INTRODUCTION TO PROOFS

formerly called Foundation and Proofs

Notes by Dr. Lynne H. Walling

7. Strong induction and the Fundamental Theorem of Arithmetic

An argument by strong induction proceeds as follows. Suppose $P(n)$ is the proposition that the integer n has property P. Fix $n_0 \in \mathbb{Z}$. To prove that $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \geq n_0$ using strong induction, we first establish that $P(n_0)$ holds, and then we show that for $k \in \mathbb{Z}$ with $k \geq n_0$,

$$[P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k)] \implies P(k+1).$$

As an example, we will prove the Fundamental Theorem of Arithmetic, which states that for $n \in \mathbb{Z}$ with $n > 1$, n can be written uniquely as a product of primes. Recall that a prime is an integer $p > 1$ so that the only positive integers that divide p are 1 and p.

Before we can prove the Fundamental Theorem of Arithmetic, we need to establish some other basic results.

Definition. We say a positive integer p is prime if $p > 1$, and the only positive divisors of p are 1 and p.

Remark: Later we will see that there are infinitely many primes.

Proposition 7.1. *Suppose $q_1, \ldots, q_r \in \mathbb{Z}$ where $r \in \mathbb{Z}$ with $r \geq 2$, and suppose p is a prime so that $p|q_1 \cdots q_r$. Then for some $i \in \mathbb{Z}$ with $1 \leq i \leq r$, we have $p|q_i$.*

Proof. We proceed by induction on r.

Suppose that $p|q_1q_2$. Recall that we have seen that if $a, b, c \in \mathbb{Z}$ with $c \neq 0$, $c|ab$, and $\text{hcf}(b, c) = 1$, then $c|a$. If $p|q_1$ then we are done. So suppose $p \nmid q_1$. Thus $\text{hcf}(p, q_1) = 1$ [since the only positive divisors of p are 1 and p, and p is not a common factor of p and q_1]. Hence by a previous proposition, $p|q_2$.

Now suppose $k \in \mathbb{Z}$ with $k \geq 2$, and suppose that if $p|q_1 \cdots q_k$ where $q_1, \ldots, q_k \in \mathbb{Z}$, then $p|q_i$ for some $i \in \mathbb{Z}$ with $1 \leq i \leq k$. Suppose $q_1, \ldots, q_k, q_{k+1} \in \mathbb{Z}$ with $p|q_1 \cdots q_kq_{k+1}$. Set $t = q_1 \cdots q_k$. Thus $p|tq_{k+1}$, so by the above corollary, $p|t$ or $p|q_{k+1}$. If $p|t$ then our induction hypothesis tells us that $p|q_i$ for some $i \in \mathbb{Z}$ with $1 \leq i \leq k$. If $p \nmid t$ then $p|q_{k+1}$. Hence $p|q_i$ for some $i \in \mathbb{Z}$ with $1 \leq i \leq k+1$.

Thus by the principle of mathematical induction, the corollary is proved. □

Theorem 7.2. *(Fundamental Theorem of Arithmetic) For every $n \in \mathbb{Z}$ so that $n > 1$, we have $n = p_1p_2 \cdots p_r$ for some primes $p_1, p_2, \ldots, p_r$ with $p_1 \leq p_2 \leq \cdots \leq p_r$. Further, if we also have $n = q_1q_2 \cdots q_s$ for primes $q_1, q_2, \ldots, q_s$ with $q_1 \leq q_2 \leq \cdots \leq q_s$, we have $r = s$ and $p_i = q_i$ for all $i \in \mathbb{Z}$ with $1 \leq i \leq r$.*

Proof. We first argue by strong induction to show that each integer $n > 1$ is a product of primes.

First, we note that 2 is a prime, so 2 is a product of primes (where there is only one prime in this product).

Now suppose that $k \in \mathbb{Z}$ with $k \geq 2$, and suppose that for all integers $m \in \mathbb{Z}$ with $2 \leq m \leq k$, m is a product of primes. Consider the integer $k+1$. If $k+1$ is prime, then we are done. So suppose $k+1$ is not prime; thus 1 and $k+1$ are not the only positive integers dividing $k+1$. Hence there is some $a \in \mathbb{Z}_+$ so that $1 < a < k+1$ with $a|k+1$; this means there is some $b \in \mathbb{Z}_+$ so that $ab = k+1$. Since $1 < a$, we have $b < ab$, so $b < k+1$. Also, $1 \leq b$; since $a < k+1$ and $ab = k+1$, we have $1 < b$. Thus a and b are products of primes, so $k+1$ is as well. Hence by the principle of mathematical induction, every integer $n > 1$ is a product of primes.

