two integers a, b is odd and the other is even. We compute the congruence modulo 4, finding that $a^2 + 5b^2 \equiv 1$ (modulo 4). Hence $p \equiv 1$ (modulo 4) in this case. If $a^2 + 5b^2 = 2p$, we compute the congruences modulo 8. Since $p \equiv 1$ or 3 (modulo 4), we know that $2p \equiv 2$ or 6 (modulo 8). Any square is congruent 0, 1, or 4 (modulo 8). Hence $5b^2 \equiv 0, 5$, or 4 (modulo 8), which shows that $a^2 + 5b^2$ can not be congruent to 2 (modulo 8). Thus $p \equiv 3$ (modulo 4) in this case. We have therefore proved the following lemma:

(12.9) **Lemma.** Let p be an odd prime. Assume that the congruence $x^2 \equiv -5$ (modulo p) has a solution. Then $x^2 + 5y^2 = p$ has an integer solution if $p \equiv 1$ (modulo 4), and $x^2 + 5y^2 = 2p$ has an integer solution if $p \equiv 3$ (modulo 4).

There remains finally the problem of characterizing the odd primes p such that the congruence $x^2 \equiv -5$ has a solution modulo p. This is done by means of the amazing *Quadratic Reciprocity Law*, which asserts that $x^2 \equiv 5$ (modulo p) has a solution if and only if $x^2 \equiv p$ (modulo 5) has one! And the second congruence has a solution if and only if $p \equiv \pm 1$ (modulo 5). Combining this with the previous lemma and with the fact that -1 is a square modulo 5, we find:

(12.10) **Theorem.** Let p be an odd prime. The equation $x^2 + 5y^2 = p$ has an integer solution if and only if $p \equiv 1$ (modulo 4) and $p \equiv \pm 1$ (modulo 5). □

Nullum vero dubium nobis esse videtur,
quin multa eaque egregia in hoc genere adhuc lateant
in quibus alii vires suas exercere possint.

Karl Friedrich Gauss

EXERCISES

1. Factorization of Integers and Polynomials

1. Let a, b be positive integers whose sum is a prime p. Prove that their greatest common divisor is 1.
2. Define the greatest common divisor of a set of n integers, and prove its existence.
3. Prove that if d is the greatest common divisor of $a_1, \ldots, a_n$, then the greatest common divisor of $a_1/d, \ldots, a_n/d$ is 1.
4. **(a)** Prove that if n is a positive integer which is not a square of an integer, then $\sqrt{n}$ is not a rational number.
   (b) Prove the analogous statement for nth roots.
5. **(a)** Let a, b be integers with $a \neq 0$, and write $b = aq + r$, where $0 \leq r < |a|$. Prove that the two greatest common divisors (a, b) and (a, r) are equal.
   (b) Describe an algorithm, based on (a), for computing the greatest common divisor.

(c) Use your algorithm to compute the greatest common divisors of the following: (a) 1456, 235, (b) 123456789, 135792468.

6. Compute the greatest common divisor of the following polynomials: $x^3 - 6x^2 + x + 4$, $x^5 - 6x + 1$.

7. Prove that if two polynomials f, g with coefficients in a field F factor into linear factors in F, then their greatest common divisor is the product of their common linear factors.

8. Factor the following polynomials into irreducible factors in $\mathbb{F}_p[x]$.
(a) $x^3 + x + 1, p = 2$ **(b)** $x^2 - 3x - 3, p = 5$ **(c)** $x^2 + 1, p = 7$

9. Euclid proved that there are infinitely many prime integers in the following way: If $p_1, \ldots, p_k$ are primes, then any prime factor p of $n = (p_1 \cdots p_n) + 1$ must be different from all of the p_i.
(a) Adapt this argument to show that for any field F there are infinitely many monic irreducible polynomials in $F[x]$.
(b) Explain why the argument fails for the formal power series ring $F[[x]]$.

10. *Partial fractions for integers:*
(a) Write the fraction $r = 7/24$ in the form $r = a/8 + b/3$.
(b) Prove that if $n = uv$, where u and v are relatively prime, then every fraction $r = m/n$ can be written in the form $r = a/u + b/v$.
(c) Let $n = n_1 n_2 \cdots n_k$ be the factorization of an integer n into powers of distinct primes: $n_i = p_i^{e_i}$. Prove that every fraction $r = m/n$ can be written in the form $r = m_1/n_1 + \cdots + m_k/n_k$.

