Exercises from Section 1.2.1

Tord M. Johnson

May 17, 2020

1. [*05*] Explain how to modify the idea of a proof by mathematical induction, in case we want to prove some statement $P(n)$ for all *nonnegative* integers—that is, for $n = 0, 1, 2, \ldots$ instead of for $n = 1, 2, 3, \ldots$.

> We may modify the idea of a proof by mathematical induction in the case we want to prove some statement for all nonnegative integers as follows:
>
> > Let $P(n)$ be some statement about the integer n. In order to prove that $P(n)$ is true for all nonnegative integers n:
> >
> > a. Give a proof that $P(0)$ is true.
> >
> > b. Give a proof that "if all of $P(0), P(1), \ldots, P(n)$ are true, then $P(n+1)$ is also true"; this proof should be valid for any nonnegative integer n.

► **2.** [*15*] There must be something wrong with the following proof. What is it? "**Theorem.** Let a be any positive number. For all positive integers n we have $a^{n-1} = 1$. *Proof.* If $n = 1$, $a^{n-1} = a^{1-1} = a^0 = 1$. And by induction, assuming that the theorem is true for $1, 2, \ldots, n$, we have

$$a^{(n+1)-1} = a^n = \frac{a^{n-1} \times a^{n-1}}{a^{(n-1)-1}} = \frac{1 \times 1}{1} = 1;$$

so the theorem is true for $n + 1$ as well."

> The proof, in particular during the induction step, makes an assumption about $a^{(n-1)-1}$, instead of a^{n-1}, requiring the case for both $n = 1$ and $n = 2$ to be proved, which has not been done. Otherwise, if $a^{(n-1)-1} = a^{(1-1)-1} = a^{-1} = 1$, the theorem would indeed be true.

3. [*18*] The following proof by induction seems correct, but for some reason the equation for $n = 6$ gives $\frac{1}{2} + \frac{1}{6} + \frac{1}{12} + \frac{1}{20} + \frac{1}{30} = \frac{5}{6}$ on the left-hand side, and $\frac{3}{2} - \frac{1}{6} = \frac{4}{3}$ on the right-hand side. Can you find a mistake? "**Theorem.**

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

Proof. We use induction on n. For $n = 1$, clearly $3/2 - 1/n = 1/(1 \times 2)$; and, assuming that the theorem is true for n,

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

> The proof, in particular during the base step for $n = 1$, fails to prove that $\frac{3}{2} - \frac{1}{1} = \frac{1}{(1-1)\times 1}$ or that $\frac{3}{2} - \frac{1}{1} = 0$, the former which is in fact undefined.

4. [*20*] Prove that, in addition to Eq. (3), Fibonacci numbers satisfy $F_n \geq \phi^{n-2}$.

> **Proposition.** *For $\phi = \frac{1+\sqrt{5}}{2}$ and all positive integers n, Fibonacci numbers satisify $F_n \geq \phi^{n-2}$.*
>
> *Proof.* If $n = 1$, $F_n = 1 \geq \frac{2}{3} = \frac{2}{1+2} > \frac{2}{1+\sqrt{5}} = \frac{1}{\phi} = \phi^{-1} = \phi^{1-2} = \phi^{n-2}$.

Then, assuming $F_n \geq \phi^{n-2}$ for all positive integers n, we must show that $F_{n+1} \geq \phi^{(n+1)-2} = \phi^{n-1}$. If $n = 2$, $F_n = 1 \geq \phi^0 = \phi^{2-2} = \phi^{n-2}$. Otherwise, if $n > 2$:

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &\geq \phi^{n-2} + \phi^{n-3} \\ &= \frac{\phi^{n+1} + \phi^n}{\phi^3} \\ &= \phi^{n-1}(\frac{\phi+1}{\phi^2}) \\ &= \phi^{n-1}(\frac{1}{\phi} + \frac{1}{\phi^2}) \\ &> \phi^{n-1}(2) && \text{since } 1/\phi < 1 \\ &> \phi^{n-1} \end{aligned}$$

which we needed to show. □

5. [*21*] A *prime number* is an integer > 1 that has no exact divisors other than 1 and itself. Using this definition and mathematical induction, prove that every integer > 1 may be written as a product of one or more prime numbers. (A prime number is considered to be the "product" of a single prime, namely itself.)

Proposition. *Every integer $n > 1$ may be written as a product of one or more prime numbers.*

Proof. If $n = 2$, then n is prime.

Then, assuming every integer $n > 1$ may be written as a product of one or more prime numbers, we must show that $n+1$ may be as well. In the case that $n+1$ is prime, this is trivially true. Otherwise, in the case that $n + 1$ is composite, there must exist two factors p and q such that $n + 1 = pq$ where $1 < p, q < n + 1$; but by hypothesis, p and q are the products of one or more prime numbers, and so their product is such, as we needed to show. □

6. [*20*] Prove that if Eqs. (6) hold just before step E4, they hold afterwards also.

Proposition. *In **Algorithm E**, given $am + bn = d \wedge a'm + b'n = c = qd + r$ prior to step E4, afterwards we have $am + bn = d \wedge a'm + b'n = c$.*

Proof. Assume $am + bn = d \wedge a'm + b'n = c = qd + r$.

