Induction and Divisibility

Andres Buritica Monroy

1 Induction and variants

Arguably, the defining property of the integers is the **Principle of Mathematical Induction**: if we have a set $S \subseteq \mathbb{N}$ such that $1 \in S$ and $\forall a \in S,\ a+1 \in S$ then $S = \mathbb{N}$.

To prove that some sentence $P(n)$ is true for all positive integers n, we follow the following structure.

- Prove that $P(1)$ is true.
- Prove that if $P(n)$ is true, then $P(n+1)$ is true.

If we've done both of those things, why can we conclude that $P(a)$ is true for all $a \in \mathbb{N}$?

We may use induction to prove some foundational results about the integers:

- For all positive integers n, $n \geq 1$.
- If S is a nonempty set of positive integers, there is some $a \in S$ such that for any $b \in S$ we have $a \leq b$. This is known as the **Well-Ordering Principle**.

The final addition to our induction toolkit will be **strong induction**: if S is a set of positive integers such that $1 \in S$ and

$$\forall a \in \mathbb{N},\ (\forall b \in \mathbb{N},\ b \leq a \implies b \in S) \implies a+1 \in S,$$

then $\mathbb{N} = S$.

2 Divisibility

For integers a and b, we say $a \mid b$ (read "a divides b") if there is some integer c with $b = a \times c$.

- Prove that if $a \mid b$ and $a \mid c$, then for any integers m and n, $a \mid bm + cn$.
- Prove that if a and b are positive integers with $a \mid b$ then $a \leq b$.

We define a *prime* as a positive integer larger than 1 which is not divisible by any positive integer other than 1 and itself.

- Prove that every positive integer larger than 1 has a prime factor.
- Prove that there are infinitely many primes.

3 GCD, Euclid, Bezout

We define the *greatest common divisor* of two integers a and b, not both of which are 0, as the largest positive integer d such that $d \mid a$ and $d \mid b$. We notate it by $\gcd(a, b)$. For convenience we also define $\gcd(0, 0) = 0$.

Similarly, the *least common multiple* $\operatorname{lcm}(a, b)$ is the smallest positive integer l such that $a \mid l$ and $b \mid l$. For convenience we also define $\gcd(0, a) = 0$.

- Let a be an integer and let b be a positive integer. Prove that there is exactly one pair of integers (q, r) with $0 \leq r < b$ such that $a = qb + r$. (Division Algorithm)
- Prove that for any integers a, b, q, r, if $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$. (Euclid's Algorithm)
- Let a and b be integers. Prove that there are integers c and d such that $ac + bd = \gcd(a, b)$. (Bezout's Identity)
- Let a and b be integers with $\gcd(a, b) = 1$, and let c be an integer. Prove that if $a \mid c$ and $b \mid c$ then $ab \mid c$.
- Assume that $p_1, \ldots, p_m,\ q_1, \ldots, q_n$ are primes such that

  $$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

  Prove that the q_is are a permutation of the p_is.

4 Prime Factorisations

Therefore, each positive integer has a unique prime factorisation (the Fundamental Theorem of Arithmetic). In particular we can write a positive integer n uniquely as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where p_i are all prime and e_i are all positive integers.

Prime factorisations allow us to view statements about divisibility and multiplication in terms of the exponents e_i.

In what follows, let

$$a = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m},\ b = q_1^{f_1} q_2^{f_2} \cdots q_k^{e_k}.$$

- Prove that $a \mid b$ if and only if for each i we have that $p_i = q_j$ for some j, and that $e_i \leq f_j$.
- Prove that a is a perfect kth power if and only if $k \mid e_i$ for all i.
- Prove that the lcm is found by taking the maximum power of each prime that divides either a or b, while the gcd is found by taking the minimum power of each prime that divides both a and b.
- Prove that $\gcd(a, b) \times \operatorname{lcm}(a, b) = ab$.

5 Strategies

- Take out the gcd: that is, if you have two integers a and b you can write $a = dx,\ b = dy$ where x and y are coprime.
- Factorisations: two especially useful ones are

$$axy + bx + cy = d \iff (ax + c)(ay + b) = ad + bc,$$
$$a^k - b^k = (a - b)\left(a^{k-1} + a^{k-2}b + \cdots + b^{k-1}\right).$$

6 Problems

1. Find all integers n such that $n^2 + 1$ divides $n^3 + n^2 - n - 15$.
2. Given three distinct natural numbers a, b, c, show that

$$\gcd(ab + 1, bc + 1, ca + 1) \le \frac{a + b + c}{3}.$$

3. Let p be a prime with $p > 3$. Prove that there are positive integers $a < b < \sqrt{p}$ such that $p - b^2 \mid p - a^2$.
4. Let S be the set of ordered pairs of integers. We say that two elements (a, b) and (c, d) of S are k-friends if there is an element (e, f) of S such that the area of the triangle formed by these three points is k.[1] Find the smallest positive integer k such that there exists a set of 200 elements of S such that any pair of them are k-friends.
5. Find all pairs of positive integers a, b such that

$$b^2 - a \mid a^2 + b \quad \text{and} \quad a^2 - b \mid b^2 + a.$$

6. Prove that for any nonnegative integer n, the number $7^{7^n} + 1$ is the product of at least $2n + 3$ (not necessarily distinct) primes.

[1] The *shoelace formula* states that the area of this triangle is $\frac{1}{2}(ad - bc + cf - de + eb - af)$.

7 Homework

1. Prove that every positive integer can be uniquely represented as a sum of one or more Fibonacci numbers such that the sum does not include two consecutive Fibonacci numbers.

2. Let a, b, c be positive integers with $a^2 + b^2 = c^2$, such that no positive integer larger than 1 divides all of them. Prove that there exist positive integers x, y, z such that a, b, c equal $x^2 - y^2, 2xy, x^2 + y^2$ in some order.

3. (a) Find all integers a, b, c with $1 < a < b < c$ such that $(a-1)(b-1)(c-1)$ divides $abc - 1$.

   (b) Do there exist distinct prime numbers a, b, c such that

$$a \mid bc + b + c, \;\; b \mid ac + a + c, \;\; c \mid ab + a + b?$$