Preliminary Chapter on Induction

0.1. Fibonacci numbers and other recurrence sequences

Exercise 0.1.1. (a) Use the recurrence relation for the Fibonacci numbers, and induction to prove that every Fibonacci number is an integer.
(b) Prove that (0.1.1) is correct by verifying that it holds for $n = 0, 1$ and then, for all larger integers n, by induction.

Exercise 0.1.2. Use induction on $n \geq 1$ to prove that
(a) $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$ and
(b) $1 + F_2 + F_4 + \cdots + F_{2n} = F_{2n+1}$.

Exercise 0.1.3. (a) Prove that ϕ satisfies $\phi^2 = \phi + 1$.
(b) Prove that $\phi^n = F_n\phi + F_{n-1}$ for all integers $n \geq 1$, by induction.

Exercise 0.1.4. (a) Prove (0.1.3) is correct by verifying that it holds for $n = 0, 1$ (with x_0 and x_1 as in the last displayed equation) and then by induction for $n \geq 2$.
(b) Show that c_α and c_β are uniquely determined by x_0 and x_1, provided $\alpha \neq \beta$.
(c) Show that if $\alpha \neq \beta$ with $x_0 = 0$ and $x_1 = 1$, then $x_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ for all integers $n \geq 0$.
(d) Show that if $\alpha \neq \beta$ with $y_0 = 2, y_1 = a$ with $y_n = ay_{n-1} + by_{n-2}$ for all $n \geq 2$, then $y_n = \alpha^n + \beta^n$ for all integers $n \geq 0$.

The $\{x_n\}_{n\geq 0}$ in (c) is a *Lucas sequence*, and the $\{y_n\}_{n\geq 0}$ in (d) its *companion sequence*

Exercise 0.1.5.[1] (a) Prove that $\alpha = \beta$ if and only if $a^2 + 4b = 0$.
(b)† Show that if $a^2 + 4b = 0$, then $\alpha = a/2$ and $x_n = (cn + d)\alpha^n$ for all integers $n \geq 0$, for some constants c and d.
(c) Deduce that if $\alpha = \beta$ with $x_0 = 0$ and $x_1 = 1$, then $x_n = n\alpha^{n-1}$ for all $n \geq 0$.

Exercise 0.1.6. Prove that if $x_0 = 0$ and $x_1 = 1$, if (0.1.2) holds, and if α is a root of $x^2 - ax - b$, then $\alpha^n = \alpha x_n + bx_{n-1}$ for all $n \geq 1$.

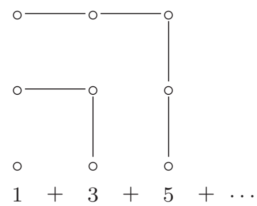
[1] In this question, and from here on, induction should be used at the reader's discretion.

0.2. Formulas for sums of powers of integers

Exercise 0.2.1. (a) Prove that $1+3+5+\cdots+(2N-1)=N^2$ for all $N\geq 1$ by induction.

(b) Prove the formula in part (a) by the young Gauss's method.

(c) Start with a single dot, thought of as a 1-by-1 array of dots, and extend it to a 2-by-2 array of dots by adding an appropriate row and column. You have added 3 dots to the original dot and so $1+3=2^2$.



In general, draw an N-by-N array of dots, and add an additional row and column of dots to obtain an $(N+1)$-by-$(N+1)$ array of dots. By determining how many dots were added to the number of dots that were already in the array, deduce the formula in (a).

Exercise 0.2.2. Prove these last two formulas by induction.

0.3. The binomial theorem, Pascal's triangle, and the binomial coefficients

Exercise 0.3.1. (a) Prove that $\binom{n+1}{m}=\binom{n}{m}+\binom{n}{m-1}$ for all integers m, and all integers $n\geq 0$.

(b) Deduce from (a) that each $\binom{n}{m}$ is an integer.

