INTRODUCTION TO PROOFS

formerly called Foundation and Proofs

Notes by Dr. Lynne H. Walling

10. More proofs using contradiction, construction, and induction

Proposition 10.1. *For prime $p \in \mathbb{Z}$, $\sqrt{p}$ is irrational.*

Proof. For the sake of contradiction, suppose $\sqrt{p} \in \mathbb{Q}$. Thus $\sqrt{p} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ with $b \neq 0$; we can assume $\text{hcf}(a, b) = 1$. Then $p = \frac{a^2}{b^2}$, so $pb^2 = a^2$. Thus $p|a$; hence $a = pc$ for some $c \in \mathbb{Z}$. This means we have $pb^2 = (pc)^2 = p^2c^2$, so $b^2 = pc^2$ and hence $p|b$. But then $p|\text{hcf}(a, b)$, contradicting that $\text{hcf}(a, b) = 1$. Hence $\sqrt{p}$ cannot be rational. □

Proposition 10.2. *There are infinitely many primes in $\mathbb{Z}_+$; in fact, there are countably many primes.*

Proof. Let X be the set of primes. Note that since $X \subseteq \mathbb{Z}_+$, we know X is either finite or countable.

For the sake of contradiction, suppose there are only finitely many primes in $\mathbb{Z}_+$; let t be the number of primes. We know there is at least one prime, namely 2, so $t \geq 1$. Let $p_1, \ldots, p_t$ be all the primes in $\mathbb{Z}_+$. Consider $m = p_1 \cdots p_t + 1$. Since $m \in \mathbb{Z}$ with $m > 1$, by the Fundamental Theorem of Arithmetic we know there is some prime $q \in \mathbb{Z}_+$ so that $q|m$. So there is some $m' \in \mathbb{Z}$ so that $m = qm'$, and hence $1 = qm' - p_1 \cdots p_t$. Since we have assumed there are finitely many primes, we must have $q = p_j$ for some $j \in \mathbb{Z}$ with $1 \leq j \leq t$. Hence $1 = p_j m' - p_1 \cdots p_t$, so $p_j|1$. But since $q = p_j$ is prime and thus $p_j > 1$, this is impossible. Thus there cannot be finitely many primes. □

Given $a, b, c \in \mathbb{Z}$, we can use Euclid's algorithm to find all $x, y \in \mathbb{Z}$ so that $ax + by = c$. Before we prove the general theorem, let us consider a specific example.

Example: We want to construct all $x, y \in \mathbb{Z}$ so that $6x + 8y = 2$.

First note that for $x, y \in \mathbb{Z}$, we have $6x + 8y = 2$ if and only if we have $3x + 4y = 1$. Since $\text{hcf}(3, 4) = 1$, we know (by Euclid's algorithm) that $\exists s, t \in \mathbb{Z}$ so that $3s + 4t = 1$. (By inspection, we see that $3 \cdot (-1) + 4 \cdot 1 = 1$, so in this case we don't need to use Euclid's algorithm to find $s, t \in \mathbb{Z}$ so that $3s + 4t = 1$.) Now suppose we also have $x, y \in \mathbb{Z}$ so that $3x + 4y = 1$. Hence $3s + 4t = 3x + 4y$, so $3(s - x) = 4(y - t)$. Thus $3|4(y - t)$, and since $\text{hcf}(3, 4) = 1$, $3|y - t$. Hence $\exists k \in \mathbb{Z}$ so that $y - t = 3k$, or equivalently, $y = t + 3k$. A virtually identical argument shows that $4|s - x$, so $\exists k' \in \mathbb{Z}$ so that $x = s - 4k'$. Therefore

$$3s + 4t = 3x + 4y = 3(s - 4k') + 4(t + 3k),$$

hence $0 = -12k' + 12k$, or equivalently, $k' = k$. In summary, we have shown that if $s, t, x, y \in \mathbb{Z}$ so that $3s + 4t = 1 = 3x + 4y$, then $\exists k \in \mathbb{Z}$ so that $x = s - 4k$ and $y = t + 3k$.