But:

$$\begin{aligned} am + bn = d \wedge a'm + b'n = c = qd + r \quad &\text{iff} \quad am + bn = d \wedge a'm + b'n = qd + r \\ &\text{iff} \quad am + bn = d \wedge a'm + b'n = q(am + bn) + r \\ &\text{iff} \quad am + bn = d \wedge a'm + b'n = qam + qbn + r \\ &\text{iff} \quad am + bn = d \wedge a'm + b'n - qam - qbn = r \\ &\text{iff} \quad am + bn = d \wedge (a' - qa)m + (b' - qb)n = r \\ &\text{iff} \quad (a' - qa)m + (b' - qb)n = r \wedge am + bn = d \end{aligned}$$

Then, given $(a' - qa)m + (b' - qb)n = r \wedge am + bn = d$, in executing step E4:

$$\begin{aligned}
c &\leftarrow d & (a' - qa)m + (b' - qb)n &= r \wedge am + bn = c \\
d &\leftarrow r & (a' - qa)m + (b' - qb)n &= d \wedge am + bn = c \\
t &\leftarrow a' & (t - qa)m + (b' - qb)n &= d \wedge am + bn = c \\
a' &\leftarrow a & (t - qa)m + (b' - qb)n &= d \wedge a'm + bn = c \\
a &\leftarrow t - qa & am + (b' - qb)n &= d \wedge a'm + bn = c \\
t &\leftarrow b' & am + (t - qb)n &= d \wedge a'm + bn = c \\
b' &\leftarrow b & am + (t - qb)n &= d \wedge a'm + b'n = c \\
b &\leftarrow t - qb & am + bn &= d \wedge a'm + b'n = c
\end{aligned}$$

as we needed to show. □

7. [*23*] Formulate and prove by induction a rule for the sums 1^2, $2^2 - 1^2$, $3^2 - 2^2 + 1^2$, $4^2 - 3^2 + 2^2 - 1^2$, $5^2 - 4^2 + 3^2 - 2^2 + 1^2$, etc.

Proposition. *Let $S_n = 1^2$ if $n = 1$ or $n^2 + (-1)S_{n-1}$ if $n > 1$ otherwise, for all positive integers n. That is, let S_n be a sum in the sequence 1^2, $2^2 - 1^2$, $3^2 - 2^2 + 1^2$, $4^2 - 3^2 + 2^2 - 1^2$, $5^2 - 4^2 + 3^2 - 2^2 + 1^2$, etc. For all positive integers n, $S_n = \sum_{1 \le k \le n} (-1)^{n-k} k^2$.*

Proof. For $n = 1$, we have $S_n = 1^2 = (-1)^0 1^2 = \sum_{1 \le k \le 1} (-1)^{1-k} k^2 = \sum_{1 \le k \le n} (-1)^{n-k} k^2$.

Then, assuming for all positive integers $n \ge 1$ if $S_n = \sum_{1 \le k \le n} (-1)^{n-k} k^2$, we must prove that $S_{n+1} = \sum_{1 \le k \le n+1} (-1)^{(n+1)-k} k^2$.

But:

$$\begin{aligned}
S_{n+1} &= (n+1)^2 + (-1)S_n \\
&= (n+1)^2 + (-1) \sum_{1 \le k \le n} (-1)^{n-k} k^2 \\
&= (n+1)^2 + \sum_{1 \le k \le n} (-1)^{(n+1)-k} k^2 \\
&= (-1)^{(n+1)-(n+1)} (n+1)^2 + \sum_{1 \le k \le n} (-1)^{(n+1)-k} k^2 \\
&= \sum_{1 \le k \le n+1} (-1)^{(n+1)-k} k^2
\end{aligned}$$

as was to be shown. □

► **8.** [*25*] (a) Prove the following theorem of Nicomachus (A.D. c. 100) by induction: $1^3 = 1$, $2^3 = 3 + 5$, $3^3 = 7 + 9 + 11$, $4^3 = 13 + 15 + 17 + 19$, etc. (b) Use this result to prove the remarkable formula $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.

[*Note:* An attractive geometric interpretation of this forumula, suggested by Warren Lushbaugh, is shown in Fig. 5; see *Math. Gazzette* **49** (1965), 200. The idea is related to Nicomachus's theorem and Fig. 3. Other "look-see" proofs can be found in books by Martin Gardner, *Knotted Doughnuts* (New York: Freeman, 1986), Chapter 16; J. H. Conway and R. K. Guy, *The Book of Numbers* (New York: Copernicus, 1996), Chapter 2.]

a. We shall prove a theorem of Nicomachus.

Proposition. *For all positive integers n, $n^3 = \sum_{1\leq k\leq n} n^2 - n + 2k - 1$.*

Proof. If $n = 1$, $n^3 = 1^3 = 1 = 1^2 - 1 + 2 - 1 = \sum_{1\leq k\leq n} n^2 - n + 2k - 1$.

Then, assuming $n^3 = \sum_{1\leq k\leq n} n^2 - n + 2k - 1$ for all positive integers n, we must show that $(n+1)^3 = \sum_{1\leq k\leq n+1}(n+1)^2 - (n+1) + 2k - 1$. But:

$$\begin{aligned}
(n+1)^3 &= n^3 + 3n^2 + 3n + 1 \\
&= 3n^2 + 3n + 1 + n^3 \\
&= 3n^2 + 3n + 1 + \sum_{1\leq k\leq n} n^2 - n + 2k - 1 \\
&= 3n^2 + 3n + 1 + n(n^2 - n) + \sum_{1\leq k\leq n} 2k - 1 \\
&= 3n^2 + 3n + 1 + n^3 - n^2 + \sum_{1\leq k\leq n} 2k - 1 \\
&= 2n^2 + 3n + 1 + n^3 + \sum_{1\leq k\leq n} 2k - 1 \\
&= n^3 + 2n^2 + 3n + 1 + \sum_{1\leq k\leq n} 2k - 1 \\
&= n^3 + 2n^2 + n + 2n + 1 + \sum_{1\leq k\leq n} 2k - 1 \\
&= (n+1)(n^2 + n) + 2n + 1 + \sum_{1\leq k\leq n} 2k - 1 \\
&= (n+1)(n^2 + 2n + 1 - n - 1) + 2n + 1 + \sum_{1\leq k\leq n} 2k - 1 \\
&= (n+1)((n+1)^2 - (n+1)) + 2(n+1) - 1 + \sum_{1\leq k\leq n} 2k - 1 \\
&= (n+1)((n+1)^2 - (n+1)) + \sum_{1\leq k\leq n+1} 2k - 1 \\
&= \sum_{1\leq k\leq n+1} (n+1)^2 - (n+1) + 2k - 1
\end{aligned}$$

as we needed to show. □

b. We shall use the proof above to prove another formula.

