Chapter 3

The basic algebra of number theory

Exercise 3.0.1. Suppose that p is a prime number. Prove that $\gcd(p, a) = 1$ if and only if p does not divide a.

3.1. The Fundamental Theorem of Arithmetic

Exercise 3.1.1. Prove that any integer $n > 1$ can be factored into a product of primes.

Exercise 3.1.2. (a) Prove that if prime p divides $a_1 a_2 \cdots a_k$, then p divides a_j for some j, $1 \leq j \leq k$.
(b) Deduce that if prime p divides $q_1 \cdots q_k$ where each q_i is prime, then $p = q_j$ for some j, $1 \leq j \leq k$.

Exercise 3.1.3. (a) Prove that every natural number has a unique representation as $2^k m$ with $k \geq 0$ and m an odd natural number.
(b) Show that each integer $n \geq 3$ is either divisible by 4 or has at least one odd prime factor.
(c) An integer is *squarefree* if every prime in its factorization appears to the power 1. Prove that every non-zero integer can be written, uniquely, in the form mn^2 where m is a squarefree integer and n is a non-zero positive integer.
(d)† Deduce that every non-zero rational number can be written, uniquely, in the form mr^2 where m is a squarefree integer and r is a positive rational number.

Exercise 3.1.4. (a) Show that if all of the prime factors of an integer n are $\equiv 1 \pmod m$, then $n \equiv 1 \pmod m$. Deduce that if $n \not\equiv 1 \pmod m$ then n has a prime factor that is $\not\equiv 1 \pmod m$.
(b)† Show that if all of the prime factors of an integer n are $\equiv 1$ or $3 \pmod 8$, then $n \equiv 1$ or $3 \pmod 8$. Prove this with 3 replaced by 5 or 7.
(c)† Generalize this as much as you can to other moduli and other sets of congruence classes.

3.2. Abstractions

Exercise 3.2.1. Suppose that $(a, b) = 1$. Prove that if a and b both divide m, then ab divides m.

3.3. Divisors using factorizations

Exercise 3.3.1. Use the description of the divisors of a given integer to prove the following: If $m = \prod_p p^{m_p}$ and $n = \prod_p p^{n_p}$ are positive integers, then (a) $\gcd(m,n) = \prod_p p^{\min\{m_p,n_p\}}$ and (b) $\operatorname{lcm}[m,n] = \prod_p p^{\max\{m_p,n_p\}}$.

Exercise 3.3.2. Deduce that $mn = \gcd(m,n) \cdot \operatorname{lcm}[m,n]$ for all pairs of natural numbers m and n using exercise 3.3.1. (The proof in Corollary 3.2.2 is more difficult.)

Exercise 3.3.3. (a) Prove that d divides $\gcd(a,b)$ if and only if d divides both a and b.
(b) Prove that $\operatorname{lcm}[a,b]$ divides m if and only if a and b both divide m.
(c) Prove that if $(a,b) = g$, then $(a/g, b/g) = 1$.
(d) Prove that if $(a,m) = (b,m) = 1$, then $(ab,m) = 1$.
(e) Prove that if $(a,b) = 1$, then $(ab,m) = (a,m)(b,m)$.
(f)† Show that the hypothesis $(a,b) = 1$ is necessary in part (e), by constructing a counterexample to the conclusion when $(a,b) > 1$.

Exercise 3.3.4. Prove that $\gcd(a,b,c) = \gcd(a,\gcd(b,c))$ and $\operatorname{lcm}[a,b,c] = \operatorname{lcm}[a,\operatorname{lcm}[b,c]]$.

Exercise 3.3.5. Prove that if each of $a, b, c, \ldots$ is coprime with m, then so is $abc\ldots$.

Exercise 3.3.6. Prove that if prime p divides a^n, then p^n divides a^n.

Exercise 3.3.7. (a) Prove that a positive integer A is the square of an integer if and only if the exponent of each prime factor of A is even.
(b) Prove that if $a, b, c, \ldots$ are pairwise coprime, positive integers and their product is a square, then they are each a square.
(c) Prove that if ab is a square, then either $a = gA^2$ and $b = gB^2$, or $a = -gA^2$ and $b = -gB^2$, where $g = \gcd(a,b)$, for some coprime integers A and B.

