INTRODUCTION TO PROOFS

formerly called Foundation and Proofs

Notes by Dr. Lynne H. Walling

6. Algorithms, recursion, and mathematical induction

An algorithm is a logical step-by-step procedure for solving a problem in a finite number of steps. Many algorithms are recursive, meaning that after one or more initial steps, a general method is given for determining each subsequent step on the basis of steps already taken.

As an example of a recursive algorithm, we discuss Euclid's algorithm for finding the highest common factor of two nonzero integers.

First, recall that we have a "division algorithm" for $a, b \in \mathbb{Z}_+$:

Theorem 6.1. *Suppose $a, b \in \mathbb{Z}_+$. Then $\exists! q, r \in \mathbb{Z}$ so that $b = aq + r$ where $0 \leq r < a$.*

Proof. Consider the set $A = \{u \in \mathbb{Z} : \ au \leq b \ \}$. Since $0 \in A$, we know A is nonempty, and since $b \leq ab$, A is bounded above; hence we can choose q to be the maximal element in A. [Thus q is the largest integer so that $aq \leq b$.] Set $r = b - aq$. So $b = aq + r$ with $0 \leq r < a$. [If $r \geq a$, then we would have $a(q+1) \leq b$, contrary to our choice of q.] Note also that q, r are the unique integers so that $b = aq + r$ with $0 \leq r < a$. To see this, suppose $q', r' \in \mathbb{Z}$ so that

$$b = aq' + r' \text{ with } 0 \leq r' < a.$$

Thus $aq + r = aq' + r'$, so $a(q - q') = r' - r$. Since $0 \leq r < a$ and $0 \leq r' < a$, we have $-a < r' - r < a$. Note that 0 is the only integer strictly between $-a$ and a that is divisible by a. Since $q - q'$ is an integer with $a(q - q') = r' - r$, we must have $r' - r = 0$ and $q - q' = 0$, meaning $r' = r$ and $q' = q$. Hence there are unique $q, r \in \mathbb{Z}$ so that $b = aq + r$ with $0 \leq r < a$. □

Note: An immediate consequence is that with $n \in \mathbb{Z}_+$, $\forall b \in \mathbb{Z}$, $\exists! r \in \mathbb{Z}$ so that $b \equiv r \pmod{n}$ with $0 \leq r < n$. Hence there are n congruence classes modulo n: $[0], [1], [2], \ldots, [n-1]$ where, for $r \in \mathbb{Z}$,

$$[r] = \{m \in \mathbb{Z} : \ m \equiv r \pmod{n} \ \}.$$

As an exercise, one proves the following.

Proposition 6.2. *Suppose $a, b, c \in \mathbb{Z}_+$. Then $\exists! q, r \in \mathbb{Z}$ so that $b = aq + r$ with $c \leq r < a + c$.*

Remark: We can extend the division algorithm to show that for $a, b \in \mathbb{Z}$ with $a \neq 0$, there exist unique $q, r \in \mathbb{Z}$ so that $b = aq + r$ with $0 \leq r < |a|$.

Definitions. With $a, b, c \in \mathbb{Z}$, c is a common divisor of a and b if $c|a$ and $c|b$. Note that 1 is always a common divisor of a and b, and if $a \neq 0$, no integer larger than $|a|$ can be a common divisor of a and b. Also note that every $x \in \mathbb{Z}$ is a divisor of 0, as $0 = 0 \cdot x$. With $a, b \in \mathbb{Z}$, a, b not both 0, we write $\text{hcf}(a, b)$ (or equivalently, $gcd(a, b)$) to denote the highest common factor (or equivalently, greatest common divisor) of a and b, meaning $\text{hcf}(a, b)$ is the largest common divisor of a and b.