Proposition. *For all positive integers n, $\sum_{1\leq k\leq n} k^3 = (\sum_{1\leq k\leq n} k)^2$.*

Proof. We have that for all positive integers n, $n^3 = \sum_{1\leq k\leq n} n^2 - n + 2k - 1$.

First, we will show that $\sum_{1\leq j\leq n} \sum_{1\leq k\leq j} j^2 - j + 2k - 1 = \sum_{1\leq k\leq \frac{n^2+n}{2}} 2k - 1$.

In the case that $n = 1$:

$$\begin{aligned}
\sum_{1\le j\le n}\sum_{1\le k\le j} j^2 - j + 2k - 1 &= \sum_{1\le j\le 1}\sum_{1\le k\le j} j^2 - j + 2k - 1 \\
&= \sum_{1\le k\le 1} 1^2 - 1 + 2k - 1 \\
&= 1 \\
&= \sum_{1\le k\le 1} 2k - 1 \\
&= \sum_{1\le k\le \frac{1^2+1}{2}} 2k - 1 \\
&= \sum_{1\le k\le \frac{n^2+n}{2}} 2k - 1
\end{aligned}$$

Then, assuming that $\sum_{1\le j\le n}\sum_{1\le k\le j} j^2 - j + 2k - 1 = \sum_{1\le k\le \frac{n^2+n}{2}} 2k - 1$ for all positive integers n, we must first show that $\sum_{1\le j\le n+1}\sum_{1\le k\le j} j^2 - j + 2k - 1$ $= \sum_{1\le k\le \frac{(n+1)^2+n+1}{2}} 2k - 1$. But:

$$\begin{aligned}
\sum_{1\le j\le n+1}\sum_{1\le k\le j} j^2 - j + 2k - 1 &= (\sum_{1\le j\le n}\sum_{1\le k\le j} j^2 - j + 2k - 1) + \sum_{1\le k\le n+1} (n+1)^2 - (n+1) + 2k - 1 \\
&= (\sum_{1\le k\le \frac{n^2+n}{2}} 2k - 1) + \sum_{1\le k\le n+1} (n+1)^2 - (n+1) + 2k - 1 \\
&= (\sum_{1\le k\le \frac{n^2+n}{2}} 2k - 1) + \sum_{1\le \frac{k+1-(n+1)^2+(n+1)}{2}\le n+1} k \\
&= (\sum_{1\le k\le \frac{n^2+n}{2}} 2k - 1) + \sum_{\frac{n^2+n}{2}+1\le \frac{k+1}{2}\le \frac{(n+1)^2+(n+1)}{2}} k \\
&= (\sum_{1\le k\le \frac{n^2+n}{2}} 2k - 1) + \sum_{\frac{n^2+n}{2}+1\le k\le \frac{(n+1)^2+(n+1)}{2}} 2k - 1 \\
&= (\sum_{1\le k\le \frac{(n+1)^2+(n+1)}{2}} 2k - 1)
\end{aligned}$$

as was to be shown.

Second, and finally, we note that:

$$\begin{aligned}
\sum_{1\le k\le n} k^3 &= \sum_{1\le j\le n}\sum_{1\le k\le j} j^2 - j + 2k - 1 \\
&= \sum_{1\le k\le \frac{n^2+n}{2}} 2k - 1 \\
&= (\frac{n^2+n}{2})^2 && \text{the sum of } \frac{n^2+n}{2} \text{ odd integers} \\
&= (\frac{n(n+1)}{2})^2 \\
&= (\sum_{1\le k\le n} k)^2
\end{aligned}$$

as we needed to show. □

9. [*20*] Prove by induction that if $0 < a < 1$, then $(1-a)^n \ge 1 - na$.

Proposition. *For all positive integers n, if $0 < a < 1$, then $(1-a)^n \geq 1 - na$.*

Proof. If $n = 1$, then $(1-a)^n = (1-a)^1 = 1 - a = 1 - (1)a = 1 - na$.

Then, assuming that $(1-a)^n \geq 1 - na$ for all positive integers n, we must show that $(1-a)^{n+1} \geq 1 - (n+1)a$. But:

$$\begin{aligned}(1-a)^{n+1} &= (1-a)(1-a)^n \\ &\geq (1-a)(a-na) \\ &= 1 - na - a + na^2 \\ &\geq 1 - na - a \\ &= 1 - (n+1)a\end{aligned}$$

as we needed to show. □

10. [*M22*] Prove by induction that if $n \geq 10$, then $2^n > n^3$.

Proposition. *For all integers $n \geq 10$, $2^n > n^3$.*

Proof. If $n = 10$, then $2^n = 2^{10} = 1024 > 1000 = 10^3 = n^3$.

Also note that if $n \geq 10$, then $(1 + \frac{1}{n})^3 \leq (1 + \frac{1}{10})^3 < 2$.

Then, assuming $2^n > n^3$ for all integers $n \geq 10$, we must show that $2^{n+1} > (n+1)^3$. But:

$$\begin{aligned}2^{n+1} &= (2)2^n \\ &> (2)n^3 \\ &> (1 + \frac{1}{n})^3 n^3 \\ &= (n+1)^3\end{aligned}$$

as we needed to show. □

11. [*M30*] Find and prove a simple formula for the sum

$$\frac{1^3}{1^4+4} - \frac{3^3}{3^4+4} + \frac{5^3}{5^4+4} - \cdots + \frac{(-1)^n(2n+1)^3}{(2n+1)^4+4}.$$

When we enumerate the first five terms and cumulative sums of the sequence $S_n = \frac{(-1)^{n-1}(2n-1)^3}{(2n-1)^4+4}$:

n	S_n	$\sum_{1 \leq k \leq n} S_k$
1	1/5	1/5
2	-27/85	-2/17
3	125/629	3/37
4	-343/2405	-4/65
5	729/6565	5/101

we conjecture that $\sum_{1 \leq k \leq n} \frac{(-1)^{k-1}(2k-1)^3}{(2k-1)^4+4} = \frac{(-1)^{n-1}n}{4n^2+1}$.