11. *Chinese Remainder Theorem:*
(a) Let n, m be relatively prime integers, and let a, b be arbitrary integers. Prove that there is an integer x which solves the simultaneous congruence $x \equiv a$ (modulo m) and $x \equiv b$ (modulo n).
(b) Determine all solutions of these two congruences.

12. Solve the following simultaneous congruences.
(a) $x \equiv 3$ (modulo 15), $x \equiv 5$ (modulo 8), $x \equiv 2$ (modulo 7).
(b) $x \equiv 13$ (modulo 43), $x \equiv 7$ (modulo 71).

13. *Partial fractions for polynomials:*
(a) Prove that every rational function in $\mathbb{C}(x)$ can be written as sum of a polynomial and a linear combination of functions of the form $1/(x - a)^i$.
(b) Find a basis for $\mathbb{C}(x)$ as vector space over $\mathbb{C}$.

***14.** Let F be a subfield of $\mathbb{C}$, and let $f \in F[x]$ be an irreducible polynomial. Prove that f has no multiple root in $\mathbb{C}$.

15. Prove that the greatest common divisor of two polynomials f and g in $\mathbb{Q}[x]$ is also their greatest common divisor in $\mathbb{C}[x]$.

16. Let a and b be relatively prime integers. Prove that there are integers m, n such that $a^m + b^n \equiv 1$ (modulo ab).

2. Unique Factorization Domains, Principal Ideal Domains, and Euclidean Domains

1. Prove or disprove the following.
(a) The polynomial ring $\mathbb{R}[x, y]$ in two variables is a Euclidean domain.
(b) The ring $\mathbb{Z}[x]$ is a principal ideal domain.

2. Prove that the following rings are Euclidean domains.
   (a) $\mathbb{Z}[\zeta]$, $\zeta = e^{2\pi i/3}$ **(b)** $\mathbb{Z}[\sqrt{-2}]$.
3. Give an example showing that division with remainder need not be unique in a Euclidean domain.
4. Let m, n be two integers. Prove that their greatest common divisor in $\mathbb{Z}$ is the same as their greatest common divisor in $\mathbb{Z}[i]$.
5. Prove that every prime element of an integral domain is irreducible.
6. Prove Proposition (2.8), that a domain R which has existence of factorizations is a unique factorization domain if and only if every irreducible element is prime.
7. Prove that in a principal ideal domain R, every pair a, b of elements, not both zero, has a greatest common divisor d, with these properties:
   (i) $d = ar + bs$, for some $r, s \in R$;
   (ii) d divides a and b;
   (iii) if $e \in R$ divides a and b, it also divides d.
   Moreover, d is determined up to unit factor.
8. Find the greatest common divisor of $(11 + 7i, 18 - i)$ in $\mathbb{Z}[i]$.
9. **(a)** Prove that $2, 3, 1 \pm \sqrt{-5}$ are irreducible elements of the ring $R = \mathbb{Z}[\sqrt{-5}]$ and that the units of this ring are ± 1.
   (b) Prove that existence of factorizations is true for this ring.
10. Prove that the ring $\mathbb{R}[[t]]$ of formal real power series is a unique factorization domain.
11. **(a)** Prove that if R is an integral domain, then two elements a, b are associates if and only if they differ by a unit factor.
    ***(b)** Give an example showing that (a) is false when R is not an integral domain.
12. Let R be a principal ideal domain.
    (a) Prove that there is a *least common multiple* $[a, b] = m$ of two elements which are not both zero such that a and b divide m, and that if a, b divide an element $r \in R$, then m divides r. Prove that m is unique up to unit factor.
    (b) Denote the greatest common divisor of a and b by (a, b). Prove that $(a, b)[a, b]$ is an associate of ab.
13. If a, b are integers and if a divides b in the ring of Gauss integers, then a divides b in $\mathbb{Z}$.
14. **(a)** Prove that the ring R (2.4) obtained by adjoining 2^k-th roots x_k of x to a polynomial ring is the union of the polynomial rings $F[x_k]$.
    (b) Prove that there is no factorization of x_1 into irreducible factors in R.
15. By a *refinement* of a factorization $a = b_1 \cdots b_k$ we mean the expression for a obtained by factoring the terms b_i. Let R be the ring (2.4). Prove that any two factorizations of the same element $a \in R$ have refinements, all of whose factors are associates.
16. Let R be the ring $F[u, v, y, x_1, x_2, x_3, \ldots]/(x_1 y = uv, x_2^2 = x_1, x_3^2 = x_2, \ldots)$. Show that u, v are irreducible elements in R but that the process of factoring uv need not terminate.
17. Prove Proposition (2.9) and Corollary (2.10).
18. Prove Proposition (2.11).
19. Prove that the factorizations (2.22) are prime in $\mathbb{Z}[i]$.
20. The discussion of unique factorization involves only the multiplication law on the ring R, so it ought to be possible to extend the definitions. Let S be a commutative semigroup, meaning a set with a commutative and associative law of composition and with an iden-

tity. Suppose the Cancellation Law holds in S: If $ab = ac$ then $b = c$. Make the appropriate definitions so as to extend Proposition (2.8) to this situation.