Exercise 3.3.8. (a) Prove that a positive integer A is the nth power of an integer if and only if n divides the exponent of all of the prime power factors of A.
(b) Prove that if $a, b, c, \ldots$ are pairwise coprime, positive integers and their product is an nth power, then they are each an nth power.

3.4. Irrationality

Exercise 3.4.1. Give a proof of Proposition 3.4.2, which is analogous to the proof of Proposition 3.4.1 above.

Exercise 3.4.2.† Prove that $17^{1/3}$ is irrational (using the ideas of the proof of Proposition 3.4.1).

Exercise 3.4.3. Prove that m divides a_0 by reducing the above equation mod m.

Exercise 3.4.4. Prove that the polynomial $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$.

3.5. Dividing in congruences

Exercise 3.5.1. Assume that $(a,m) = 1$.
(a) Prove that if b is an integer, then $a.0 + b,\ a.1 + b,\ \ldots,\ a(m-1) + b$ form a complete set of residues (mod m).
(b) Deduce that for all given integers b and c, there is a unique value of $x \pmod m$ for which $ax + b \equiv c \pmod m$.

Exercise 3.5.2. Prove that if $\{r_1, \ldots, r_k\}$ is a reduced set of residues mod m and $(a,m) = 1$, then $\{ar_1, \ldots, ar_k\}$ is also a reduced set of residues mod m

Exercise 3.5.3. (a) Show that there exists $r \pmod b$ for which $ar \equiv c \pmod b$ if and only if $\gcd(a,b)$ divides c.
(b)† Prove that the solutions r are precisely the elements of a residue class mod $b/\gcd(a,b)$.

Exercise 3.5.4. Prove that if $(a, m) > 1$, then there does not exist an integer r such that $ar \equiv 1 \pmod{m}$. (And so Corollary 3.5.2 could have been phrased as an "if and only if" condition.)

Exercise 3.5.5. Explain how the Euclidean algorithm may be used to efficiently determine the inverse of $a \pmod{m}$ whenever $(a, m) = 1$. (Calculating the inverse of $a \pmod{m}$ is an essential part of the RSA algorithm discussed in section 10.3.)

3.6. Linear equations in two unknowns

Exercise 3.6.1. Show that if there exists a solution in integers m, n to $am+bn = c$ with $(a, b) = 1$, then there exists a solution with $0 \le m < b$.

Exercise 3.6.2. (a) Find all solutions in integers m, n to $7m + 5n = 1$.
(b) Find all solutions in integers u, v to $7v - 5u = 3$.
(c) Find all solutions in integers j, k to $3j - 9k = 1$.
(d) Find all solutions in integers r, s to $5r - 10s = 15$.

Exercise 3.6.3. Show that a linear equation $am + bn = c$ where a, b, and c are given integers, cannot have exactly one solution in integers m, n.

Exercise 3.6.4 (The local-global principle for linear equations)**.** Let a, b, c be given non-zero integers. There are solutions in integers m, n to $am + bn = c$ if and only if there exist residue classes $u, v \pmod{b}$ such that $au + bv \equiv c \pmod{b}$.

"Global" refers to looking over the infinite number of possibilities for integer solutions, "local" to looking through the finite number of possibilities mod b. This exercise will be revisited in exercise 3.9.13.

3.7. Congruences to several moduli

Exercise 3.7.1. Determine all integers n for which $n \equiv 101 \pmod{7^{11}}$ and $n \equiv 101 \pmod{13^{17}}$, in terms of one congruence.

Exercise 3.7.2. Suppose that $a, b, c, \ldots$ are pairwise coprime integers.
(a) Prove that if $a, b, c, \ldots$ each divide m, then $abc\ldots$ divides m.
(b) Deduce that if $m \equiv n \pmod{a}$ and $m \equiv n \pmod{b}$ and $m \equiv n \pmod{c}$, $\ldots$, then $m \equiv n \pmod{abc\ldots}$.