Proposition. *For all positive integers n, $\sum_{1 \leq k \leq n} \frac{(-1)^{k-1}(2k-1)^3}{(2k-1)^4+4} = \frac{(-1)^{n-1}n}{4n^2+1}$.*

Proof. If $n = 1$, $\sum_{1 \leq k \leq n} \frac{(-1)^{k-1}(2k-1)^3}{(2k-1)^4+4} = \frac{(-1)^0(2-1)^3}{(2-1)^4+4} = \frac{1}{5} = \frac{(-1)^0(1)}{4(1)^2+1} = \frac{(-1)^{n-1}n}{4n^2+1}$.

Then, assuming $\sum_{1\le k\le n}\frac{(-1)^{k-1}(2k-1)^3}{(2k-1)^4+4}=\frac{(-1)^{n-1}n}{4n^2+1}$ for all positive integers n, we must show that $\sum_{1\le k\le n+1}\frac{(-1)^{k-1}(2k-1)^3}{(2k-1)^4+4}=\frac{(-1)^n(n+1)}{4(n+1)^2+1}$. But:

$$\begin{aligned}\sum_{1\le k\le n+1}\frac{(-1)^{k-1}(2k-1)^3}{(2k-1)^4+4}&=\Big(\sum_{1\le k\le n}\frac{(-1)^{k-1}(2k-1)^3}{(2k-1)^4+4}\Big)+\frac{(-1)^n(2(n+1)-1)^3}{(2(n+1)-1)^4+4}\\&=\frac{(-1)^{n-1}n}{4n^2+1}+\frac{(-1)^n(2(n+1)-1)^3}{(2(n+1)-1)^4+4}\\&=\frac{(-1)^{n-1}n((2n+1)^4+4)+(-1)^n(2n+1)^3(4n^2+1)}{(4n^2+1)((2n+1)^4+4)}\\&=\frac{(-1)^{n-1}n((2n+1)^4+4)+(-1)^n(2n+1)^3(4n^2+1)}{(4(n+1)^2+1)(4n^2+1)^2}\\&=\frac{(-1)^n-n((2n+1)^4+4)+(-1)^n(2n+1)^3(4n^2+1)}{(4(n+1)^2+1)(4n^2+1)^2}\\&=\frac{(-1)^n(-n((2n+1)^4+4)+(2n+1)^3(4n^2+1))}{(4(n+1)^2+1)(4n^2+1)^2}\\&=\frac{(-1)^n(n+1)(4n^2+1)^2}{(4(n+1)^2+1)(4n^2+1)^2}\\&=\frac{(-1)^n(n+1)}{4(n+1)^2+1}\end{aligned}$$

as we needed to show. □

12. [*M25*] Show how Algorithm E can be generalized as stated in the text so that it will accept input values of the form $u+v\sqrt{2}$, where u and v are integers, and the computations can still be done in an elementary way (that is, without using the infinite decimal expansion of $\sqrt{2}$). Prove that the computation will not terminate, however, if $m=1$ and $n=\sqrt{2}$.

Algorithm E can be generalized to accept input values of the form $u+v\sqrt{2}$ for integers u and v, using repeated subtraction instead of division. The algorithm relies on the fact that $u+v\sqrt{2}=u'+v'\sqrt{2}\iff u'-u=0\wedge v'-v=0$, our test for a zero remainder; and on the fact that $(u-u')+(v-v')\sqrt{2}<0\iff(u-u')+\lfloor(v-')\sqrt{2}\rfloor<0$.

Algorithm F (*Generalized Euclid's algorithm*). Given two numbers $m=m_r+m_i\sqrt{2}$ and $n=n_r+n_i\sqrt{2}$ with integers m_r,m_i,n_r,n_i, we compute their greatest common divisor $d=d_r+d_i\sqrt{2}$ with integers d_r,d_i, and we also compute two integers a and b such that $am+bn=d$.

F1a. [Initialize.] Set $a'\leftarrow b\leftarrow 1$, $a\leftarrow b'\leftarrow 0$, $(c_r,c_i)\leftarrow(m_r,m_i)$, $(d_r,d_i)\leftarrow(n_r,n_i)$, $y\leftarrow z\leftarrow 1$.

F1b1. [Initialize $c=|m|$.] Set $v\leftarrow 0$.

F1b2. If $(v+1)^2\le 2c_i^2$, $v\leftarrow v+1$, and go to step F1b2. Otherwise, if $c_i<0$, $v\leftarrow-(v+1)$. (Afterwards, we have $v=\lfloor c_i\sqrt{2}\rfloor$.)

F1b3. If $c_r+v<0$, $y\leftarrow-1$, $(c_r,c_i)\leftarrow(-c_r,-c_i)$.

F1c1. [Initialize $d=|n|$.] Set $v\leftarrow 0$.

F1c2. If $(v+1)^2\le 2d_i^2$, $v\leftarrow v+1$, and go to step F1c2. Otherwise, if $d_i<0$, $v\leftarrow-(v+1)$. (Afterwards, we have $v=\lfloor d_i\sqrt{2}\rfloor$.)

F1c3. If $d_r+v<0$, $z\leftarrow-1$, $(d_r,d_i)\leftarrow(-d_r,-d_i)$.

F2a. [Divide.] Let $q\leftarrow 0$, $(e_r,e_i)\leftarrow(c_r,c_i)$.

F2b1. Let $(e_r,e_i)\leftarrow(e_r-d_r,e_i-d_i)$ and $v\leftarrow 0$.

F2b2. If $(v+1)^2\le 2e_i^2$, $v\leftarrow v+1$ and go to step F2b2. Otherwise, if $e_i<0$, $v\leftarrow-(v+1)$. (Afterwards, we have $v=\lfloor e_i\sqrt{2}\rfloor$.)

F2c. If $e_r + v \geq$, $q \leftarrow q + 1$ and go to step F2b1.