*21. Given elements $v_1, \ldots v_n$ in $\mathbb{Z}^2$, we can define a semigroup S as the set of all linear combinations of $(v_1, \ldots, v_n)$ with nonnegative integer coefficients, the law of composition being *addition*. Determine which of these semigroups has unique factorization.

3. Gauss's Lemma

1. Let a, b be elements of a field F, with $a \neq 0$. Prove that a polynomial $f(x) \in F[x]$ is irreducible if and only if $f(ax + b)$ is irreducible.
2. Let $F = \mathbb{C}(x)$, and let $f, g \in \mathbb{C}[x, y]$. Prove that if f and g have a common factor in $F[y]$, then they also have a common factor in $\mathbb{C}[x, y]$.
3. Let f be an irreducible polynomial in $\mathbb{C}[x, y]$, and let g be another polynomial. Prove that if the variety of zeros of g in $\mathbb{C}^2$ contains the variety of zeros of f, then f divides g.
4. Prove that two integer polynomials are relatively prime in $\mathbb{Q}[x]$ if and only if the ideal they generate in $\mathbb{Z}[x]$ contains an integer.
5. Prove Gauss's Lemma without reduction modulo p, in the following way: Let a_i be the coefficient of lowest degree i of f which is not divisible by p. So p divides a_ν if $\nu < i$, but p does not divide a_i. Similarly, let b_j be the coefficient of lowest degree of g which is not divisible by p. Prove that the coefficient of h of degree $i + j$ is not divisible by p.
6. State and prove Gauss's Lemma for Euclidean domains.
7. Prove that an integer polynomial is primitive if and only if it is not contained in any of the kernels of the maps (3.2).
8. Prove that $\det\begin{bmatrix} x & y \\ z & w \end{bmatrix}$ is irreducible in the polynomial ring $\mathbb{C}[x, y, z, w]$.
9. Prove that the kernel of the homomorphism $\mathbb{Z}[x] \longrightarrow \mathbb{R}$ sending $x \rightsquigarrow 1 + \sqrt{2}$ is a principal ideal, and find a generator for this ideal.
10. (a) Consider the map ψ: $\mathbb{C}[x, y] \longrightarrow \mathbb{C}[t]$ defined by $f(x, y) \rightsquigarrow f(t^2, t^3)$. Prove that its kernel is a principal ideal, and that its image is the set of polynomials $p(t)$ such that $p'(0) = 0$.
    (b) Consider the map φ: $\mathbb{C}[x, y] \longrightarrow \mathbb{C}[t]$ defined by $f(x, y) \rightsquigarrow (t^2 - t, t^3 - t^2)$. Prove that $\ker \varphi$ is a principal ideal, and that its image is the set of polynomials $p(t)$ such that $p(0) = p(1)$. Give an intuitive explanation in terms of the geometry of the variety $\{f = 0\}$ in $\mathbb{C}^2$.

4. Explicit Factorization of Polynomials

1. Prove that the following polynomials are irreducible in $\mathbb{Q}[x]$.
   (a) $x^2 + 27x + 213$ (b) $x^3 + 6x + 12$ (c) $8x^3 - 6x + 1$ (d) $x^3 + 6x^2 + 7$
   (e) $x^5 - 3x^4 + 3$
2. Factor $x^5 + 5x + 5$ into irreducible factors in $\mathbb{Q}[x]$ and in $\mathbb{F}_2[x]$.
3. Factor $x^3 + x + 1$ in $\mathbb{F}_p[x]$, when $p = 2, 3, 5$.

