We say a **divides** b, denoted as $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $ac = b$.

Definition 0.2.2

A positive integer > 1 is **prime** if and only if $p = ab \implies a = 1 \vee b = 1$.

Example 0.2.3. There are infinitely primes. (Product +1 trick.)

Theorem 0.2.4: The Division Algorithm

Let a, b be non-negative integers with $b > 0$. Then there exist (unique) q and (unique) r such that $a = bq + r$ with $0 \leqslant r < b$.

Proof. We'll only show existence. Let $\mathcal{S}$ be the set of non-negative integers of the form $a - bn$ for $n \in \mathbb{Z}$. Clearly setting $n = 0$ tells $\mathcal{S}$ is nonempty. By the Well-Ordering Principle, $\mathcal{S}$ has a smallest number r'. By definition $r' = a - bn$ and so $a = bn + r'$. If $r' \geqslant b$, subtracting b from both sides gives

$$0 < r' - b = a - bn - b = a - b(n+1) \implies a - b(n+1) \in \mathcal{S},$$

contradicting the assumption that r' is the minimal element. Hence $r' < b$ (and of course $r' \geqslant 0$). Done. □

Definition 0.2.5

The **greatest common divisor**, gcd, of $a, b \in \mathbb{Z}$ is the maximal integer that divides both a and b.

Corollary 0.2.6

If $\gcd(a, b) = 1$ then a and b are said to be **relatively prime**.

Euclidean Algorithm

Omitted

Theorem 0.2.7: Bezout's Identity

Let $a, b \in \mathbb{Z}$. Then there exists a $\mathbb{Z}$-combination of a and b that gives $\gcd(a, b)$, and $\gcd(a, b)$ is the smallest (positive) integer with this property. Proof is obvious by back substitution in Euclid's algorithm. *Or the one below.*

> ***Proof.*** Again define $\mathcal{S} := \{k > 0 : k = na + mb, n.m \in \mathbb{Z}\}$. It's nonempty since $|a| + |b| \in \mathcal{S}$. Then $\mathcal{S}$ has a minimal element q by the Well-Ordering Principle. We claim that $q = \gcd(a, b)$.
> By definition $q = na + mb$ for some n, m. It follows that if $p \mid a$ and $p \mid b$ implies $p \mid$ RHS and so $p \mid q$. Now it remains to show $q \mid a$ and $q \mid b$, i.e., q itself is a common divisor.
> Indeed, by the division algorithm, $a = qc + r$ or $r = a - qc$ for some $0 \leqslant r < q$. By definition since $q = na + mb$, rewriting $r = a - c(na + mb)$ suggests $r \in \mathcal{S}$. If $r > 0$, we have a contradiction since $r < q$ but q is assumed to be the minimal member of $\mathcal{S}$. Hence $r = 0$. □

Lemma 0.2.7.1: Euclid's Lemma

Suppose a and b are integers and p a prime. If p divides ab then $p \mid a \vee p \mid b$.

> ***Proof.*** Suppose $p \nmid a$. We'll show $p \mid b$. Indeed, from the assumption we have $\gcd(a, p) = 1$, and by Bezout's identity there exists some n, m such that $1 = na + mp$. Multiplying both sides by b gives $b = nab + mbp$. Since $p \mid ab$, $p \mid$ the RHS, and thus $p \mid b$. □

Theorem 0.2.8: Fundamental Theorem of Arithmetic

Every positive integer factors uniquely.

0.3 Modular Arithmetic, Congruences

Definition 0.3.1

Fix a modulus m, a positive integer. If a, b are integers define $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$. The relation $a \equiv b \pmod{m}$ is called a **congruence** and we say a and b are in the same **congruence class** $[a]$ mod n.