F2d. Let $(r_r, r_i) \leftarrow (c_r - qd_r, c_i - qd_i)$. (We have $c_r + c_i\sqrt{2} = qd + r_r + r_i\sqrt{2}$ and $0 \leq r_r + r_i\sqrt{2} < d$.)

F3. [Remainder zero?] If $(r_r, r_i) = (0, 0)$, let $a \leftarrow ya$, $b \leftarrow zb$ and the algorithm terminates; we have in this case $am + bn = d$ as desired.

F4. [Recycle.] Set $(c_r, c_i) \leftarrow (d_r, d_i)$, $(d_r, d_i) \leftarrow (r_r, r_i)$, $t \leftarrow a', a' \leftarrow a, a \leftarrow t - qa$, $t \leftarrow b', b' \leftarrow b, b \leftarrow t - qb$, and go back to F2a.

■

Unfortunately, Algorithm F will not terminate given inputs $m = 1, n = \sqrt{2}$. If it did terminate, we would have $r_r + r_i\sqrt{2} = 0 = c_r + c_i\sqrt{2} - q(d_r + d_i\sqrt{2}) = (c_r - qd_r) + (c_i - qd_i\sqrt{2})$, or equivalently, $\sqrt{2} = \frac{qd_r - c_r}{c_i - qd_i}$; that is, we would find $\sqrt{2}$ to be rational, which cannot be. We can be assured that $c_i \neq qd_i$ in this case, since $1 \neq q\sqrt{2}$ for any rational q. Hence, the algorithm will not terminate.

Note: ... For further information, see "quadratic Euclidean domains" in number theory textbooks.

▶ **13.** [*M23*] Extend Algorithm E by adding a new variable T and adding the operation "$T \leftarrow T + 1$" at the beginning of each step. (Thus, T is like a clock, counting the number of steps executed.) Assume that T is initially zero, so that assertion $A1$ in Fig. 4 becomes "$m > 0$, $n > 0$, $T = 0$." The additional condition "$T = 1$" should similarly be appended to $A2$. Show how to append additional conditions to the assertions in such a way that any one of $A1, A2, \ldots, A6$ implies $T \leq 3n$, and such that the inductive proof can still be carried out. (Hence the computation must terminate in at most $3n$ steps.)

Initially, we are given the following algorithm with various assertions.

Algorithm E (*Extended Euclid's algorithm*). Given two positive integers m and n, we compute their greatest common divisor d, and we also compute two not-necessarily-positive integers a and b such that $am + bn = d$.

A1. [Precondition.] $m > 0$, $n > 0$.

E1. [Initialize.] Set $a' \leftarrow b \leftarrow 1$, $a \leftarrow b' \leftarrow 0$, $c \leftarrow m$, $d \leftarrow n$.

A2. [E1 postcondition.] $c = m > 0$, $d = n > 0$, $a = b' = 0$, $a' = b = 1$.

A6. [E4 postcondition.] $am + bn = d$, $a'm + b'n = c$, $d > 0$, $\gcd(c, d) = \gcd(m, n)$.

E2. [Divide.] Let q and r be the quotient and remainder, respectively, of c divided by d. (We have $c = qd + r$ and $0 \leq r < d$.)

A3. [E2 postcondition.] $am + bn = d$, $a'm + b'n = c = qd + r$, $0 \leq r < d$, $\gcd(c, d) = \gcd(m, n)$.

E3. [Remainder zero?] If $r = 0$, the algorithm terminates; we have in this case $am + bn = d$ as desired.

A4. [E3 postcondition, $r = 0$.] $am + bn = d = \gcd(m, n)$.

A5. [E3 postcondition, $r \neq 0$.] $am + bn = d$, $a'm + b'n = c = qd + r$, $0 < r < d$, $\gcd(c, d) = \gcd(m, n)$.

E4. [Recycle.] Set $c \leftarrow d$, $d \leftarrow r$, $t \leftarrow a'$, $a' \leftarrow a$, $a \leftarrow t - qa$, $t \leftarrow b'$, $b' \leftarrow b$, $b \leftarrow t - qb$, and go back to E2.

■

We can augment this with a step variable T to show that $T \leq 3n$.

Algorithm G (*Extended Euclid's algorithm with steps*). Given two positive integers m and n, we compute their greatest common divisor d, and we also compute two not-necessarily-positive integers a and b such that $am + bn = d$, as well as steps T to show that $T \leq 3n$.

G0. [Initialze steps.] $T \leftarrow 0$.

B1. [Precondition, G0 postcondition.] $m > 0$, $n > 0$, $T = 0$.

G1. [Initialize.] Set $a' \leftarrow b \leftarrow 1$, $a \leftarrow b' \leftarrow 0$, $c \leftarrow m$, $d \leftarrow n$, $T \leftarrow T + 1$.

B2. [G1 postcondition.] $c = m > 0$, $d = n > 0$, $a = b' = 0$, $a' = b = 1$, $T = 1$.

B6. [G4 postcondition.] $am + bn = d$, $a'm + b'n = c$, $d > 0$, $\gcd(c, d) = \gcd(m, n)$, $T \leq 3(n - d) + 1$.

G2. [Divide.] Let q and r be the quotient and remainder, respectively, of c divided by d. Also set $T \leftarrow T + 1$. (We have $c = qd + r$ and $0 \leq r < d$.)

B3. [G2 postcondition.] $am+bn = d$, $a'm+b'n = c = qd+r$, $0 \leq r < d$, $\gcd(c, d) = \gcd(m, n)$, $T \leq 3(n - d) + 2$.

G3. [Remainder zero?] Set $T \leftarrow T + 1$. If $r = 0$, the algorithm terminates; we have in this case $am + bn = d$ and $T \leq 3n$ as desired.

B4. [G3 postcondition, $r = 0$.] $am + bn = d = \gcd(m, n)$, $d > 0$, $T \leq 3(n - d) + 3$.