4. Factor $x^4 + x^2 + 1$ into irreducible factors in $\mathbb{Q}[x]$.
5. Suppose that a polynomial of the form $x^4 + bx^2 + c$ is a product of two quadratic factors in $\mathbb{Q}[x]$. What can you say about the coefficients of these factors?
6. Prove that the following polynomials are irreducible.
   (a) $x^2 + x + 1$ in the field $\mathbb{F}_2$ **(b)** $x^2 + 1$ in $\mathbb{F}_7$ **(c)** $x^3 - 9$ in $\mathbb{F}_{31}$
7. Factor the following polynomials into irreducible factors in $\mathbb{Q}[x]$.
   (a) $x^3 - 3x - 2$ **(b)** $x^3 - 3x + 2$ **(c)** $x^9 - 6x^6 + 9x^3 - 3$
8. Let p be a prime integer. Prove that the polynomial $x^n - p$ is irreducible in $\mathbb{Q}[x]$.
9. Using reduction modulo 2 as an aid, factor the following polynomials in $\mathbb{Q}[x]$.
   (a) $x^2 + 2345x + 125$ **(b)** $x^3 + 5x^2 + 10x + 5$ **(c)** $x^3 + 2x^2 + 3x + 1$
   (d) $x^4 + 2x^3 + 2x^2 + 2x + 2$ **(e)** $x^4 + 2x^3 + 3x^2 + 2x + 1$
   (f) $x^4 + 2x^3 + x^2 + 2x + 1$ **(g)** $x^5 + x^4 - 4x^3 + 2x^2 + 4x + 1$
10. Let p be a prime integer, and let $f \in \mathbb{Z}[x]$ be a polynomial of degree $2n + 1$, say $f(x) = a_{2n+1}x^{2n+1} + \cdots + a_1x + a_0$. Suppose that $a_{2n+1} \not\equiv 0$ (modulo p), $a_0, a_1, \ldots, a_n \equiv 0$ (modulo p^2), $a_{n+1}, \ldots, a_{2n} \equiv 0$ (modulo p), $a_0 \not\equiv 0$ (modulo p^3). Prove that f is irreducible in $\mathbb{Q}[x]$.
11. Let p be a prime, and let $A \neq I$ be an $n \times n$ integer matrix such that $A^p = I$ but $A \neq I$. Prove that $n \geq p - 1$.
12. Determine the monic irreducible polynomials of degree 3 over $\mathbb{F}_3$.
13. Determine the monic irreducible polynomials of degree 2 over $\mathbb{F}_5$.
14. *Lagrange interpolation formula:*
    (a) Let $x_0, \ldots, x_d$ be distinct complex numbers. Determine a polynomial $p(x)$ of degree n which is zero at $x_1, \ldots, x_n$ and such that $p(x_0) = 1$.
    (b) Let $x_0, \ldots, x_d$; $y_0, \ldots, y_d$ be complex numbers, and suppose that the x_i are all different. There is a unique polynomial $g(x) \in \mathbb{C}[x]$ of degree $\leq d$, such that $g(x_i) = y_i$ for each $i = 0, \ldots, d$. Prove this by determining the polynomial g explicitly in terms of x_i, y_i.

*15. Use the Lagrange interpolation formula to give a method of finding all integer polynomial factors of an integer polynomial in a finite number of steps.

16. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a monic polynomial with integer coefficients, and let $r \in \mathbb{Q}$ be a rational root of $f(x)$. Prove that r is an integer.
17. Prove that the polynomial $x^2 + y^2 - 1$ is irreducible by the method of undetermined coefficients, that is, by studying the equation $(ax + by + c)(a'x + b'y + c') = x^2 + y^2 - 1$, where a, b, c, a', b', c' are unknown.

5. Primes in the Ring of Gauss Integers

1. Prove that every Gauss prime divides exactly one integer prime.
2. Factor 30 into primes in $\mathbb{Z}[i]$.
3. Factor the following into Gauss primes.
   (a) $1 - 3i$ **(b)** 10 **(c)** $6 + 9i$
4. Make a neat drawing showing the primes in the ring of Gauss integers in a reasonable size range.
5. Let π be a Gauss prime. Prove that π and $\overline{\pi}$ are associate if and only if either π is associate to an integer prime or $\pi\overline{\pi} = 2$.