Exercise 0.3.2.† Using exercise 0.3.1(a) and induction on $n\geq 1$, prove the binomial theorem.

Exercise 0.3.3. Prove (0.3.2) for each fixed $k\geq 1$, for each $N\geq k+1$, using induction and exercise 0.3.1. You might also try to prove it by induction using the idea behind the illustration in the last diagram.

Exercise 0.3.4. Prove (0.3.3) for each integer $n\geq 1$, by induction using exercise 0.3.1(a).

Additional exercises

Exercise 0.4.1. (a) Prove that for all $n\geq 1$ we have

$$\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}^n=\begin{pmatrix}F_{n+1} & F_n\\ F_n & F_{n-1}\end{pmatrix}.$$

(b) Deduce that $F_{n+1}F_{n-1}-F_n^2=(-1)^n$ for all $n\geq 1$.

(c) Deduce that $F_{n+1}^2-F_{n+1}F_n-F_n^2=(-1)^n$ for all $n\geq 0$.

Exercise 0.4.2.† Deduce from (0.1.1) that the Fibonacci number F_n is the nearest integer to $\phi^n/\sqrt{5}$, for each integer $n\geq 0$, where the constant $\phi:=\frac{1+\sqrt{5}}{2}$. This *golden ratio* appears in art and architecture when attempting to describe "perfect proportions".

Exercise 0.4.3. Prove that $F_n^2+F_{n+3}^2=2(F_{n+1}^2+F_{n+2}^2)$ for all $n\geq 0$.

Exercise 0.4.4. Prove that for all $n\geq 1$ we have

$$F_{2n-1}=F_{n-1}^2+F_n^2 \quad\text{and}\quad F_{2n}=F_{n+1}^2-F_{n-1}^2.$$

Exercise 0.4.5. Use (0.1.1) to prove the following:

(a) For every r we have $F_n^2-F_{n+r}F_{n-r}=(-1)^{n-r}F_r^2$ for all $n\geq r$.

(b) For all $m\geq n\geq 0$ we have $F_mF_{n+1}-F_{m+1}F_n=(-1)^nF_{m-n}$.

Exercise 0.4.6. Let $u_0=b$ and $u_{n+1}=au_n$ for all $n\geq 0$. Give a formula for all u_n with $n\geq 0$.

Exercise 0.4.7.† (a) If $0w$ is a string of 0's and 1's of length n, prove that $0w \in A_n$ if and only if $w \in A_{n-1}$.

(b) If $10w$ is a string of 0's and 1's of length n, prove that $10w \in A_n$ if and only if $w \in A_{n-2}$.

(c) Prove that $|A_n| = F_{n+2}$ for all $n \geq 1$, by induction on n.

Exercise 0.4.8.† Prove that every positive integer other than the powers of 2 can be written as the sum of two or more consecutive integers.

Exercise 0.4.9. Prove that $\binom{n}{m}\binom{n-m}{a-m} = \binom{a}{m}\binom{n}{a}$ for any integers $n \geq a \geq m \geq 0$.

Exercise 0.4.10.† Suppose that a and b are integers and $\{x_n : n \geq 0\}$ is the second-order linear recurrence sequence given by (0.1.2) with $x_0 = 0$ and $x_1 = 1$.

(a) Prove that for all non-negative integers m we have

$$x_{m+k} = x_{m+1}x_k + bx_m x_{k-1} \text{ for all integers } k \geq 1.$$

(b) Deduce that

$$x_{2n+1} = x_{n+1}^2 + bx_n^2 \quad \text{and} \quad x_{2n} = x_{n+1}x_n + bx_n x_{n-1} \quad \text{for all natural numbers } n.$$

Exercise 0.4.11. Suppose that the sequences $\{x_n : n \geq 0\}$ and $\{y_n : n \geq 0\}$ both satisfy (0.1.2) and that $x_0 = 0$ and $x_1 = 1$, whereas y_0 and y_1 might be anything. Prove that

$$y_n = y_1 x_n + b y_0 x_{n-1} \text{ for all } n \geq 1.$$

Exercise 0.4.12. Suppose that $x_0 = 0$, $x_1 = 1$, and $x_{n+2} = ax_{n+1} + bx_n$. Prove that for all $n \geq 1$ we have