Exercise 3.7.3.† Use this method to give a general formula for $x \pmod{1001}$ when $x \equiv a \pmod{7}$, $x \equiv b \pmod{11}$, and $x \equiv c \pmod{13}$.

Exercise 3.7.4.† Find the smallest positive integer n which can be written as $n = 2a^2 = 3b^3 = 5c^5$ for some integers a, b, c.

Exercise 3.7.5.† Given residue classes $a_1 \pmod{m_1}, \ldots, a_k \pmod{m_k}$ let $m = \operatorname{lcm}[m_1, \ldots, m_k]$. Prove that there exists a residue class $b \pmod{m}$ for which $b \equiv a_j \pmod{m_j}$ for each j if and only if $a_i \equiv a_j \pmod{(m_i, m_j)}$ for all $i \ne j$.

Exercise 3.7.6. (a) Prove that each of $a, b, c, \ldots$ divides m if and only if $\operatorname{lcm}[a, b, c, \ldots]$ divides m.
(b) Deduce that if $m \equiv n \pmod{a}$ and $m \equiv n \pmod{b}$ and $\ldots$, then $m \equiv n \pmod{\operatorname{lcm}[a, b, \ldots]}$.
(c) Prove that if $b \pmod{m}$ in exercise 3.7.5 exists, then it is unique.

Exercise 3.7.7.† Let M, N, g be positive integers with $(M, N, g) = 1$. Prove that the set of residues $\{aN + bM \pmod{g} : 0 \le a, b \le g - 1\}$ is precisely g copies of the complete set of residues mod g.

Exercise 3.7.8. (a) Prove that for any odd integer m there are infinitely many integers n for which $(n, m) = (n + 1, m) = 1$.
(b) Why is this false if m is even?

(c) Prove that for any integer m there are infinitely many integers n for which $(n, m) = (n + 2, m) = 1$.

(d)‡ Let $a_1 < a_2 < \cdots < a_k$ be given integers. Give an "if and only if" criterion in terms of the $a_i \pmod p$, for each prime p dividing m, to determine whether there are infinitely many integers n for which $(n + a_1, m) = (n + a_2, m) = \cdots = (n + a_k, m) = 1$.

Exercise 3.7.9. Prove that there exist one million consecutive integers, each of which is divisible by the cube of an integer > 1.

3.8. Square roots of $1 \pmod n$

Exercise 3.8.1. Prove that if $(x, 6) = 1$, then $x^2 \equiv 1 \pmod{24}$ *without working mod* 24. You are allowed to work mod 8 and mod 3.

Exercise 3.8.2. (a)† What are the roots of $x^2 \equiv 1 \pmod{2^e}$ for each integer $e \geq 1$? (This must be different from the odd prime case since $x^2 \equiv 1 \pmod 8$ has four solutions, $1, 3, 5, 7 \pmod 8$.)

(b)† Prove that if m has k distinct prime factors, there are exactly $2^{k+\delta}$ solutions $x \pmod m$ to the congruence $x^2 \equiv 1 \pmod m$, where, if $2^e \| m$, then $\delta = 0$ if $e = 0$ or 2, $\delta = -1$ if $e = 1$, and $\delta = 1$ if $e \geq 3$.

(c) Deduce that the product of the square roots of $1 \pmod{2^e}$ equals $1 \pmod{2^e}$ if $e \geq 3$.

Exercise 3.8.3.† Prove that the product of the square roots of $1 \pmod m$ equals $1 \pmod m$, unless $m = 4$ or $m = p^e$ or $m = 2p^e$ for some power p^e of an odd prime p, in which case it equals $-1 \pmod m$.

Additional exercises

Exercise 3.9.1. Prove that if $2^n - 1$ is prime, then n must be prime.

Exercise 3.9.2. Suppose that $0 \leq x_0 \leq x_1 \leq \cdots$ is a division sequence (that is, $x_m | x_n$ whenever $m|n$; see exercise 1.7.22), with $x_{n+1} > x_n$ whenever $n \geq n_0$ (≥ 1). Prove that if x_n is prime for some integer $n > n_0^2$, then n is prime.

