Chapter 1

The Euclidean algorithm

1.1. Finding the gcd

Exercise 1.1.1. In this question, and throughout, we assume that a, b, and c are integers.
(a) Prove that if b divides a, then either $a = 0$ or $|a| \geq |b|$.
(b) Deduce that if $a|b$ and $b|a$, then $b = a$ or $b = -a$ (which, in future, we will write as "$b = \pm a$").
(c) Prove that if a divides b and c, then a divides $bx + cy$ for all integers x, y.
(d) Prove that a divides b if and only if a divides $-b$ if and only if $-a$ divides b.
(e) Prove that if a divides b, and b divides c, then a divides c.
(f) Prove that if $a \neq 0$ and ac divides ab, then c divides b.

Exercise 1.1.2. Suppose that $a \geq 1$ and $b \geq 2$ are integers. Show that we can write a in base b; that is, show that there exist integers $a_0, a_1, \ldots \in [0, b-1]$ for which $a = a_d b^d + a_{d-1} b^{d-1} + a_1 b + a_0$.

Exercise 1.1.3. Use Corollary 1.1.1 to prove that the Euclidean algorithm indeed yields the greatest common divisor of two given integers. (You might prove this by induction on the smallest of the two integers.)

Exercise 1.1.4. Prove that $(F_n, F_{n+1}) = 1$ by induction on $n \geq 0$.

1.2. Linear combinations

Exercise 1.2.1. (a) Prove that if d divides both a and b, then d divides $\gcd(a, b)$.
(b) Deduce that d divides both a and b *if and only if* d divides $\gcd(a, b)$.
(c) Prove that $1 \leq \gcd(a, b) \leq |a|$ and $|b|$.
(d) Prove that $\gcd(a, b) = |a|$ if and only if a divides b.

Exercise 1.2.2. Suppose that a divides m, and b divides n.
(a) Deduce that $\gcd(a, b)$ divides $\gcd(m, n)$.
(b) Deduce that if $\gcd(m, n) = 1$, then $\gcd(a, b) = 1$.

Exercise 1.2.3. Show that Theorem 1.1 holds for any integers a and b that are not both 0. (It is currently stated and proved only for positive integers a and b.)

Exercise 1.2.4. (a) Use exercise 1.1.1(c) to show that if $au + bv = 1$, then $(a, b) = (u, v) = 1$.
(b) Prove that $\gcd(u, v) = 1$ in Theorem 1.1.

Exercise 1.2.5. (a) Show that if A and B are given integers, not both 0, with $g = \gcd(A, B)$, then $\gcd(A/g, B/g) = 1$.
(b) Prove that any rational number u/v where $u, v \in \mathbb{Z}$ with $v \neq 0$ may be written as r/s where r and s are coprime integers with $s > 0$. This is called a *reduced fraction*.

1.3. The set of linear combinations of two integers

Exercise 1.3.1. Suppose that a, b, and c are non-zero integers for which $a + b = c$.
(a) Show that a, b, c are relatively prime if and only if they are pairwise coprime.
(b) Show that $(a, b) = (a, c) = (b, c)$.
(c) Show that the analogy to (a) is false for integer solutions a, b, c, d to $a + b = c + d$ (perhaps by constructing a counterexample).

1.4. The least common multiple

Exercise 1.4.1. Prove that $\mathrm{lcm}[m, n] = n$ if and only if m divides n.

Exercise 1.4.2. Prove that $\mathrm{lcm}[ma, mb] = m \cdot \mathrm{lcm}[a, b]$ for any positive integer m.

1.5. *Continued fractions*

Exercise 1.5.1. (a) Show that if $a_k > 1$, then $[a_0,\ a_1, \ldots,\ a_k] = [a_0,\ a_1, \ldots,\ a_k - 1, 1]$.
(b) Prove that the set of positive rational numbers are in 1-1 correspondence with the finite length continued fractions that do not end in 1.

1.6. *Tiling a rectangle with squares*

Exercise 1.6.1. Given an a-by-b rectangle show how to write $a \cdot b$ as a sum of squares, as above, in terms of the partial quotients and convergents of the continued fraction for a/b.

Exercise 1.6.2. (a) Use this to show that $F_{n+1}F_n = F_n^2 + F_{n-1}^2 + \cdots + F_0^2$, where F_n is the nth Fibonacci number (see section 0.1 for the definition and a discussion of Fibonacci numbers and exercise 0.4.12 (b) for a generalization of this exercise).
(b)† Find the correct generalization to more general second-order linear recurrence sequences.

Additional exercises

Exercise 1.7.1. (a) Does 0 divide 0? (Use the definition of "divides".)
(b) Show that there is no unique meaning to $0/0$.
(c) Prove that if b divides a and $b \neq 0$, then there is a unique meaning to a/b.