(a) $(a + b - 1)\sum_{j=1}^{n} x_j = x_{n+1} + bx_n - 1$;

(b) $a(b^n x_0^2 + b^{n-1}x_1^2 + \cdots + bx_{n-1}^2 + x_n^2) = x_n x_{n+1}$;

(c) $x_n^2 - x_{n-1}x_{n+1} = (-b)^{n-1}$.

Exercise 0.4.13. Suppose that $x_{n+2} = ax_{n+1} + bx_n$ for all $n \geq 0$.

(a) Show that

$$\begin{pmatrix} x_{n+2} & x_{n+1} \\ x_{n+1} & x_n \end{pmatrix} = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} x_2 & x_1 \\ x_1 & x_0 \end{pmatrix} \text{ for all } n \geq 0.$$

(b) Deduce that $x_{n+2}x_n - x_{n+1}^2 = c(-b)^n$ for all $n \geq 0$ where $c := x_2 x_0 - x_1^2$.

(c) Deduce that $x_{n+1}^2 - ax_{n+1}x_n - bx_n^2 = -c(-b)^n$.

Exercise 0.4.14. Show that if $F_0 = 3$ and $F_{n+1} = F_n^2 - 2F_n + 2$, then $F_n = 2^{2^n} + 1$ for all $n \geq 0$.

Exercise 0.4.15. (a) Show that if $M_0 = 0$, $M_1 = 1$, and $M_{n+2} = 3M_{n+1} - 2M_n$ for all integers $n \geq 0$, then $M_n = 2^n - 1$ for all integers $n \geq 0$. The integer M_n is the nth *Mersenne number* (see exercise 2.5.16 and sections 4.2, 5.1, etc.).

(b) Show that if $M_0 = 0$ with $M_{n+1} = 2M_n + 1$ for all $n \geq 0$, then $M_n = 2^n - 1$.

Exercise 0.4.16.‡ We can reinterpret exercise 0.4.3 as giving a recurrence relation for the sequence $\{F_n^2\}_{n \geq 0}$, where F_n is the nth Fibonacci number; that is,

$$F_{n+3}^2 = 2F_{n+2}^2 + 2F_{n+1}^2 - F_n^2 \text{ for all } n \geq 0.$$

Here F_{n+3}^2 is described in terms of the last three terms of the sequence; this is called a *linear recurrence of order* 3. Prove that for any integer $k \geq 1$, the sequence $\{F_n^k\}_{n \geq 0}$ satisfies a linear recurrence of order $k + 1$.

Appendix 0A. A closed formula for sums of powers

0.5. Formulas for sums of powers of integers, II

Exercise 0.5.1.[‡] (a) Establish that (0.5.1) holds with

$$c_m = m^k - \binom{m}{1}(m-1)^k + \binom{m}{2}(m-2)^k - \cdots + (-1)^{m-2}\binom{m}{m-2}2^k + (-1)^{m-1}m,$$

for all $m \geq 1$ and for all $k \geq 1$. The integers $c_m/m!$ are the *Stirling numbers of the second kind*, usually denoted by $S_2(k,m)$. They arise in several interesting combinatorial settings; for example, $S_2(k,m)$ is the number of ways to partition a set of k objects into m non-empty subsets.

(b) Deduce that, for any given integer $k \geq 0$, there exist rational numbers $a_0, a_1, \ldots, a_{k+1}$ for which $\sum_{n=0}^{N-1} n^k = a_0 + a_1 N + \cdots + a_{k+1}N^{k+1}$ for all integers $N \geq 1$.

Exercise 0.5.2. Prove that $c_j/j!$ is an integer for all $j \geq 0$ in (0.5.1).