Exercise 3.9.3. We introduced the companion sequence $(y_n)_{n\geq 0}$ of the Lucas sequence $(x_n)_{n\geq 0}$ in exercise 0.1.4. Note that $y_1 = a$ does not necessarily divide $y_2 = a^2 + 2b$.

(a)‡ Prove that y_m divides y_n whenever m divides n and n/m is odd.

(b) Assume that $a > 1$ and $b > 0$. Deduce that if y_n is prime, then n must be a power of 2.

(c) Deduce that if $2^n + 1$ is prime, then it must be a Fermat number.

Exercise 3.9.4.‡ Prove that the Fundamental Theorem of Arithmetic implies that for any finite set of primes $\mathcal{P}$, the numbers $\log p$, $p \in \mathcal{P}$, are linearly independent over $\mathbb{Q}$ if they are not linearly dependent over $\mathbb{Q}$.

Exercise 3.9.5.† Prove that $\gcd(a, b, c) \cdot \operatorname{lcm}[a, b, c] = abc$ if and only if a, b, and c are pairwise coprime.

Exercise 3.9.6.† Prove that if a and b are positive integers whose product is a square and whose difference is a prime p, then $a + b = (p^2 + 1)/2$.

Exercise 3.9.7. Let p be an odd prime and x, y, and z pairwise coprime, positive integers.

(a)† Prove that $\frac{z^p - y^p}{z - y} \equiv py^{p-1} \pmod{z - y}$.

(b) Deduce that $\gcd(\frac{z^p - y^p}{z - y}, z - y) = 1$ or p.

(This problem is continued in exercise 7.10.6.)

Exercise 3.9.8. Suppose that $f(x) \in \mathbb{Z}[x]$ is monic and $f(0) = 1$. Prove that if $r \in \mathbb{Q}$ and $f(r) = 0$, then $r = 1$ or -1.

Exercise 3.9.9 (Another proof that $\sqrt{2}$ is irrational)**.** Suppose that $\sqrt{2} = a/b$ where a and b are coprime integers, so that $a^2 = 2b^2$.

(a) Prove that 3 cannot divide b, and so let $c \equiv a/b \pmod 3$.

(b) Prove that $c^2 \equiv 2 \pmod 3$, and therefore obtain a contradiction

Exercise 3.9.10.‡ (a) Prove that $\sqrt{2} + \sqrt{3}$ is irrational.

(b) Prove that $\sqrt{a} + \sqrt{b}$ is irrational unless a and b are both squares of integers.

Exercise 3.9.11. Suppose that d is an integer and $\sqrt{d}$ is rational.

(a) Show that there exists an integer m such that $\sqrt{d} - m = p/q$ where $0 \le p < q$ and $(p, q) = 1$.

(b) If $p \neq 0$, show that $\sqrt{d} + m = Q/p$ for some integer Q.

(c) Use (a) and (b) to establish a contradiction when $p \neq 0$.

(d) Deduce that $d = m^2$.

Exercise 3.9.12.† In this question we prove that if N can be represented by $ax + by$, then it can be represented properly. Let $A = a/(a, b)$ and $B = b/(a, b)$. Theorem 3.5 states that if $N = ar + bs$, then all solutions to $am + bn = N$ take the form $m = r + kB, n = s - kA$ for some integer k.

(a) Prove that $\gcd(m, n)$ divides N.

(b) Prove that at least one of A and B is not divisible by p, for each prime p.

(c) Prove that if $p \nmid A$, then there exists a residue class $k_p \pmod p$ such that $p | s - kA$ if and only if $k \equiv k_p \pmod p$. Therefore deduce that $p \nmid s - kA$ if $k \equiv k_p + 1 \pmod p$. Note an analogous result if $p | A$ (in which case $p \nmid B$).

(d) Deduce that there exists an integer k such that, for all primes p dividing N, either p does not divide $r + kB$ or p does not divide $s - kA$ (or both).

(e) Deduce that if $m = r + kB$ and $n = s - kA$, then N is properly represented by $am + bn$.