6. Let R be the ring $\mathbb{Z}[\sqrt{3}]$. Prove that a prime integer p is a prime element of R if and only if the polynomial $x^2 - 3$ is irreducible in $\mathbb{F}_p[x]$.
7. Describe the residue ring $\mathbb{Z}[i]/(p)$ in each case.
   (a) $p = 2$ **(b)** $p \equiv 1$ (modulo 4) **(c)** $p \equiv 3$ (modulo 4)

*8. Let $R = \mathbb{Z}[\zeta]$, where $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$ is a complex cube root of 1. Let p be an integer prime $\neq 3$. Adapt the proof of Theorem (5.1) to prove the following.
   (a) The polynomial $x^2 + x + 1$ has a root in $\mathbb{F}_p$ if and only if $p \equiv 1$ (modulo 3).
   (b) (p) is a prime ideal of R if and only if $p \equiv -1$ (modulo 3).
   (c) p factors in R if and only if it can be written in the form $p = a^2 + ab + b^2$, for some integers a, b.
   (d) Make a drawing showing the primes of absolute value ≤ 10 in R.

6. Algebraic Integers

1. Is $\frac{1}{2}(1 + \sqrt{3})$ an algebraic integer?
2. Let α be an algebraic integer whose monic irreducible polynomial over $\mathbb{Z}$ is $x^n + a_{n-1}n^{n-1} + \cdots + a_1x + a_0$, and let $R = \mathbb{Z}[\alpha]$. Prove that α is a unit in R if and only if $a_0 = \pm 1$.
3. Let d, d' be distinct square-free integers. Prove that $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d'})$ are different subfields of $\mathbb{C}$.
4. Prove that existence of factorizations is true in the ring of integers in an imaginary quadratic number field.
5. Let α be the real cube root of 10, and let $\beta = a + b\alpha + c\alpha^2$, with $a, b, c, \in \mathbb{Q}$. Then β is the root of a monic cubic polynomial $f(x) \in \mathbb{Q}[x]$. The irreducible polynomial for α over $\mathbb{Q}$ is $x^3 - 10$, and its three roots are α, $\alpha' = \zeta\alpha$, and $\alpha'' = \zeta^2\alpha$, where $\zeta = e^{2\pi i/3}$. The three roots of f are β, $\beta' = a + b\zeta\alpha + c\zeta^2\alpha^2$, and $\beta'' = a + b\zeta^2\alpha + c\zeta\alpha^2$, so $f(x) = (x - \beta)(x - \beta')(x - \beta'')$.
   (a) Determine f by expanding this product. The terms involving α and α^2 have to cancel out, so they need not be computed.
   (b) Determine which elements β are algebraic integers.
6. Prove Proposition (6.17).
7. Prove that the ring of integers in an imaginary quadratic field is a maximal subring of $\mathbb{C}$ with the property of being a lattice in the complex plane.
8. **(a)** Let $S = \mathbb{Z}[\alpha]$, where α is a complex root of a monic polynomial of degree 2. Prove that S is a lattice in the complex plane.
   (b) Prove the converse: A subring S of $\mathbb{C}$ which is a lattice has the form given in (a).
9. Let R be the ring of integers in the field $\mathbb{Q}[\sqrt{d}]$.
   (a) Determine the elements $\alpha \in R$ such that $R = \mathbb{Z}[\alpha]$.
   (b) Prove that if $R = \mathbb{Z}[\alpha]$ and if α is a root of the polynomial $x^2 + bx + c$ over $\mathbb{Q}$, then the discriminant $b^2 - 4c$ is D (6.18).

7. Factorization in Imaginary Quadratic Fields

1. Prove Proposition (7.3) by arithmetic.
2. Prove that the elements $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible elements of the ring $\mathbb{Z}[\sqrt{-5}]$.

3. Let $d = -5$. Determine whether or not the lattice of integer linear combinations of the given vectors is an ideal.
   (a) $(5, 1 + \delta)$ **(b)** $(7, 1 + \delta)$ **(c)** $(4 - 2\delta, 2 + 2\delta, 6 + 4\delta)$
4. Let A be an ideal of the ring of integers R in an imaginary quadratic field. Prove that there is a lattice basis for A one of whose elements is a positive integer.
5. Let $R = \mathbb{Z}[\sqrt{-5}]$. Prove that the lattice spanned by $(3, 1 + \sqrt{-5})$ is an ideal in R, determine its nonzero element of minimal absolute value, and verify that this ideal has the form (7.9), Case 2.
6. With the notation of (7.9), show that if α is an element of R such that $\frac{1}{2}(\alpha + \alpha\delta)$ is also in R, then $(\alpha, \frac{1}{2}(\alpha + \alpha\delta))$ is a lattice basis of an ideal.
7. For each ring R listed below, use the method of Proposition (7.9) to describe the ideals in R. Make a drawing showing the possible shapes of the lattices in each case.
   (a) $R = \mathbb{Z}[\sqrt{-3}]$ **(b)** $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-3})]$ **(c)** $R = \mathbb{Z}[\sqrt{-6}]$ **(d)** $R = \mathbb{Z}[\sqrt{-7}]$
   (e) $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-7})]$ **(f)** $R = \mathbb{Z}[\sqrt{-10}]$
8. Prove that R is not a unique factorization domain when $d \equiv 2$ (modulo 4) and $d < -2$.
9. Let $d \leq -3$. Prove that 2 is not a prime element in the ring $\mathbb{Z}[\sqrt{d}]$, but that 2 is irreducible in this ring.