On the other hand, suppose $3s + 4t = 1$ (which is the case when $s = -1$, $t = 1$). Take any $k \in \mathbb{Z}$ and set $x = s - 4k$, $y = t + 3k$. Then

$$3x + 4y = 3s + 4t = 1.$$

So $3x + 4y = 1$ if and only if $x = -1 - 4k$, $y = 1 + 3k$ for some $k \in \mathbb{Z}$, and hence $6x + 8y = 2$ if and only if $x = -1 - 4k$, $y = 1 + 3k$ for some $k \in \mathbb{Z}$.

More generally, we have the following proposition and corollary, which one proves as exercises.

Proposition 10.3. *Fix $a, b, c \in \mathbb{Z}$ so that $a, b \neq 0$. Let $d = hcf(a, b)$. Take $a', b' \in \mathbb{Z}$ so that $a = da'$ and $b = db'$.*

(a) *If $d \nmid c$ then there do not exist $x, y \in \mathbb{Z}$ so that $ax + by = c$.*
(b) *Suppose $d|c$. Then $\exists s, t \in \mathbb{Z}$ so that $as + bt = c$. Also, for $x, y \in \mathbb{Z}$, we have $ax + by = c$ if and only if $\exists k \in \mathbb{Z}$ so that $x = s - b'k$ and $y = t + a'k$.*

Corollary 10.4. *Fix $a, b, n \in \mathbb{Z}$ so that $n \geq 1$. There $\exists x \in \mathbb{Z}$ so that $ax \equiv b \pmod{n}$ if and only if $hcf(a, n)|b$.*

Proposition 10.5. *Suppose $m \in \mathbb{Z}_+$ with $m \geq 2$ and $A_1, \ldots, A_m$ are nonempty, finite sets.*

(a) *Suppose $A_1, \ldots, A_m$ are pairwise disjoint, meaning that for $i, j \in \mathbb{Z}_+$ with $i, j \leq m$ and $i \neq j$, we have $A_i \cap A_j = \emptyset$. Then*

$$|A_1 \cup \cdots \cup A_m| = |A_1| + \cdots + |A_m|.$$

(b) $|A_1 \times \cdots \times A_m| = |A_1| \cdots |A_m|$.

Proof. We prove (b) and leave (a) as an exercise.

(b) We argue by induction on m.

[Base case.] Let $|A_1| = s$, $|A_2| = t$. Thus we know there exist bijections $f : \{1, 2, \ldots, s\} \to A_1$ and $g : \{1, 2, \ldots, t\} \to A_2$. For $i, j \in \mathbb{Z}_+$ with $i \leq s$, $j \leq t$, set $a_i = f(i)$ and set $b_j = g(j)$. Notice that since f and g are bijections, $a_1, a_2, \ldots, a_s$ are distinct and $b_1, b_2, \ldots, b_t$ are distinct.

We define $h : \{1, 2, \ldots, st\} \to A_1 \times A_2$ as follows. Take $n \in \{1, 2, \ldots, st\}$. Recall that as a consequence of the division algorithm for $\mathbb{Z}$, $\exists! q, r \in \mathbb{Z}$ so that $n = tq + r$ where $1 \leq r \leq t$. Note that since $n \geq 1$, we must have $q \geq 0$, for if $q < 0$ then $q \leq -1$ and $n \leq -t + r \leq 0$. Also note that $q < s$, else $st + 1 \leq n = tq + r \leq st$. Hence $a_{q+1} \in A_1$, and $b_r \in A_2$. We define

$$h(n) = (a_{q+1}, b_r) \text{ where } q, r \in \mathbb{Z} \text{ so that } n = tq + r \text{ where } 1 \leq r \leq t.$$

Since the conditions on q and r determine them uniquely, there is no ambiguity in the meaning of $h(n)$, or in other words, h is well-defined.

We need to show that h is bijective. Suppose first that $m, n \in \{1, 2, \ldots, st\}$ so that $h(m) = h(n)$. Take the unique $q, r, q', r' \in \mathbb{Z}$ so that $n = tq + r$, $m = tq' + r'$ where $1 \leq r \leq t$, $1 \leq r' \leq t$. Then $(a_{q'+1}, b_{r'}) = f(m) = f(n) = (a_{q+1}, b_r)$. Thus we have $a_{q'+1} = a_{q+1}$ and $b_{r'} = b_r$; hence $q' + 1 = q + 1$ (since $a_1, a_2, \ldots, a_s$ are distinct) and $r' = r$ (since $b_1, b_2, \ldots, b_t$ are distinct). Thus $m = tq' + r' = tq + r = n$, showing that h is injective. Now take an arbitrary element $(a_i, b_j) \in A_1 \times A_2$; thus $1 \leq i \leq s$ and $1 \leq j \leq t$, so $1 \leq t(i - 1) + j \leq st$. Hence with $n = t(i - 1) + j$, we

have $h(n) = (a_i, b_j)$, showing that h is surjective. Thus h is bijective. So $|A_1 \times A_2| = st = |A_1||A_2|$.