Exercise 3.9.13. Prove the following version of the local-global principle for linear equations (exercise 3.6.4): Let a, b, c be given integers. There are solutions in integers m, n to $am + bn = c$ if and only if for all prime powers p^e (where p is prime and e is an integer ≥ 1) there exist residue classes $u, v \pmod{p^e}$ for which $au + bv \equiv c \pmod{p^e}$.

Exercise 3.9.14. Find all solutions to $5a + 7b = 211$ where a and b are positive integers.

Exercise 3.9.15. Suppose that $f(x) \in \mathbb{Z}[x]$ and m and n are coprime integers.

(a) Prove that there exist integers a and b for which $f(a) \equiv 0 \pmod m$ and $f(b) \equiv 0 \pmod n$ if and only if there exists an integer c for which $f(c) \equiv 0 \pmod{mn}$, and show that we may take $c \equiv a \pmod m$ and $c \equiv b \pmod n$.

(b) Suppose that $p_1 < p_2 < \cdots < p_k$ are primes. Prove that there exist integers $a_1, \dots, a_k$ such that $f(a_i) \equiv 0 \pmod{p_i}$ for $1 \le i \le k$ if and only if there exists an integer a such that $f(a) \equiv 0 \pmod{p_1 p_2 \dots p_k}$.

Exercise 3.9.16.† Suppose that m and n are coprime integers.

(a) Prove that for any integer c there exist integers a and b for which $\frac{c}{mn} = \frac{a}{m} + \frac{b}{n}$.

(b) Prove that there are (unique) positive integers a and b for which $\frac{1}{mn} = \frac{a}{m} + \frac{b}{n} - 1$.

Exercise 3.9.17. Let m and n be given positive integers.

(a) Prove that for any integers a and b there exists an integer c for which $\frac{a}{m} + \frac{b}{n} = \frac{c}{L}$ where $L = \operatorname{lcm}[m, n]$.
For the denominators 3 and 6, with $L = 6$, we have the example $\frac{1}{3} + \frac{1}{6} = \frac{1}{2}$, a case in which the sum has a denominator smaller than L when written as a reduced fraction. However $\frac{1}{3} + \frac{5}{6} = \frac{7}{6}$ so there are certainly examples with these denominators for which the sum has denominator L.

(b)† Show that $\operatorname{lcm}[m, n]$ is the smallest positive integer L such that for all integers a and b we can write $\frac{a}{m} + \frac{b}{n}$ as a fraction with denominator L. (This is why $\operatorname{lcm}[m, n]$ is sometimes called the *lowest* (or *least*) *common denominator* of the fractions $1/m$ and $1/n$.)

(c)† Show that if $\frac{a}{m}$ and $\frac{b}{n}$ are reduced fractions whose sum has denominator less than L, then there must exist a prime power p^e such that $p^e \| m$ and $p^e \| n$ for which p^{e+1} divides $an + bm$.

Appendix 3A. Factoring binomial coefficients and Pascal's triangle modulo p

3.10. The prime powers dividing a given binomial coefficient

Exercise 3.10.1. Write $n = n_0 + n_1 p + \cdots + n_d p^d$ in base p so that each $n_j \in \{0, 1, \ldots, p-1\}$.
(a) Prove that $[n/p^k] = (n - (n_0 + n_1 p + \cdots + n_{k-1}p^{k-1}))/p^k$.
The *sum of the digits of n in base p* is defined to be $s_p(n) := n_0 + n_1 + \cdots + n_d$.
(b) Prove that the exact power of prime p that divides $n!$ is $\frac{n - s_p(n)}{p-1}$.

Exercise 3.10.2. State, with proof, the analogy to Kummer's Theorem for trinomial coefficients $n!/(a!b!c!)$ where $a + b + c = n$.

Exercise 3.10.3. Prove that if $0 \le k \le n$, then $\binom{n}{k}$ divides $\operatorname{lcm}[m : \ m \le n]$.

3.11. Pascal's triangle modulo 2

Exercise 3.11.1. Deduce that there are 2^k odd entries in the nth row of Pascal's triangle, where $k = s_2(n)$, the number of 1's in the binary expansion of n.