Exercise 0.5.3.[†] Let $f(x) \in \mathbb{C}[x]$. Prove that $f(n)$ is an integer for all integers n if and only if $f(x) = \sum_m a_m \binom{x}{m}$ where the a_m are all integers.

Appendix 0B. Generating functions

Exercise 0.6.1. (a) Prove that for every integer $k \geq 0$ one has

$$\frac{1}{(1-t)^{k+1}} = \binom{k}{k} + \binom{k+1}{k}t + \binom{k+2}{k}t^2 + \cdots + \binom{k+m}{k}t^m + \cdots.$$

(b) Prove that (0.3.1) follows by equating the coefficient of t^{N-k-1} on either side of

$$\frac{1}{(1-t)^{k+1}} \cdot \frac{1}{(1-t)} = \frac{1}{(1-t)^{k+2}}.$$

(c) Multiply this identity through by $1-t$ and reprove the formula in exercise 0.3.1.(a) by equating the coefficients on each side.

0.6. Formulas for sums of powers of integers, III

Exercise 0.6.2. (a) Prove that $\sum_{m\geq 2} \frac{1}{m(m-1)} = 1$.

(b) Prove that $\sum_{k\geq 2} \frac{1}{m^k} = \frac{1}{m(m-1)}$.

(c) Deduce that $\sum_{k\geq 2}(\zeta(k)-1) = 1$.

Exercise 0.6.3. Let $\mathcal{P}$ be the set of perfect powers > 1. Let $\mathcal{N}$ be the set of integers > 1 that are not perfect powers (so that $\mathcal{P} \cup \mathcal{N}$ is a partition of the integers > 1).

(a) Prove that $\mathcal{P} = \{n^k : n \in \mathcal{N} \text{ and } k \geq 2\}$ and $\{n^k : n \in \mathcal{N} \text{ and } k \geq 1\} = \{m \geq 2\}$.

(b) Prove that $\sum_{P\in\mathcal{P}} \frac{1}{P-1} = \sum_{k\geq 2}\sum_{n\in\mathcal{N}}\sum_{j\geq 1}\frac{1}{n^{jk}}$.

(c) Deduce that $\sum_{P\in\mathcal{P}} \frac{1}{P-1} = 1$.

This result was communicated by Goldbach to Euler in 1744.

0.7. The power series view on the Fibonacci numbers

Exercise 0.7.1.[†] Use this to deduce (0.1.3) when $a^2+4b \neq 0$, and exercise 0.1.5(c) when $a^2+4b = 0$.

Exercise 0.7.2.[‡] Prove that (0.7.1) holds.

Exercise 0.7.3.‡ Let $(x_n)_{n\geq 0}$ be the sequence which begins $x_0 = 0, x_1 = 1$ and then $x_n = ax_{n-1} + bx_{n-2}$ for all $n \geq 2$. Its *companion sequence*, $(y_n)_{n\geq 0}$, begins $y_0 = 2, y_1 = x_2$ and then $y_n = ay_{n-1} + by_{n-2}$ for all $n \geq 2$. For example, $x_n = 2^n - 1$ has companion sequence $y_n = 2^n + 1$.

(a) Prove that $y_n = \alpha^n + \beta^n$ for all $n \geq 0$ and also that $y_n = x_{2n}/x_n$.
(b) Let $z_0 = -1$ and $z_n = -bz_{n-1}$ for all $n \geq 1$. Give an explicit formula for z_n.
(c) Prove that $x_{m+2n} = y_n x_{m+n} + z_n x_m$ for all $m, n \geq 0$.
(d) Deduce that $F_{n+6} = 4F_{n+3} + F_n$ for all $n \geq 0$.

Appendix 0C. Finding roots of polynomials

0.8. Solving the general cubic

Exercise 0.8.1. Show that the roots of any given cubic polynomial, $Ax^3 + Bx^2 + Cx + D$ with $A \neq 0$, can be obtained from the roots of some cubic polynomial of the form $x^3 + ax + b$, by adding $B/3A$ to each root. Moreover write a and b explicitly as functions of A, B, and C.