Exercise 1.7.2. Prove that if a and b are not both 0, then $\gcd(a, b)$ is a positive integer.

Exercise 1.7.3.† Prove that if m and n are coprime positive integers, then $\frac{(m+n-1)!}{m!n!}$ is an integer.

Exercise 1.7.4. Suppose that $a = qb + r$ with $0 \leq r \leq b - 1$.
(a) Let $[t]$ be the *integer part* of t, that is, the largest integer $\leq t$. Prove that $q = [a/b]$.
(b) Let $\{t\}$ to be the *fractional part* of t, that is, $\{t\} = t - [t]$. Prove that $r = b\{r/b\} = b\{a/b\}$.

(Beware of these functions applied to negative numbers: e.g., $[-3.14] = -4$ *not* -3, and $\{-3.14\} = .86$ *not* $.14$.)

Exercise 1.7.5.† (a) Show that if n is an integer, then $\{n+\alpha\} = \{\alpha\}$ and $[n+\alpha] = n + [\alpha]$ for all $\alpha \in \mathbb{R}$.
(b) Prove that $[\alpha+\beta] - [\alpha] - [\beta] = 0$ or 1 for all $\alpha, \beta \in \mathbb{R}$, and explain when each case occurs.
(c) Deduce that $\{\alpha\} + \{\beta\} - \{\alpha+\beta\} = 0$ or 1 for all $\alpha, \beta \in \mathbb{R}$, and explain when each case occurs.
(d) Show that $\{\alpha\} + \{-\alpha\} = 1$ unless α is an integer in which case it equals 0.
(e) Show that if $a \in \mathbb{Z}$ and $r \in \mathbb{R} \setminus \mathbb{Z}$, then $[r] + [a-r] = a - 1$.

Exercise 1.7.6. Suppose that d is a positive integer and that $N, x > 0$.
(a) Show that there are exactly $[x]$ positive integers $\leq x$.
(b) Show that kd is the largest multiple of d that is $\leq N$, where $k = [N/d]$.
(c) Deduce that there are exactly $[N/d]$ positive integers $n \leq N$ which are divisible by d.

Exercise 1.7.7. Prove that $\sum_{k=0}^{n-1} [a + \frac{k}{n}] = [na]$ for any real number a and integer $n \geq 1$.

Exercise 1.7.8. Suppose that $a + b = c$ and let $g = \gcd(a, b)$. Prove that we can write $a = gA$, $b = gB$, and $c = gC$ where $A + B = C$, where A, B, and C are pairwise coprime integers.

Exercise 1.7.9. Prove that if $(a, b) = 1$, then $(a+b, a-b) = 1$ or 2.

Exercise 1.7.10.† Prove that for any given integers $b > a \geq 1$ there exists an integer solution u, w to $au - bw = \gcd(a, b)$ with $0 \leq u \leq b-1$ and $0 \leq w \leq a-1$.

Exercise 1.7.11.† Show that if $\gcd(a, b) = 1$, then $\gcd(a^k, b^\ell) = 1$ for all integers $k, \ell \geq 1$.

Exercise 1.7.12. Let m and n be positive integers. What fractions do the two lists $\frac{1}{m}, \dots, \frac{m-1}{m}$ and $\frac{1}{n}, \dots, \frac{n-1}{n}$ have in common (when the fractions are reduced)?

Exercise 1.7.13. Suppose m and n are coprime positive integers. When the fractions $\frac{1}{m}, \frac{2}{m}, \dots, \frac{m-1}{m}, \frac{1}{n}, \dots, \frac{n-1}{n}$ are put in increasing order, what is the shortest distance between two consecutive fractions?

Exercise 1.7.14. (a) Since $3 \times 7 - 4 \times 5 = 1$ describe how we can proceed by filling the 7-liter jug each time rather than filling the 5-liter jug.
(b) Can you measure 1 liter of water using a 25-liter jug and a 17-liter jug?
(c)† Prove that if m and n are positive coprime integers then you can measure one liter of water using an m liter jug and an n liter jug?
(d) Prove that one can do this wasting less than mn liters of water.

Exercise 1.7.15. Can you weigh 1 lb of tea using scales with 25-lb and 17-lb weights?

Exercise 1.7.16. Show that $I(a_1, \dots, a_k) = I(g)$ for any non-zero integers $a_1, \dots, a_k$, where we have $g = \gcd(a_1, \dots, a_k)$.