Exercise 3.11.2.† Show that the nth row of Pascal's triangle mod 2, considered as a binary number, is given by $\prod_{j=0}^{k} F_{n_j}$, where $n = 2^{n_0} + 2^{n_1} + \cdots + 2^{n_k}$, with $0 \le n_0 < n_1 < \cdots < n_k$ (i.e., the binary expansion of n).[1]

Appendix 3B. Solving linear congruences

3.12. Composite moduli

3.13. Solving linear congruences with several unknowns

3.14. The Chinese Remainder Theorem in general

Exercise 3.14.1. Prove that $\operatorname{lcm}[\gcd(m, n_j) : \ 1 \le j \le k] \ = \ \gcd(m, \operatorname{lcm}[n_j : \ 1 \le j \le k])$.

Exercise 3.14.2. Find all integers n satisfying $13n \equiv 407 \pmod{175}$ and $55n \equiv 29 \pmod{63}$.

Exercise 3.14.3. Suppose that integer $m \ge 0$ is given. Prove that there exist infinitely many integers n such that $n + j$ is divisible by $m + j$ for $j = 1, 2, \ldots, 100$.

Appendix 3C. Groups and rings

3.15. A direct sum

Exercise 3.15.1. Verify that a direct sum of two groups indeed forms a group.

Exercise 3.15.2.† Give an example of an additive group G and a subgroup H for which G is not isomorphic with $H \oplus G/H$.

[1] An m-sided regular polygon with m odd is constructible with ruler and compass (see section 0.18 of appendix 0G) if and only if m is the product of distinct Fermat primes. Therefore the integers m created here include all of the odd m-sided, constructible, regular polygons.

3.16. The structure of finite abelian groups

Appendix 3D. Unique factorization revisited

3.17. The Fundamental Theorem of Arithmetic, clarified

Exercise 3.17.1. Prove that the numbers $(3+2\sqrt{2})^k$ with $k = 1, 2, 3, \ldots$ are distinct units in $\mathbb{Z}[\sqrt{2}]$.

Exercise 3.17.2. Let R be a set of numbers containing 1 which is closed under multiplication. Prove that the units of R form a group.

Exercise 3.17.3. Let $f(x)$ be the minimum polynomial for $u \in R$.
(a) Prove that $x^d f(1/x)$ is the minimum polynomial for $1/u$.
(b) Deduce that u is a unit if and only if $f(0)$ equals 1 or -1.

3.18. When unique factorization fails

Exercise 3.18.1. The set of positive integers, $\mathcal{F}$, which are $\equiv 1 \pmod 4$, is closed under multiplication and contains 1. Note that 21 is irreducible in $\mathcal{F}$, despite not being prime in the positive integers. Show that factorization into irreducibles in not unique in $\mathcal{F}$.

Exercise 3.18.2 (Proof of Proposition 3.18.1)**.** Let's suppose that rational prime $p = (a+b\sqrt{-5})(c+d\sqrt{-5})$ with $(a,b) = (c,d) = 1$.
(a) By studying the coefficient of the imaginary part, prove that $c + d\sqrt{-5} = \pm(a - b\sqrt{-5})$.
(b) Deduce that $p = a^2 + 5b^2$ and that this is impossible for $p = 2$ and $p = 3$. Deduce that 2 and 3 are irreducible in R.
(c) Now assume that $1 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Multiply this with its complex conjugate to prove that $6 = (a^2 + 5b^2)(c^2 + 5d^2)$.
(d) Deduce that one of a^2+5b^2 and c^2+5d^2 equals 1, and therefore either $a+b\sqrt{-5}$ or $c+d\sqrt{-5}$ is a unit. Deduce that $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible in R.

3.19. Defining ideals and factoring

Exercise 3.19.1. Prove that if $I_R(\alpha) = I_R(\beta)$, then $\beta = u\alpha$ for some unit $u \in R$.

Exercise 3.19.2. Prove that every Euclidean domain (as defined in section 2.12 of appendix 2B) is a principal ideal domain.