0.9. Solving the general quartic

0.10. Surds

Appendix 0D. What is a group?

0.11. Examples and definitions

Exercise 0.11.1. Prove that if G a subgroup of $\mathbb{Z}$ under addition, then either $G = \{0\}$ or $G = m\mathbb{Z} := \{mn : n \in \mathbb{Z}\}$ for some integer $m \geq 1$.

0.12. Matrices usually don't commute

Exercise 0.12.1. Let M be an n-by-n matrix.

(a) Prove that if A and B commute with M, then so does $rA + sB$ for any complex numbers r and s. (We call $rA + sB$ a *linear combination* of A and B.)
(b) Prove that M^k commutes with M, for all k.
(c) Deduce that all linear combinations of $I, M, \ldots, M^{n-1}$ belong to $\mathrm{Comm}(M)$.

Exercise 0.12.2. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

(a) Prove that M is not a multiple of I if and only if at least one of $a \neq d$, $b \neq 0$, $c \neq 0$ holds.
(b) Prove that if $a \neq d$, then for any matrix A there exists $r, s \in \mathbb{C}$ such that $A - rI - sM$ has zeros down the diagonal.
(c) Prove that if $b \neq 0$, then for any matrix A there exists $r, s \in \mathbb{C}$ such that $A - rI - sM$ has zeros throughout the top row.
(d) Prove that if $c \neq 0$, then for any matrix A there exists $r, s \in \mathbb{C}$ such that $A - rI - sM$ has zeros throughout the first column

Appendix 0E. Rings and fields

0.13. Mixing addition and multiplication together: Rings and fields

Exercise 0.13.1. Prove that $a \times 0 = 0$ for all $a \in A$, when A is a field.

Exercise 0.13.2. (a) Prove that $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ and that $\mathbb{Z}[\sqrt{2}]$ is a ring.
(b) Prove that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ and that $\mathbb{Q}(\sqrt{2})$ is a field.

0.14. Algebraic numbers, integers, and units, I

Exercise 0.14.1. Let $f(x)$ be the minimal polynomial of an algebraic number α.
(a) Prove that if $g(x)$ is a polynomial with integer coefficients for which $g(\alpha) = 0$, then $f(x)$ divides $g(x)$. (You may use Proposition 2.10.1 of appendix 2B in your proof.)
(b) Prove that if $f(x)$ divides $g(x) \in \mathbb{Z}[x]$ and g is monic, then f is monic. Deduce that if $g(\alpha) = 0$, then α is an algebraic integer.
(c) Prove that if $g(\alpha) = 0$ and g is irreducible, then $g = \kappa f$ for some constant $\kappa \neq 0$.
(d) Prove that $f(x)$ is the only minimal polynomial of α.
(e) Prove that $(x - \alpha)^2$ does not divide $f(x)$.

Exercise 0.14.2. Prove that if α is an algebraic number and a root of $f(x) \in \mathbb{Z}[x]$ where f has leading coefficient a, then $a\alpha$ is an algebraic integer.

Exercise 0.14.3. What are the algebraic integers in $\mathbb{Q}$?

Exercise 0.14.4. (a) Prove that $\mathbb{Z}[\sqrt{d}]$ is a subset of the algebraic integers.
(b) Prove that $\mathbb{Z}[\sqrt{2}]$ is the set of algebraic integers in $\mathbb{Q}(\sqrt{2})$.
(c) Prove that $\frac{1+\sqrt{5}}{2}$ is an algebraic integer.

Exercise 0.14.5. (a) Prove that $1/\alpha$ has minimal polynomial $x^d f(1/x)$.
(b) Prove that α and $1/\alpha$ are both algebraic integers if and only if f is monic and $f(0) = 1$ or -1. In this case α and $1/\alpha$ are called *units*.