B5. [G3 postcondition, $r \neq 0$.] $am + bn = d$, $a'm + b'n = c = qd + r$, $0 < r < d$, $\gcd(c, d) = \gcd(m, n)$, $d > 0$, $T \leq 3(n - d) + 3$.

G4. [Recycle.] Set $c \leftarrow d$, $d \leftarrow r$, $t \leftarrow a'$, $a' \leftarrow a$, $a \leftarrow t - qa$, $t \leftarrow b'$, $b' \leftarrow b$, $b \leftarrow t - qb$, $T \leftarrow T + 1$, and go back to G2.

■

The new assertions may be derived as shown below, given $n > 0$.

Summary		Precondition	Step		Postcondition
$\{\}$ **G0** $\{B1\}$		$\{\}$	$T \leftarrow 0$		$\{T = 0\}$
$\{B1\}$ **G1** $\{B2\}$		$\{T = 0\}$			
	$\Longrightarrow$	$\{T + 1 = 1\}$	$T \leftarrow T + 1$		$\{T = 1\}$
$\{B2\}$ **G2** $\{B3\}$		$\{n = d \wedge T = 1\}$			
	$\Longrightarrow$	$\{T \leq 3(n - d) + 1\}$			
	$\Longrightarrow$	$\{T + 1 \leq 3(n - d) + 2\}$	$T \leftarrow T + 1$		$\{T \leq 3(n - d) + 2\}$
$\{B3\}$ **G3** $\{B4\}$		$\{d > 0 \wedge T \leq 3(n - d) + 2\}$			
	$\Longrightarrow$	$\{d > 0 \wedge T + 1 \leq 3(n - d) + 3\}$	$T \leftarrow T + 1$		$\{d > 0 \wedge T \leq 3(n - d) + 3\}$
				$\Longrightarrow$	$\{T \leq 3n\}$
$\{B3\}$ **G3** $\{B5\}$		$\{d > 0 \wedge T \leq 3(n - d) + 2\}$			
	$\Longrightarrow$	$\{d > 0 \wedge T + 1 \leq 3(n - d) + 3\}$	$T \leftarrow T + 1$		$\{d > 0 \wedge T \leq 3(n - d) + 3\}$
$\{B5\}$ **G4** $\{B6\}$		$\{d > 0 \wedge T \leq 3(n - d) + 3\}$			
	$\Longrightarrow$	$\{T \leq 3(n - d)\}$			
	$\Longrightarrow$	$\{T + 1 \leq 3(n - d) + 1\}$	$T \leftarrow T + 1$		$\{T \leq 3(n - d) + 1\}$
$\{B6\}$ **G2** $\{B3\}$		$\{T \leq 3(n - d) + 1\}$			
	$\Longrightarrow$	$\{T + 1 \leq 3(n - d) + 2\}$	$T \leftarrow T + 1$		$\{T \leq 3(n - d) + 2\}$

14. [*50*] (R. W. Floyd.) Prepare a computer program that accepts, as input, programs in some programming language together with optional assertions, and that attempts to fill in the remaining assertions necessary to make a proof that the computer program is valid. (For example, strive to get a program that is able to prove the validity of Algorithm E, given only assertions $A1$, $A4$, and $A6$. See the papers by R. W. Floyd and J. C. King in the IFIP Congress proceedings, 1971, for further discussion.)

n.a.

▶ **15.** [*HM28*] (*Generalized induction.*) The text shows how to prove statements $P(n)$ that depend on a single integer n, but it does not describe how to prove statements $P(m, n)$ depending on two integers. In these circumstances a proof is often given by some sort of "double induction," which frequently seems confusing. Actually, there is an important principle more general than simple induction that applies not only to this case but also to situations in which statements are to be proved about uncoutnable sets—for example, $P(x)$ for all real x. This general principle is called *well-ordering*.

Let "$\prec$" be a relation on a set S, satisifying the following properties:

i. Given x, y, and z in S, if $x \prec y$ and $y \prec z$, then $x \prec z$.

ii. Given x and y in S, exactly one of the following three possibilities is true: $x \prec y$, $x = y$, or $y \prec x$.

iii. If A is any nonempty subset of S, there is an element x in A with $x \preceq y$ (that is, $x \prec y$ or $x = y$) for all y in A.

This relation is said to be a well-ordering of S. For example, it is clear that the positive integers are well-ordered by the ordinary "less than" relation, $<$.

a. Show that the set of *all* integers is not well-ordered by $<$.

b. Define a well-ordering relation on the set of all integers.

c. Is the set of all nonnegative real numbers well-ordered by $<$?

d. (*Lexicographic order.*) Let S be well-ordered by $\prec$, and for $n > 0$ let T_n be the set of all n-tuples $(x_1, x_2, \ldots, x_n)$ of elements x_j in S. Define $(x_1, x_2, \ldots, x_n) \prec (y_1, y_2, \ldots, y_n)$ if there is some k, $1 \le k \le n$, such that $x_j = y_j$ for $1 \le j < k$, but $x_k \prec y_k$ in S. Is $\prec$ a well-ordering of T_n?

e. Continuing part (d), let $T = \bigcup_{n \ge 1} T_n$; define $(x_1, x_2, \ldots, x_m) \prec (y_1, y_2, \ldots, y_n)$ if $x_j = y_j$ for $1 \le j < k$ and $x_k \prec y_k$, for some $k \le \min(m, n)$, or if $m < n$ and $x_j = y_j$ for $1 \le j \le m$. Is $\prec$ a well-ordering of T?

f. Show that $\prec$ is a well-ordering of S if and only if it satisifies (i) and (ii) above and there is no infinite sequence $x_1, x_2, x_3, \ldots$ with $x_{j+1} \prec x_j$ for all $j \ge 1$.

g. Let S be well-ordered by $\prec$, and let $P(x)$ be a statement about the element x of S. Show that if $P(x)$ can be proved under the assumption that $P(y)$ is true for all $y \prec x$, then $P(x)$ is true for *all* x in S.