(For $a, b \in \mathbb{Z}$, not both 0, let C be the set of common divisors of a and b that are positive. So

$$C = \{d \in \mathbb{Z}_+ : \ d|a \text{ and } d|b \ \}.$$

$C \neq \emptyset$ since $1 \in C$. Let M be the maximum of $|a|$ and $|b|$. Then no integer larger than M is a common divisor of a and b, so C is bounded above by M. Thus C has a maximal element, and this is $\text{hcf}(a, b)$, which is positive.)

When $\text{hcf}(a, b) = 1$, we say a, b are relatively prime.

Note that $\text{hcf}(0, 0)$ does not exist, since every integer is a divisor of 0 (for $x \in \mathbb{Z}$, $0 = x \cdot 0$ so $x|0$). For $a \in \mathbb{Z}$ with $a \neq 0$, $\text{hcf}(a, 0) = |a|$.

As an exercise, one proves the following.

Proposition 6.3. *Suppose $a, b \in \mathbb{Z}_+$ and $c = hcf(a, b)$. Take $x, y \in \mathbb{Z}$ so that $a = cx$, $b = cy$. Then $hcf(x, y) = 1$.*

Theorem 6.4. *Take $a, b \in \mathbb{Z}$ so that a, b are not both 0, and let $c = hcf(a, b)$. Then there exist $s, t \in \mathbb{Z}$ so that $c = as + bt$.*

Proof. Let d be the minimum value in the set

$$A = \{au + bv : \ (u, v \in \mathbb{Z}) \wedge (au + bv > 0) \ \}.$$

(One checks that this subset of $\mathbb{Z}$ is nonempty, and it is bounded below by 0, so it has a minimum value.) Take $s, t \in \mathbb{Z}$ so that $d = as + bt$. Note that $c|d$ since $c|a$ and $c|b$ [so $a = cx$, $b = cy$ for some $x, y \in \mathbb{Z}$, and thus $d = as + bt = c(xs + yt)$]. Hence $c \leq d$.

Take $q, r \in \mathbb{Z}$ so that $a = dq + r$ with $0 \leq r < d$. So

$$r = a - dq = a - (as + bt)q = a(1 - sq) + b(-tq).$$

If $r > 0$ then $r \in A$ with $r < d$, contrary to how we chose d. Hence we must have $r = 0$, which means $d|a$. A virtually identical argument shows that $d|b$, so d is a common divisor of a and b. As $c = \text{hcf}(a, b)$, we have $d \leq c$.

Hence $c \leq d$ and $d \leq c$, which means $c = d$. So $\text{hcf}(a, b) = c = d = as + bt$. □

Remark: Suppose $c = \text{hcf}(a, b) = as + bt$ where $a, b, s, t \in \mathbb{Z}$ with a, b not both 0. Thus $\exists a', b' \in \mathbb{Z}$ so that $a = ca'$, $b = cb'$. Then one can show that for any $k \in \mathbb{Z}$, we have $c = a(s + b'k) + b(t - a'k)$, and if $s, t \in \mathbb{Z}$ so that $as' + bt' = c$ then $s' = s + b'k$, $t' = t - a'k$ for some $k \in \mathbb{Z}$.

As an exercise, one proves the following.

Proposition 6.5. *Suppose $a, b, c \in \mathbb{Z}$ so that $c \neq 0$, $c|ab$, and $hcf(b, c) = 1$. Then $c|a$.*

Note that for $a, b \in \mathbb{Z}$, a, b not both 0, this proof shows the existence of some $s, t \in \mathbb{Z}$ so that $\text{hcf}(a, b) = as + bt$, but it does not tell us the actual values of s and t. Euclid's algorithm will produce values such values s, t; to help us prove this, we need the following, whose proof is left as an exercise.

Proposition 6.6. *Suppose $a, b, x \in \mathbb{Z}$, with a, b not both 0. Then $hcf(|a|, |b|) = hcf(a, b) = hcf(b, a + bx)$.*

Euclid's algorithm. Take $a, b \in \mathbb{Z}$ with $b \neq 0$; we will first compute $\mathrm{hcf}(a, b)$ and then we will construct $s, t \in \mathbb{Z}$ so that $\mathrm{hcf}(a, b) = as + bt$.