Another way to view this is that α is a unit if and only if α divides 1, for if $\beta = 1/\alpha$, then $\alpha\beta = 1$ and α and β are both algebraic integers.

Exercise 0.14.6. Suppose that α and β are algebraic integers such that α divides β, and β divides α. Prove that there exists a unit u for which $\beta = u\alpha$

Exercise 0.14.7. (a) Prove that if α is an algebraic number, then $\mathbb{Q}(\alpha)$ is a field.
(b) Prove that if α is an algebraic integer, then $\mathbb{Z}[\alpha]$ is a ring.

Appendix 0F. Symmetric polynomials

0.15. The theory of symmetric polynomials

Exercise 0.15.1. Show that for any permutation σ of $1, 2, \ldots, n$ and any symmetric polynomial P we have $P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = P(x_1, x_2, \ldots, x_n)$.

Exercise 0.15.2. If f is not monic, develop analogous results by working with $g(x)$ defined by $g(a_d x) = a_d^{d-1} f(x)$.

0.16. Some special symmetric polynomials

Exercise 0.16.1. Show that if $f(t) = \prod_{i=1}^{k}(t - \alpha_i) \in \mathbb{Z}[t]$, then $\prod_{j=1}^{d} f'(\alpha_j)$ is an integer, by using the theory of symmetric polynomials.

Exercise 0.16.2. Use the same argument to explain that the determinant of *Vandermonde matrix* V, where $V_{i,j} = \alpha_i^{j-1}$, $1 \le i, j \le d$, is $\prod_{1 \le i < j \le d}(\alpha_i - \alpha_j)$.

Exercise 0.16.3. Prove Theorem 0.2 when each $e_j = 1$ (assuming exercise 0.16.2).

Exercise 0.16.4.‡ (This question requires some knowledge of linear algebra.) Suppose that M is an n-by-n matrix.

(a) Prove that if M is a diagonal matrix in which all the diagonal entries are distinct, then Comm(M) equals the set of diagonal matrices.
(b) Use exercise 0.16.2 to show that the set of diagonal matrices is then given by $\{a_0 I + a_1 M + \cdots + a_{n-1}M^{n-1} : \text{ each } a_j \in \mathbb{C}\}$.
(c) Now let M, N, and T be n-by-n matrices with T invertible. Prove that M and N commute if and only if $T^{-1}MT$ and $T^{-1}NT$ commute.
(d) Prove that if M is an n-by-n matrix with n distinct eigenvalues, then $\text{Comm}(M) = \{a_0 I + a_1 M + \cdots + a_{n-1}M^{n-1} : \text{ each } a_j \in \mathbb{C}\}$.

0.17. Algebraic numbers, integers, and units, II

Exercise 0.17.1. (a)† Prove that if $\alpha \ne 0$ and β are algebraic integers, then $\alpha\beta$ is also an algebraic integer.
(b) Prove that if $\alpha \ne 0$ and β are algebraic numbers, then $\alpha + \beta$ and $\alpha\beta$ are algebraic numbers.

Exercise 0.17.2. Prove that if $\alpha_1, \ldots, \alpha_k$ are algebraic numbers, then $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ is a field. These are the *number fields*.

Appendix 0G. Constructibility

0.18. Constructible using only compass and ruler

Exercise 0.18.1. Show that the coefficients of the equation of this line can be determined by a degree-one equation in already known coordinates.

Exercise 0.18.2. Prove that any two (non-parallel) lines intersect in a point that can be determined by a degree-one equation in the coefficients of the equations of the lines.

Given a length r and a point $C = (c_1, c_2)$, we can draw the circle $(x - c_1)^2 + (y - c_2)^2 = r^2$ centered at C of radius r.

Exercise 0.18.3. Prove that the points of intersection of this circle with a given line can be given by a degree-two equation in already known coordinates.

Exercise 0.18.4. Prove that the points of intersection of two circles can be given by a degree-two equation in already known coordinates.