Now we want to show that for any integer $n > 1$, there is a unique way to realise n as a product of primes. More precisely, we want to show that if $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ with $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ primes so that $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$, then $r = s$ and $p_i = q_i$ for all $i \in \mathbb{Z}$ with $1 \leq i \leq r$. To prove this, we argue by induction on $r \in \mathbb{Z}_+$.

More formally, for $r \in \mathbb{Z}_+$, we let $P(r)$ be the proposition that if $p_1 \cdots p_r = q_1 \cdots q_s$ with $p_1 \leq \cdots \leq p_r$ primes and $q_1 \leq \cdots \leq q_s$ primes, we have $r = s$ and $p_i = q_i$ for all $i \in \mathbb{Z}$ with $1 \leq i \leq r$.

Suppose first that $p_1 = q_1 \cdots q_s$ where p_1 is prime and $q_1 \leq \cdots \leq q_s$ are prime (here $s \in \mathbb{Z}_+$). Since p_1 is prime and thus cannot be a product of two or more primes, it must be the case that $s = 1$ and $p_1 = q_1$. [This proves the base case for the induction argument, i.e. this shows $P(1)$ holds.]

Now suppose that $k \in \mathbb{Z}_+$, and that whenever $n = p_1 \cdots p_k = q_1 \cdots q_s$ with $p_1, \cdots, p_k, q_1, \ldots, q_s$ primes and $p_1 \leq \cdots \leq p_k$, $q_1 \leq \cdots \leq q_s$, we have $k = s$ and $p_i = q_i$ for all $i \in \mathbb{Z}$ with $1 \leq i \leq k$. [This is the induction hypothesis.] Suppose now that $a = p_1 \cdots p_k p_{k+1} = q_1 \cdots q_t$ with $p_1, \ldots, p_k, p_{k+1}, q_1, \ldots, q_t$ primes and $p_1 \leq \cdots \leq p_k \leq p_{k+1}$, $q_1 \leq \cdots \leq q_t$. Note that since $k \geq 1$, a is not prime, and hence $t \geq 2$. Let p be the largest prime so that $p|a$. [Note that there are only finitely many primes dividing a since each such prime q satisfies $2 \leq q \leq a$, and there are only finitely many integers between 2 and a.] Thus we have $p \geq p_{k+1}$. Also, since $p|a$, we have $p|p_1 \cdots p_k p_{k+1}$, hence $p|p_i$ for some $i \in \mathbb{Z}$, $1 \leq i \leq k+1$. Since p_i is prime, we must have $p = p_i$. So $p = p_i \leq p_{k+1}$. Also, by our choice of p, we have $p \geq p_{k+1}$; hence we must have $p = p_{k+1}$.

A virtually identical argument shows that $p = q_t$, and hence $p_{k+1} = q_t$. Thus $p_1 \cdots p_k = q_1 \cdots q_{t-1}$. By the induction hypothesis, we have $k = t-1$ and $p_i = q_i$ for $i \in \mathbb{Z}$ with $1 \leq i \leq k$. Therefore we have $k+1 = t$ and $p_i = q_i$ for all $i \in \mathbb{Z}$ with $1 \leq i \leq k+1$.

Consequently, by the principle of mathematical induction, the factorisation of an integer $n > 1$ as a product of (nondecreasing) primes is unique. □

Corollary 7.3. *For $x \in \mathbb{Q}_+$, $\exists!$ $a, b \in \mathbb{Z}_+$ so that $hcf(a, b) = 1$ and $x = \frac{a}{b}$.*

Proof. Take $x \in \mathbb{Z}_+$. Thus $\exists a, b \in \mathbb{Z}$, $a, b \neq 0$, so that $x = \frac{a}{b}$. Since $x > 0$, we have $x = |x| = \frac{|a|}{|b|}$, so we have that x is a quotient of two elements of $\mathbb{Z}_+$.

So suppose $a, b > 0$. Let $c = \text{hcf}(a, b)$, and take $a', b' \in \mathbb{Z}_+$ so that $a = ca'$ and $b = cb'$. Thus $\text{hcf}(a', b') = 1$ and $x = \frac{a'}{b'}$.