[*Notes:* Part (g) is the generalization of simple induction that was promised; in the case $S =$ positive integers, it is just the simple case of mathematical induction treated in the text. In that case we are asked to prove that $P(1)$ is true if $P(y)$ is true for all positive integers $y < 1$; this is the same as saying we should prove $P(1)$, since $P(y)$ certainly is (vacuously) true for all such y. Consequently, one finds that in many situations $P(1)$ need not be proved using a special argument.

Part (d), in connection with part (g), gives us a powerful method of n-tuple induction for proving statements $P(m_1, \ldots, m_n)$ about n positive integers $m_1, \ldots, m_n$.

Part (f) has further application to computer algorithms: If we can map each state x of a computation into an element $f(x)$ belonging to a well-ordered set S, in such a way that every step of the computation takes a state x intoa state y with $f(y) \prec f(x)$, then the algorithm must terminate. This principle generalizes the argument about strictly decreasing values of n, by which we proved the termination of Algorithm 1.1E.]

Answers are enumerated below.

a. We can show that the set of *all* integers is not well-ordered by $<$ by considering the violation of condition (iii) with the nonempty (improper) subset $\mathbb{Z}$, which has no least element.

b. We may define a well-ordering relation on the set of all integers as

$$x \prec y = \begin{cases} |x| = |y| & \text{if } -x = y > 0 \\ |x| < |y| & \text{otherwise} \end{cases} \tag{12}$$

To see that $\prec$ satisifes condition (i), assume $x \prec y$ and $y \prec z$. We must show that $x \prec z$. By hypothesis, $-x = y > 0 \vee |x| < |y|$ and $-y = z > 0 \vee |y| < |z|$.

Case I. [$-x = y > 0$ and $-y = z > 0$.] This case is impossible, as it requires both $y > 0$ and $y < 0$, and so need not be considered.

Case II. [$-x = y > 0$ and $|y| < |z|$.] In this case, since $-x = y > 0$, we have $|y| = y = -x = |x|$. But $|y| = |x| < |z|$ and so $x \prec z$ as we needed to show in this case.

Case III. [$|x| < |y|$ and $-y = z > 0$.] In this case, since $-y = z > 0$, we have $|y| = -y = z = |z|$. But $|x| < |y| = |z|$ and so $x \prec z$ as we needed to show in this

case.

Case IV. [$|x| < |y|$ and $|y| < |z|$.] In this case, clearly, as $<$ is transitive, $|x| < |z|$, and so $x \prec z$ as we needed to show in this case.

To see that $\prec$ satisifies condition (ii) we must show that for arbitrary x and y, $x \prec y$, $x = y$, or $y \prec x$. If $x = y$, $-x \neq y$, $|x| \not< |y|$, and $|y| \not< |x|$; if $-x = y > 0$, then $|x| = |y|$ and $x \prec y$; if $-y = x > 0$, then $|y| = |x|$ and $y \prec x$; otherwise, either $|x| < |y|$ or $|y| < |x|$ in which case $x \prec y$ or $y \prec x$, respectively.

To see that $\prec$ satisifies condition (iii), we must show that any nonempty subset of $\mathbb{Z}$ has a least element under $\prec$. Let S be such a subset, so that $S \neq \varnothing$ and let $T = \{t \in \mathbb{Z} | (\forall s \in S)(t \prec s)\}$. We must show that S has a least element. In the case that $0 \in S$, clearly 0 is such an element. Otherwise, in the case that $0 \notin S$, $T \neq \varnothing$, and there must exist an element $u \in T$ such that $u + 1 \notin T$ but $u + 1 \in S$. Clearly, $u + 1$ is the least element under $\prec$ in S, as we needed to show.

c. The set of all nonnegative real numbers is not well-ordered by $<$, as condition (iii) is violated with the nonempty subset of positive reals, which has no least nonnegative real number.

d. *Lexicographic order* is a well-ordering of T_n for $n > 0$.

To see that $\prec$ satisfies condition (i), assume $(x_1, x_2, \ldots, x_n) \prec (y_1, y_2, \ldots, y_n)$ and $(y_1, y_2, \ldots, y_n) \prec (z_1, z_2, \ldots, z_n)$. We must show that $(x_1, x_2, \ldots, x_n) \prec (z_1, z_2, \ldots, z_n)$. For $n = 1$, we have $(x_1) \prec (y_1)$ and $(y_1) \prec (z_1)$. Since S is well-ordered by $\prec$, $\prec$ is transitive, and so $(x_1) \prec (z_1)$. Then, assuming $(x_1, x_2, \ldots, x_k) \prec (y_1, y_2, \ldots, y_k) \wedge (y_1, y_2, \ldots, y_k) \prec (z_1, z_2, \ldots, z_k) \Longrightarrow (x_1, x_2, \ldots, x_k) \prec (z_1, z_2, \ldots, z_k)$ for some $k \geq 1$, we must show that $(x_1, x_2, \ldots, x_{k+1}) \prec (y_1, y_2, \ldots, y_{k+1}) \wedge (y_1, y_2, \ldots, y_{k+1}) \prec (z_1, z_2, \ldots, z_{k+1}) \Longrightarrow (x_1, x_2, \ldots, x_{k+1}) \prec (z_1, z_2, \ldots, z_{k+1})$. But since S is well-ordered by $\prec$ and therefore transitive, $(x_{k+1}) \prec (y_{k+1}) \wedge (y_{k+1}) \prec (z_{k+1}) \Longrightarrow (x_{k+1}) \prec (z_{k+1})$; clearly then, with our induction hypothesis, $(x_1, x_2, \ldots, x_{k+1}) \prec (z_1, z_2, \ldots, z_{k+1})$.