Step 1: Choose $q_1, r_1 \in \mathbb{Z}$ so that $a = bq_1 + r_1$ with $0 \leq r_1 \leq |b|$. If $r_1 = 0$ then we stop; otherwise we continue.

Step 2: Choose $q_2, r_2 \in \mathbb{Z}$ so that $b = r_1q_2 + r_2$ with $0 \leq r_2 < r_1$. If $r_2 = 0$ then we stop; otherwise we continue.

Step k ($k \geq 3$): Choose $q_k, r_k \in \mathbb{Z}$ so that $r_{k-2} = r_{k-1}q_k + r_k$ with $0 \leq r_k < r_{k-1}$. If $r_k = 0$ then we stop; otherwise we continue.

Notice that after k steps, we have $|b| > r_1 > r_2 > \cdots > r_k \geq 0$. Thus after at most $|b|$ steps, the algorithm must terminate.

If the algorithm terminates after 1 step, then $\mathrm{hcf}(a, b) = |b|$, and we know

$$|b| = \begin{cases} a \cdot 0 + b \cdot 1 & \text{if } b > 0, \\ a \cdot 0 + b \cdot (-1) & \text{if } b < 0. \end{cases}$$

So suppose the algorithm terminates after n steps where $n > 1$; we claim that $r_{n-1} = \mathrm{hcf}(a, b)$. To see this, first note that $r_1 = a - bq_1$, $r_2 = b - r_1q_2$, and for $3 \leq k < n$, we have $r_k = r_{k-2} - r_{k-1}q_k$. Then the preceding proposition tells us

$$\mathrm{hcf}(a, b) = \mathrm{hcf}(b, r_1) = \mathrm{hcf}(r_1, r_2) = \cdots = \mathrm{hcf}(r_{n-1}, r_n).$$

Since the algorithm terminates after n steps, this means $r_{n-1} > 0$ but $r_n = 0$; hence $\mathrm{hcf}(r_{n-1}, r_n) = \mathrm{hcf}(r_{n-1}, 0) = r_{n-1}$.

To realise r_{n-1} as $as + bt$, we substitute, using the equalities that $r_k = r_{k-2} - r_{k-1}q_k$ for $3 \leq k < n$, $r_2 = b - r_1q_2$, and $r_1 = a - bq_1$.

Example: We compute $\mathrm{hcf}(1451, 323)$ and find $s, t \in \mathbb{Z}$ so that $\mathrm{hcf}(1451, 323) = 1451s + 323t$.

Step 1: $1451 = 323 \cdot 4 + 159$ (so $q_1 = 4$, $r_1 = 159$).
Step 2: $323 = 159 \cdot 2 + 5$ (so $q_2 = 2$, $r_2 = 5$).
Step 3: $159 = 5 \cdot 31 + 4$ (so $q_3 = 31$, $r_3 = 4$).
Step 4: $5 = 4 \cdot 1 + 1$ (so $q_4 = 1$, $r_4 = 1$).
Step 5: $4 = 1 \cdot 4 + 0$ (so $q_5 = 4$, $r_5 = 0$).
Hence $\mathrm{hcf}(1451, 323) = r_4 = 1$.

Solving the above equations for r_4, r_3, r_2, r_1 gives us:

$$\begin{aligned} 1 &= 5 - 4 \cdot 1, \\ 4 &= 159 - 5 \cdot 31, \\ 5 &= 323 - 159 \cdot 2, \\ 159 &= 1451 - 323 \cdot 4. \end{aligned}$$

Thus

$$\begin{aligned} 1 &= 5 - (159 - 5 \cdot 31) \cdot 1 \\ &= 5 \cdot 32 - 159 \cdot 1 \\ &= (323 - 159 \cdot 2) \cdot 32 - 159 \cdot 1 \\ &= 323 \cdot 32 - 159 \cdot 65 \\ &= 323 \cdot 32 - (1451 - 323 \cdot 4) \cdot 65 \\ &= 323 \cdot 292 - 1451 \cdot 65. \end{aligned}$$

(So $1 = \mathrm{hcf}(1451, 323) = 1451s + 323t$ where $s = -65$, $t = 292$.)