Exercise 3.19.3. Prove that if $\alpha, \beta \in I_R$ and $r, s \in R$, then the linear combination $r\alpha + s\beta \in I_R$.

Exercise 3.19.4. Prove that if $a_1, \ldots, a_k \in R$, then $I_R(a_1, \ldots, a_k)$ is a ring.

3.20. Bases for ideals in quadratic fields

Exercise 3.20.1. Let I be an ideal of $\mathbb{Z}[\sqrt{d}]$, and let s be the smallest positive integer for which there is some $r + s\sqrt{d} \in I$.
(a) Prove that if $u + v\sqrt{d} \in I$, then s divides v.
(b)† Deduce that there exists an integer m for which $I = I_{\mathbb{Z}}(r + s\sqrt{d}, m)$.
(c) Prove that s divides both r and m, and so deduce the claimed form of the ideal.
(d) Prove that a divides $b^2 - d$.

Exercise 3.20.2. Let $R = \mathbb{Z}[\sqrt{d}]$ where d is a squarefree integer. Let $I = I(b + \sqrt{d}, a)$ where a divides $b^2 - d$.

(a) Prove that I is principal if and only if $|a| = 1$ or $|b^2 - d|$.
(b) Let $I^c := I(b - \sqrt{d}, a)$. Prove that $I \cdot I^c = (a)J$ where J is a principal ideal dividing (2).
(c) Prove that I is a prime ideal if and only if I^c is a prime ideal.
(d) Prove that if I is a non-principal prime ideal, then $I \cdot I^c = (p)$ where p is a prime number.

Appendix 3E. Gauss's approach

3.21. Gauss's approach to Euclid's Lemma

Appendix 3F. Fundamental theorems and factoring polynomials

3.22. The number of distinct roots of polynomials

Exercise 3.22.1 (Euclid's Lemma for polynomials)**.** Suppose that $\gcd(f(x), g(x))_{\mathbb{C}[x]} = 1$ and $f(x)$ divides $g(x)h(x)$. Deduce that $f(x)$ divides $h(x)$.

Exercise 3.22.2. (a) Deduce that every irreducible polynomial in $\mathbb{C}[x]$ has degree one.
(b) Prove that the set of d roots of $f(x)$ is unique.
(c) Prove that every irreducible polynomial in $\mathbb{R}[x]$ has degree one or two.

Exercise 3.22.3. Show that if α has minimal polynomial $f(x)$ and β is another root of $f(x)$, then $f(x)$ is also the minimum polynomial for β.

3.23. Interpreting resultants and discriminants

3.24. Other approaches to resultants and gcds

Exercise 3.24.1. Suppose that $f(x) \in \mathbb{Z}[x]$.
(a) Show that if f has an integer root n, then $f(n) \equiv 0 \pmod{m}$ for any integer m.
(b) Suppose that f has a rational root r/s, where r and s are coprime integers. Show that if $(s, m) = 1$, then there exists an integer n such that $f(n) \equiv 0 \pmod{m}$.
(c) For each integer m give an example of a polynomial f which has a rational root r/s with $(r, s) = 1$, but for which there does not exist an integer n such that $f(n) \equiv 0 \pmod{m}$.

Exercise 3.24.2. Suppose that $f(x) \in \mathbb{Z}[x]$ has degree d, and let $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ with $\alpha\delta - \beta\gamma = 1$.
(a) Show that $f(x)$ is irreducible if and only if $x^d f(1/x)$ is irreducible.
(b) Show that $f(x)$ is irreducible if and only if $(\gamma x + \delta)^d f(\frac{\alpha x + \beta}{\gamma x + \delta})$ is irreducible. (Remark: The easy way to prove this is to know that all such transformations can be given as a composition of the transformations $z \to z \pm 1$ and $z \to -1/z$ as we saw in section 1.10.)