[Induction step.] Suppose that $k \in \mathbb{Z}$ with $k \geq 2$, and suppose that $|A_1 \times \cdots \times A_k| = |A_1| \cdots |A_k|$. Set $A = A_1 \times \cdots \times A_k$. Thus

$$|A_1 \times \cdots \times A_k \times A_{k+1}| = |A \times A_{k+1}|,$$

and by the base case, we know $|A \times A_{k+1}| = |A| \cdot |A_{k+1}|$. So using the induction hypothesis, we get

$$|A_1 \times \cdots \times A_k \times A_{k+1}| = |A| \cdot |A_{k+1}| = |A_1| \cdots |A_k| \cdot |A_{k+1}|.$$

Hence by the principle of mathematical induction, (b) holds for all $m \in \mathbb{Z}$ with $m \geq 2$. □

As an exercise, one proves the following.

Proposition 10.6. *The union of countably many nonempty, pairwise disjoint finite sets is countable.*

Proposition 10.7. *Suppose A and B are nonempty finite sets with $|A| = |B|$.*

(a) *Suppose $f : A \to B$ is injective. Then f is bijective.*
(b) *Suppose $f : A \to B$ is surjective. Then f is bijective.*

Proof. Let $n \in \mathbb{Z}_+$ so that $n = |A|$. So $|B| = n$, and there are bijections $g : \{1, 2, \ldots, n\} \to A$ and $h : \{1, 2, \ldots, n\} \to B$; for $i \in \{1, 2, \ldots, n\}$, set $a_i = g(i)$, $b_i = h(i)$. Since g is injective, this means $a_1, \ldots, a_n$ are distinct; similarly, $b_1, \ldots, b_n$ are distinct.

(a) Suppose $f : A \to B$ is injective. Then $f(a_1), \ldots, f(a_n)$ are distinct, so $|f(A)| = |A| = n$. Since $f(A) \subseteq B$ and $|f(A)| = |B| = n \leq \infty$, we must have $f(A) = B$. Thus f is surjective and hence bijective.

(b) Suppose $f : A \to B$ is surjective. For the sake of contradiction, suppose f is not injective. Thus $\exists i, j \in \{1, 2, \ldots, n\}$ so that $a_i \neq a_j$ but $f(a_i) = f(a_j)$. Since $a_i \neq a_j$, we have $i \neq j$. Thus

$$f(A) = \{a_k : \ k \in \mathbb{Z}, \ 1 \leq k \leq n, \ k \neq j \ \}.$$

So $|f(A)| < n$. But since f is surjective, we know $f(A) = B$ and hence $|f(A)| = |B| = n$. This gives us a contradiction, so we must have that f is injective and hence bijective. □

Finally, we offer a "party trick" based on the theory presented in these notes.

Take $x \in \mathbb{Z}_+$. Written as a decimal expansion, we write x as

$$a_m a_{m-1} \cdots a_1 a_0$$

where $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ for $0 \leq i \leq m$. Thus

$$x = \sum_{i=0}^{m} a_i 10^i.$$

We know $10 \equiv 1 \pmod 9$. One uses induction to show that for all $i \in \mathbb{Z}_+$, we have $10^i \equiv 1 \pmod 9$. Hence, again using induction, one shows that

$$\sum_{i=0}^{m} a_i 10^i \equiv \sum_{i=0}^{m} a_i \pmod 9.$$

Recall that x is divisible by 9 if and only if $x \equiv 0 \pmod 9$, so x is divisible by 9 if and only if the digits of x sum to a number divisible by 9.

One can devise a similar party trick to test for divisibility by 11. In this case one uses that for $i \in \mathbb{Z}$, $i \geq 0$, $10^i \equiv 1 \pmod{11}$ when i is even, and $10^i \equiv -1 \pmod{11}$ when i is odd. [So what is the party trick?]