Now suppose $x \in \mathbb{Q}_+$ and $a, b, c, d \in \mathbb{Z}_+$ so that $x = \frac{a}{b} = \frac{c}{d}$ with $\text{hcf}(a, b) = 1 = \text{hcf}(c, d)$. Thus $ad = bc$. Suppose $a = 1$; then $d = bc$, so $c|d$. Since $\text{hcf}(c, d) = 1$ and $c > 0$, this means $c = 1$ and hence $a = c$ and $b = d$. So suppose $a > 1$; then $a = p_1 \cdots p_r$ for some $r \in \mathbb{Z}_+$ and primes $p_1, \ldots, p_r$. We now argue by induction on r to show that $a = c$ and $b = d$. First, suppose $a = p_1$ (p_1 prime). We have $p_1|bc$ and $\text{hcf}(a, b) = 1$, so $\text{hcf}(p_1, b) = 1$ and hence $p_1|c$. Thus $c = p_1c'$ for some $c' \in \mathbb{Z}_+$. So $d = bc'$ and hence $c'|d$. Since $\text{hcf}(c, d) = 1$ and c' is a positive factor of d, we must have $c' = 1$ and hence $a = p_1 = c$ and $b = d$. Now suppose $k \geq 1$ and whenever $p_1, \ldots, p_k$ are prime and $b', c', d' \in \mathbb{Z}_+$ so that $\text{hcf}(p_1 \cdots p_k, b') = 1 = \text{hcf}(c', d')$ with $p_1 \cdots p_k d' = b'c'$, we have $p_1 \cdots p_k = c'$. Suppose $a = p_1 \cdots p_k p_{k+1}$ where $p_1, \ldots, p_k, p_{k+1}$ are prime. Thus $p_{k+1}|c$, so $c = p_{k+1}c'$ for some $c' \in \mathbb{Z}_+$. Therefore $p_1 \cdots p_k d = bc'$, so by the induction hypothesis, $p_1 \cdots p_k = c'$. Hence $a = c$ and $b = d$. □

Remark: One can use induction and the Fundamental Theorem of Arthmetic to prove the following generalisation of the Chinese Remainder Theorem: Suppose $r \in \mathbb{Z}$ with $r \geq 2$, and $m_1, \ldots, m_r \in \mathbb{Z}_+$ are pairwise relatively prime, meaning that $\text{hcf}(m_i, m_j) = 1$for $i, j \in \mathbb{Z}$ with $1 \leq i \leq r$, $1 \leq j \leq r$ and $i \neq j$. For any $a_1, \ldots, a_r \in \mathbb{Z}$, there is some $x \in \mathbb{Z}$ so that $x \equiv a_i \pmod{m_i}$ for all $i \in \mathbb{Z}$ with $1 \leq i \leq r$. Further, with x as above and $x' \in \mathbb{Z}$, we have $x' \equiv a_i \pmod{m_i}$ for $i = 1, 2, \ldots, r$ if and only if $x' \equiv x \pmod{m_1 m_2 \cdots m_r}$.

Application: We make use of the Fundamental Theorem of Arithmetic to find all primes p so that $5p + 9 = n^2$ for some $n \in \mathbb{Z}_+$.

Strategy: First, we suppose we have a prime p so that $5p + 9 = n^2$ for some $n \in \mathbb{Z}_+$, and we deduce constraints on p. Then we consider all primes p subject to these constraints and determine for which of these p we have that $5p + 9 = n^2$ for some $n \in \mathbb{Z}_+$.

Suppose p is prime and $n \in \mathbb{Z}_+$ so that $5p + 9 = n^2$. Since so $5p = (n+3)(n-3)$, and $n+3 > 0$. By the Fundamental Theorem of Arithmetic, the only positive factors of $5p$ are $1, 5, p, 5p$. Since $n \in \mathbb{Z}_+$, we know that $n + 3$ is positive.

Suppose $n+3 = 1$. Then $n-3 = -5$, meaning $5p = (n+3)(n-3) = -5$. But this implies $p = -1$, which is not prime. So we cannot have $n + 3 = 1$.

Suppose $n + 3 = 5$. Then $n - 3 = -1$, so $5p = (n + 3)(n - 3) = -5$ and hence $p = -1$. But this is impossible [since -1 is not prime].

Suppose $n+3 = p$. Thus $n-3 = p-6$, so $5p = p(p-6)$. Hence $5 = p-6$, so $p = 11$, which is prime. [So $n + 3 = p$ does not lead to a contradiction.]

Suppose $n+3 = 5p$. Thus $5p = (n+3)(n-3) = 5p(n-3)$. Hence $n-3 = 1$, and so $n = 4$. Then $5p = (n + 3)(n - 3) = 7$; but this is impossible, since 5 does not divide [the prime] 7.

This shows that if p is a prime so that $5p + 9 = n^2$ for some $n \in \mathbb{Z}_+$ then $p = 11$. On the other hand, with $p = 11$, we have $5p + 9 = 55 + 9 = 64 = 8^2$.

Hence p is a prime with $5p+9 = n^2$ for some $n \in \mathbb{Z}_+$ if and only if $p = 11$.