Remark: As a later exercise, one shows that for $x, y \in \mathbb{Z}$ with $x, y \neq 0$ and $\text{hcf}(x, y) = 1$, there are infinitely many ways to choose $u, v \in \mathbb{Z}$ so that $xu + yv = 1$. Recall that with $c = \text{hcf}(a, b)$ we have $a = cx$, $b = cy$ where $x, y \in \mathbb{Z}$ with $\text{hcf}(x, y) = 1$. Consequently for any $a, b \in \mathbb{Z}$ with $a, b \neq 0$, there are infinitely many ways to choose $s, t \in \mathbb{Z}$ so that $as + bt = \text{hcf}(a, b)$.

As an application of Euclid's algorithm, we prove the following.

Theorem 6.7. *(Chinese Remainder Theorem) Suppose $m, n \in \mathbb{Z}+$ with $hcf(m, n) = 1$. For any $a, b \in \mathbb{Z}$, there is some $x \in \mathbb{Z}$ so that*

$$x \equiv a \ (mod\ m) \text{ and } x \equiv b \ (mod\ n).$$

Further, for $x' \in \mathbb{Z}$, we have $x' \equiv a \ (mod\ m)$ and $x' \equiv b \ (mod\ n)$ if and only if $x' \equiv x \ (mod\ mn)$.

Proof. Since $\text{hcf}(m, n) = 1$, there exist $s, t \in \mathbb{Z}$ so that $ms + nt = 1$. Thus

$$1 \equiv ms + nt \equiv nt \ (\text{mod } m)$$

and

$$1 \equiv ms + nt \equiv ms \ (\text{mod } n).$$

Take $x = msb + nta$. Then

$$x \equiv nta \equiv 1 \cdot a \equiv a \ (\text{mod } m)$$

and

$$x \equiv msb \equiv 1 \cdot b \equiv b \ (\text{mod } m).$$

We leave it as an exercise to show that for $x' \in \mathbb{Z}$, we have $x' \equiv a \ (\text{mod } m)$ and $x' \equiv b \ (\text{mod } n)$ if and only if $x' \equiv x \ (\text{mod } mn)$. □

Mathematical induction. Mathematical induction is a method of proof wherein we show the smallest instance of a given proposition is true, and from that deduce that each successive instance of the given proposition is true. Thus we establish a base case, or some base cases, then set up a recursive process to establish the succeeding cases.

More formally, suppose $P(n)$ is the proposition that the integer n has property P. To prove that $P(n)$ holds for all $n \in \mathbb{Z}_+$ using induction, we first prove $P(1)$ holds (this is called the base case). Then we show that for any $k \in \mathbb{Z}_+$, $P(k) \implies P(k + 1)$ (this is called the induction step); to do this, one supposes that $P(k)$ holds (called the induction hypothesis), and then argues that this implies $P(k+1)$ must hold. Hence for any $n \in \mathbb{Z}$ with $n > 1$, this second step shows that $P(1) \implies P(2)$, $P(2) \implies P(3)$, …, $P(n - 1) \implies P(n)$. Having established that $P(1)$ holds, $P(1) \implies P(2)$ shows that $P(2)$ holds; then $P(2) \implies P(3)$ shows that $P(3)$ holds; and so on. A proof using induction to show that $P(n)$ holds for all $n \in \mathbb{Z}_+$ is called a proof by induction on n.

Remarks:

(1) Proving $P(k) \implies P(k+1)$ for $k \in \mathbb{Z}_+$ does not allow us to conclude $P(n)$ holds for some $n \in \mathbb{Z}_+$ unless we have established that $P(m)$ holds for some $m \in \mathbb{Z}_+$ with $m < n$.