To see that $\prec$ satisifies condition (ii) we must show for arbitrary n that $(x_1, x_2, \ldots, x_n) \prec (y_1, y_2, \ldots, y_n)$, $(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n)$, or $(y_1, y_2, \ldots, y_n) \prec (x_1, x_2, \ldots, x_n)$. Clearly the condition is satisfied for $n = 1$ since S is well-ordered. Then, assuming $(x_1, x_2, \ldots, x_k) \prec (y_1, y_2, \ldots, y_k)$, $(x_1, x_2, \ldots, x_k) = (y_1, y_2, \ldots, y_k)$, or $(y_1, y_2, \ldots, y_k) \prec (x_1, x_2, \ldots, x_k)$ for some $k \geq 1$; we must show that $(x_1, x_2, \ldots, x_{k+1}) \prec (y_1, y_2, \ldots, y_{k+1})$, $(x_1, x_2, \ldots, x_{k+1}) = (y_1, y_2, \ldots, y_{k+1})$, or $(y_1, y_2, \ldots, y_{k+1}) \prec (x_1, x_2, \ldots, x_{k+1})$.

Case I. [$(x_1, x_2, \ldots, x_k) \prec (y_1, y_2, \ldots, y_k)$ and $(x_{k+1}) \prec (y_{k+1})$.] Clearly $(x_1, x_2, \ldots, x_{k+1}) \prec (y_1, y_2, \ldots, y_{k+1})$.

Case II. [$(x_1, x_2, \ldots, x_k) = (y_1, y_2, \ldots, y_k)$ and $(x_{k+1}) \prec (y_{k+1})$.] $(x_1, x_2, \ldots, x_{k+1}) \prec (y_1, y_2, \ldots, y_{k+1})$ by definition.

Case III. [$(y_1, y_2, \ldots, y_k) \prec (x_1, x_2, \ldots, x_k)$ and $(x_{k+1}) \prec (y_{k+1})$.] In this case, we have $(y_1, y_2, \ldots, y_{k+1}) \prec (x_1, x_2, \ldots, x_{k+1})$.

Case IV. [$(x_1, x_2, \ldots, x_k) \prec (y_1, y_2, \ldots, y_k)$ and $(x_{k+1}) = (y_{k+1})$.] In this case, we have $(x_1, x_2, \ldots, x_{k+1}) \prec (y_1, y_2, \ldots, y_{k+1})$.

Case V. [$(x_1, x_2, \ldots, x_k) = (y_1, y_2, \ldots, y_k)$ and $(x_{k+1}) = (y_{k+1})$.] In this case, we have $(x_1, x_2, \ldots, x_{k+1}) = (y_1, y_2, \ldots, y_{k+1})$.

Case VI. [$(y_1, y_2, \ldots, y_k) \prec (x_1, x_2, \ldots, x_k)$ and $(y_{k+1}) = (x_{k+1})$.] In this case, we have $(y_1, y_2, \ldots, y_{k+1}) \prec (x_1, x_2, \ldots, x_{k+1})$.

Case VII. [$(x_1, x_2, \ldots, x_k) \prec (y_1, y_2, \ldots, y_k)$ and $(y_{k+1}) \prec (x_{k+1})$.] In this case, we have $(x_1, x_2, \ldots, x_{k+1}) \prec (y_1, y_2, \ldots, y_{k+1})$.

Case VIII. [$(x_1, x_2, \ldots, x_k) = (y_1, y_2, \ldots, y_k)$ and $(y_{k+1}) \prec (x_{k+1})$.] In this case, we have $(y_1, y_2, \ldots, y_{k+1}) \prec (x_1, x_2, \ldots, x_{k+1})$.

Case IX. $[(y_1, y_2, \ldots, y_k) \prec (x_1, x_2, \ldots, x_k)$ and $(y_{k+1}) \prec (x_{k+1}).]$ In this case, we have $(y_1, y_2, \ldots, y_{k+1}) \prec (x_1, x_2, \ldots, x_{k+1})$.

To see that $\prec$ satisfies condition (iii) we must show that for arbitrary n, T_n has a least element under $\prec$. For $n = 1$, clearly this is true as S is well-ordered under $\prec$. Then, assuming T_k has a least element, we must show that so does T_{k+1}. But if both T_k and S have least elements, $(t_1, t_2, \ldots, t_k)$ and (s_1) respectively, then clearly T_{k+1} does too; namely, $(t_1, t_2, \ldots, t_k, s_1)$.

e. Continuing part (d), if we let $T = \bigcup_{n \geq 1} T_n$ and define $(x_1, x_2, \ldots, x_m) \prec (y_1, y_2, \ldots, y_n)$ if $x_j = y_j$ for $1 \leq j < k$ and $x_k \prec y_k$, for some $k \leq \min(m, n)$, or if $m < n$ and $x_j = y_j$ for $1 \leq j \leq m$; then $\prec$ is not a well-ordering of T, as condition (ii) can be violated. Consider $\{a, b\}$ with $a \prec b$. Then, $(b) \not\prec (a, b)$, $(b) \neq (a, b)$, and $(a, b) \not\prec (b)$.

f. We need to show that $\prec$ is a well-ordering of S if and only if it satisifies conditions (i) and (ii) and there is no infinite sequence $x_1, x_2, x_3, \ldots$ with $x_{j+1} \prec x_j$ for all $j \geq 1$. That is, we must show the equivalence of condition (iii), that S has a least element, and the nonexistence of an infinite descending sequence x_j such that $x_{j+1} \prec x_j$ for all $j \geq 1$. If S has a least element, then clearly, there is an $s \in S$ such that for any $x \in S$, $x \not\prec s$ unless $s = x$. Conversely, if no such sequence exists, there is some s such that $x \not\prec s$ for all $x \in S$, and this s is precisely the least element of S.

g. Let S be well-ordered by $\prec$, and let $P(x)$ be a statement about the element x of S. We must show that if $P(x)$ can be proved under the assumption that $P(y)$ is true for all $y \prec x$, then $P(x)$ is true for *all* x in S.

Suppose not. That is, suppose there is some p such that $P(p)$ does not hold, despite the fact that for all $y \prec x$, $P(y) \Longrightarrow P(x)$. If $P(y)$ holds for all $y \prec p$, then by hypothesis, $P(p)$ holds. This is a condraction. Hence, $P(x)$ holds for all $x \in S$.