Exercise 3.24.3.
(a) Give examples of cubic polynomials in $\mathbb{Z}[x]$ with no roots in $\mathbb{Z}$.
(b) Give examples of cubic polynomials in $\mathbb{Z}[x]$ with all three roots in $\mathbb{Z}$.
(c) Give examples of cubic polynomials in $\mathbb{Z}[x]$ with exactly one root in $\mathbb{Z}$.
(d) Prove that there are no examples with precisely two roots in $\mathbb{Z}$.
(e) Answer these same questions for cubic polynomials when $\mathbb{Z}$ is replaced by $\mathbb{Z}/p\mathbb{Z}$ for some odd prime p.

Appendix 3G. Open problems

3.25. The Frobenius postage stamp problem, II

Exercise 3.25.1. Let a and b be positive integers with $g = \gcd(a,b)$. Prove that $ab/g - a - b$ is the largest integer, divisible by g, that is not represented as $am + bn$ with $m, n \geq 0$.

Exercise 3.25.2. Let a and b be positive coprime integers. Suppose that $r = ma + nb$ for some integers m, n in the ranges $1 \leq m \leq b-1$ and $1 \leq n \leq a-1$.
(a) Prove that r is the smallest integer in $\mathcal{P}(a,b)$ which is $\equiv r \pmod{ab}$.
(b) What is the smallest integer $s \in \mathcal{P}(a,b)$ which is $\equiv -r \pmod{ab}$?
(c) Show that exactly one of r and s is $< ab$, and deduce that if $1 \leq N \leq ab$ where $a \nmid N$ and $b \nmid N$, then exactly one of N and $ab - N$ belongs to $\mathcal{P}(a,b)$.
(d) Show that there are exactly $\frac{1}{2}(a-1)(b-1)$ elements of $\mathcal{E}(a,b)$.

Exercise 3.25.3. (This continues from exercise 1.16.2.) An integer n is *powerful* if p^2 divides n whenever prime p divides n. Prove that we can write any powerful integer n as $n = a^2b^3$ where a and b are integers.

Exercise 3.25.4. Let a and b be positive coprime integers and select r and s in the ranges $1 \leq r \leq b-1$ and $1 \leq s \leq a-1$ so that $ar \equiv 1 \pmod{b}$ and $bs \equiv 1 \pmod{a}$. Prove that there are $\frac{N}{ab} + 1 - \{\frac{rN}{b}\} - \{\frac{sN}{a}\}$ representations of N as $N = ma + nb$ with integers $m, n \geq 0$.

Exercise 3.25.5. Suppose that $a_1, \dots, a_k$ are positive integers for which $\gcd(a_1, \dots, a_k) = 1$. Let

$$\mathcal{P}(a_1, \dots, a_k) := \{a_1n_1 + \cdots + a_kn_k : \ n_1, \dots, n_k \in \mathbb{Z}, \ n_1, \dots, n_k \geq 0\}.$$

(a) Prove that there exists an integer N such that every integer $\geq N$ belongs to $\mathcal{P}(a_1, \dots, a_k)$.
(b) Show that we may take $N = (k-1)\ \mathrm{lcm}[a_1, \dots, a_k]$.

3.26. Egyptian fractions for $3/b$

Exercise 3.26.1. Fix integer $a \geq 3$. Suppose that b is a prime. Prove that a/b can be written as the sum of two distinct Egyptian fractions if and only if $b \equiv -1 \pmod{a}$.

Exercise 3.26.2. Suppose that a and b are coprime positive integers. Prove that we have a solution to $\frac{a}{b} = \frac{1}{m} + \frac{1}{n}$ with $(m,n) = 1$ if and only if $a^2 - 4b$ is the square of an integer.

3.27. The $3x+1$ conjecture

Exercise 3.27.1. Let $x_0 = 2^k m - 1$. Suppose that the iterates of the modified $3x+1$ algorithm go $x_0 \to y_1 \to x_1 \to y_2 \to x_2 \to \dots$.
(a) Prove that $x_j = 3^j 2^{k-j} m - 1$ for $j = 0, 1, \dots, k$.
(b) Deduce that there exist integers x_0 such that there is an nth iterate x_n for which x_n/x_0 is arbitrarily large.

Exercise 3.27.2. Prove that $2^k \| N$ if and only if $N \equiv 2^k \pmod{2^{k+1}}$.