(2) An induction argument gives us an algorithm, which we can only apply finitely many times. Hence if $P(n)$ is a proposition that states that

the integer n has property P where we begin by showing $P(1)$ holds, the induction step $P(k) \implies P(k+1)$ does not allow us to conclude that property $P(\infty)$ holds. For example, consider the proposition $P(n)$ that says "for any subset A of $\mathbb{Z}$ with n elements, A has a maximal element"; while this proposition is true for any subset A of $\mathbb{Z}$ where A has finitely many elements, this proposition clearly does not hold for $A = \mathbb{Z}_+$. (Curious students may want to read other sources about a proof technique called "transfinite induction", which is beyond the scope of this course.)

(3) A proof by induction on n does not need to begin by establishing $P(1)$. More generally, if we establish that $P(n_0)$ holds for some (fixed) $n_0 \in \mathbb{Z}$, and that $P(k) \implies P(k+1)$ for any $k \in \mathbb{Z}$ with $k \geq n_0$, then the principle of mathematical induction allows us to conclude that $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \geq n_0$.

We now present some examples of proofs by induction.

Proposition 6.8. *For every $n \in \mathbb{Z}_+$,*

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof. For $n \in \mathbb{Z}_+$, let $P(n)$ be the proposition that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

(Base case:) We have $1 = \frac{1(1+1)}{2}$, so $P(1)$ holds.

(Induction step:) Suppose $k \geq 1$ and $P(k)$ holds; recall that $P(k)$ is the proposition that

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}.$$

[We need to deduce that $P(k+1)$ holds.] Then

$$\begin{aligned} 1 + 2 + 3 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{k^2 + 3k + 2}{2} \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

Hence $P(k+1)$ holds if $P(k)$ holds, or equivalently, $P(k) \implies P(k+1)$.

By the principle of mathematical induction, this shows that for every $n \in \mathbb{Z}_+$, $P(n)$ holds. □

Proposition 6.9. *Let X be a set, and let $A, B_1, B_2, \ldots, B_n \subseteq X$ where $n \in \mathbb{Z}_+$. Then we have the following results.*

(a) $A \cup (B_1 \cap B_2 \cap \cdots \cap B_n) = (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_n)$.
(b) $A \cap (B_1 \cup B_2 \cup \cdots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)$.
(c) *For $n \geq 2$,* $(B_1 \cap B_2 \cap \cdots \cap B_n)^c = B_1^c \cup B_2^c \cup \cdots \cup B_n^c$.
(d) *For $n \geq 2$,* $(B_1 \cup B_2 \cup \cdots \cup B_n)^c = B_1^c \cap B_2^c \cap \cdots \cap B_n^c$.

Proof. We prove (a) and leave (b), (c), (d) as exercises.

(Base case:) First note that $A \cup B_1 = A \cup B_1$.

(Induction step:) Now suppose that $k \geq 1$ and that $A \cup (B_1 \cap B_2 \cap \cdots \cap B_k) = (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_k)$. Let $C = B_1 \cap B_2 \cap \cdots \cap B_k$. Then

$$A \cup (B_1 \cap B_2 \cap \cdots \cap B_{k+1}) = A \cup (C \cap B_{k+1}).$$

By Proposition 4.3, $A \cup (C \cap B_{k+1}) = (A \cup C) \cap (A \cup B_{k+1})$. By our induction hypothesis,

$$\begin{aligned} A \cup C &= A \cup (B_1 \cap B_2 \cap \cdots \cap B_k) \\ &= (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_k). \end{aligned}$$

Hence

$$\begin{aligned} &A \cup (B_1 \cap B_2 \cap \cdots \cap B_{k+1}) \\ &= A \cup (C \cap B_{k+1}) \\ &= (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_k) \cap (A \cup B_{k+1}). \end{aligned}$$

Thus by the priniciple of mathematical induction, (a) holds for all $n \in \mathbb{Z}_+$. $\square$