Exercise 1.7.17.† Deduce that if we are given integers $a_1, a_2, \dots, a_k$, not all zero, then there exist integers $m_1, m_2, \dots, m_k$ such that

$$m_1 a_1 + m_2 a_2 + \cdots + m_k a_k = \gcd(a_1, a_2, \dots, a_k).$$

We say that the integers $a_1, a_2, \dots, a_k$ are *relatively prime* if $\gcd(a_1, a_2, \dots, a_k) = 1$. We say that they are *pairwise coprime* if $\gcd(a_i, a_j) = 1$ whenever $i \neq j$. Note that $6, 10, 15$ are relatively prime, but not pairwise coprime (since each pair of integers has a common factor > 1).

Exercise 1.7.18. Prove that if $g = \gcd(a_1, a_2, \dots, a_k)$, then $\gcd(a_1/g, a_2/g, \dots, a_k/g) = 1$.

Exercise 1.7.19.† (a) Prove that $abc = [a, b, c] \cdot \gcd(ab, bc, ca)$.
(b)‡ Prove that if $r + s = n$, then

$$a_1 \cdots a_n = \operatorname{lcm}\left[\prod_{i\in I} a_i : \ I \subset \{1, \dots, n\}, \ |I| = r\right] \cdot \gcd\left(\prod_{j\in J} a_j : \ J \subset \{1, \dots, n\}, \ |J| = s\right).$$

Divisors in recurrence sequences

Exercise 1.7.20. (a) Prove that if $m|n$, then $2^m - 1$ divides $2^n - 1$.
(b)† Prove that if $n = qm + r$ with $0 \le r \le m-1$, then there exists an integer Q such that

$$2^n - 1 = Q(2^m - 1) + (2^r - 1) \qquad \text{(and note that } 0 \le 2^r - 1 < 2^m - 1\text{)}.$$

(c)† Use the Euclidean algorithm to show that $\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(n,m)} - 1$.
(d) What is the value of $\gcd(N^a - 1, N^b - 1)$ for arbitrary integer $N \neq -1, 0,$ or 1?

We assume that a and b are coprime integers with $x_0 = 0,\ x_1 = 1$ and that $x_n = ax_{n-1} + bx_{n-2}$ for all $n \ge 2$.

Exercise 1.7.21. Use exercise 0.4.10(a) to show that $\gcd(x_m, x_n) = \gcd(x_m, x_{m+1}x_{n-m})$ whenever $n \ge m$.

Exercise 1.7.22.† Prove that if $m|n$, then $x_m|x_n$; that is, $\{x_n :\ n \ge 0\}$ is a *division sequence*.

Exercise 1.7.23.† Assume that $(a, b) = 1$.
(a) Prove that $\gcd(x_n, b) = 1$ for all $n \ge 1$.
(b) Prove that $\gcd(x_n, x_{n-1}) = 1$ for all $n \ge 1$.
(c) Prove that if $n > m$, then $(x_n, x_m) = (x_{n-m}, x_m)$.
(d) Deduce that $(x_n, x_m) = x_{(n,m)}$.

Exercise 1.7.24.† For any given integer $d \ge 2$, let $m = m_d$ be the smallest positive integer for which d divides x_m. Prove that d divides x_n if and only if m_d divides n.

Exercise 1.7.25. Let us suppose that $x_n = ax_{n-1} + x_{n-2}$ for all integers n, both positive and negative, with $x_0 = 0$ and $x_1 = 1$. Prove, by induction on $n \ge 1$, that $x_{-n} = (-1)^{n-1}x_n$ for all $n \ge 2$.

Appendix 1A. Reformulating the Euclidean algorithm

1.8. Euclid matrices and Euclid's algorithm

Exercise 1.8.1. Prove that this description of the Euclidean algorithm really works.

Exercise 1.8.2. (a) Show that $p_jq_{j-1} - p_{j-1}q_j = (-1)^{j+1}$ for all $j \ge 0$.
(b) Explain how to use the Euclidean algorithm, along with (1.8.1), to determine, for given positive integers a and b, an integer solution u, v to the equation $au + bv = \gcd(a, b)$.

Exercise 1.8.3. With the notation as above, show that $[a_k, \dots, a_0] = a/c$ for some integer c for which $0 < c < a$ and $bc \equiv (-1)^k \pmod a$.

Exercise 1.8.4. Prove that for every $n \ge 1$ we have

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

where F_n is the nth Fibonacci number.

1.9. Euclid matrices and ideal transformations

Exercise 1.9.1. (a) With the notation of section 1.8, establish that $xu_j + yu_{j+1} = ma + nb$ where the variables x and y are obtained from the variables m and n by a linear transformation.
(b) Deduce that $I(u_j, u_{j+1}) = I(a, b)$ for $j = 0, \dots, k$.

1.10. The dynamics of the Euclidean algorithm

Appendix 1B. Computational aspects of the Euclidean algorithm

1.11. Speeding up the Euclidean algorithm

1.12. Euclid's algorithm works in "polynomial time"

Exercise 1.12.1.† (a) Prove that if F_n is the nth Fibonacci number, then $v_n \geq F_n$ for all n.
(b)‡ Show that this inequality cannot be improved, in general.
(c) Show that if we apply the usual Euclid algorithm to $a \geq b \geq 1$, then it terminates in $\leq \frac{\log a}{\log \phi} + 2$ steps, where $\phi = \frac{1+\sqrt{5}}{2}$.

Exercise 1.12.2. Find two coprime four-digit integers a and b for which the Euclidean algorithm works in (a) as few steps as possible and (b) as many steps as possible.

Appendix 1C. Magic squares

1.13. Turtle power

Exercise 1.13.1. Prove that if A is a magic square, then $mA + n$ is also a magic square for any integers m, n, where $(mA + n)_{i,j} = mA_{i,j} + n$ for all i, j.

1.14. Latin squares

Exercise 1.14.1. For a given integer $n > 1$, let $(\ell)_n$ be the least non-negative residue of $\ell \pmod n$.
(a) Show that if $(ab, n) = 1$ and $A_{i,j} = (ai + bj)_n$, then A is an n-by-n Latin square.
(b) Show that if, also, $(cd, n) = (ad - bc, n) = 1$ and $B_{i,j} = (ci + dj)_n$, then A and B are orthogonal n-by-n Latin squares.
(c) Prove that there exist integers a, b, c, d for which $(abcd, n) = (ad - bc, n) = 1$ if and only if n is odd.
(d) Deduce that there are n-by-n normal magic squares whenever n is odd and > 1.

1.15. Factoring magic squares

Exercise 1.15.1. (a) Verify that C is a normal magic square.
(b) Suppose that we have constructed a normal magic square of order 8. Deduce that there are normal magic squares of order n, whenever n is divisible by 4.

Exercise 1.15.2. Let $n = 4m$ and define $O = \{0, \dots, m-1\} \cup \{3m, \dots, 4m-1\}$ whereas $I = \{m, \dots, 3m-1\}$. We define an n-by-n magic square A with (i, j)th entry, for $0 \leq i, j \leq n-1$,

$$A(i,j) = \begin{cases} in + j + 1 & \text{if } i, j \in I \text{ or } i, j \in O, \\ (n-1-i)n + (n-1-j) + 1 & \text{if } i \in I \text{ and } j \in O, \text{ or if } i \in O \text{ and } j \in I. \end{cases}$$

Prove that A is a normal n-by-n magic square in which any two symmetrically placed integers, around the center, sum to $n^2 + 1$.

Appendix 1D. The Frobenius postage stamp problem

1.16. The Frobenius postage stamp problem, I

Exercise 1.16.1. (a) Rewrite this last proof as a formal proof by induction to establish that $\{n \in \mathbb{Z} : \ n \geq 8\} \subset \mathcal{P}(3,5)$.
(b) Suppose that $1 \leq a < b$. Assume there exists an integer N (which may depend on a and b), for which $N, N+1, \ldots, N+a-1$ all belong to $\mathcal{P}(a,b)$. Deduce that $\{n \in \mathbb{Z} : \ n \geq N\} \subset \mathcal{P}(a,b)$.

In section 3.25 of appendix 3G, we will develop a technique for establishing that this assumption holds for some integer N whenever $\gcd(a,b) = 1$.

Exercise 1.16.2. (a) Prove that $\mathcal{E}(2,3) = \{1\}$.
(b) An integer n is a *power* if $n = m^k$ for some integers m and $k \geq 2$. Prove that we can write any power n as $n = a^2b^3$ where a and b are integers.

Exercise 1.16.3. (a) Construct $\mathcal{E}(a,b)$ for various pairs of coprime integers a and b.
(b) Guess at a formula (in terms of a and b) for the largest element of $\mathcal{E}(a,b)$, that is, the largest positive integer not representable in the form $am + bn$ with $m, n \geq 0$. (Use your data from part (a).)
(c)‡ Prove that your conjectural formula in (b) is true.

Appendix 1E. Egyptian fractions

1.17. Simple fractions

Exercise 1.17.1. Deduce that $1/b$ with $b > 1$ may always be written as $1/m + 1/n$ with m and n distinct positive integers.

Exercise 1.17.2. Suppose that $b > a \geq 2$ are positive coprime integers. Let $q = [b/a]$.
(a) Prove that $a/b = 1/(q+1) + A/B$ where A and B are positive integers with $A < a, B$.
(b) Deduce that a/b can be written as a sum of no more than a distinct unit fractions.