8. Ideal Factorization

1. Let $R = \mathbb{Z}[\sqrt{-6}]$. Factor the ideal (6) into prime ideals explicitly.
2. Let $\delta = \sqrt{-3}$ and $R = \mathbb{Z}[\delta]$. (This is not the ring of integers in the imaginary quadratic number field $\mathbb{Q}[\delta]$.) Let A be the ideal $(2, 1 + \delta)$. Show that $A\bar{A}$ is not a principal ideal, hence that the Main Lemma is not true for this ring.
3. Let $R = \mathbb{Z}[\sqrt{-5}]$. Determine whether or not 11 is an irreducible element of R and whether or not (11) is a prime ideal in R.
4. Let $R = \mathbb{Z}[\sqrt{-6}]$. Find a lattice basis for the product ideal AB, where $A = (2, \delta)$ and $B = (3, \delta)$.
5. Prove that $A \supset A'$ implies that $AB \supset A'B$.
6. Factor the principal ideal (14) into prime ideals explicitly in $R = \mathbb{Z}[\delta]$, where $\delta = \sqrt{-5}$.
7. Let P be a prime ideal of an integral domain R, and assume that existence of factorizations is true in R. Prove that if $a \in P$ then some irreducible factor of a is in P.

9. The Relation Between Prime Ideals of R and Prime Integers

1. Find lattice bases for the prime divisors of 2 and 3 in the ring of integers in (a) $\mathbb{Q}[\sqrt{-14}]$ and (b) $\mathbb{Q}[\sqrt{-23}]$.
2. Let $d = -14$. For each of the following primes p, determine whether or not p splits or ramifies in R, and if so, determine a lattice basis for a prime ideal factor of (p): $2, 3, 5, 7, 11, 13$.
3. **(a)** Suppose that a prime integer p remains prime in R. Prove that $R/(p)$ is then a field with p^2 elements.
   (b) Prove that if p splits in R, then $R/(p)$ is isomorphic to the product ring $\mathbb{F}_p \times \mathbb{F}_p$.

4. Let p be a prime which splits in R, say $(p) = P\bar{P}$, and let $\alpha \in P$ be any element which is not divisible by p. Prove that P is generated as an ideal by (p, α).
5. Prove Proposition (9.3b).
6. If $d \equiv 2$ or 3 (modulo 4), then according to Proposition (9.3a) a prime integer p remains prime in the ring of integers of $\mathbb{Q}[\sqrt{d}]$ if the polynomial $x^2 - d$ is irreducible modulo p.
   (a) Prove the same thing when $d \equiv 1$ (modulo 4) and $p \neq 2$.
   (b) What happens to $p = 2$ in this case?
7. Assume that $d \equiv 2$ or 3 (modulo 4). Prove that a prime integer p ramifies in R if and only if $p = 2$ or p divides d.
8. State and prove an analogue of problem 7 when d is congruent 1 modulo 4.
9. Let p be an integer prime which ramifies in R, and say that $(p) = P^2$. Find an explicit lattice basis for P. In which cases is P a principal ideal?
10. A prime integer might be of the form $a^2 + b^2 d$, with $a, b \in \mathbb{Z}$. Discuss carefully how this is related to the prime factorization of (p) in R.

*11. Prove Proposition (9.1).

10. Ideal Classes in Imaginary Quadratic Fields

1. Prove that the ideals A and A' are similar if and only if there is a nonzero ideal C such that AC and $A'C$ are principal ideals.
2. The estimate of Corollary (10.12) can be improved to $|\alpha|^2 \leq 2\Delta(L)/\sqrt{3}$, by studying lattice points in a circle rather than in an arbitrary centrally symmetric convex set. Work this out.
3. Let $R = \mathbb{Z}[\delta]$, where $\delta^2 = -6$.
   (a) Prove that the lattices $P = (2, \delta)$ and $Q = (3, \delta)$ are prime ideals of R.
   (b) Factor the principal ideal (6) into prime ideals explicitly in R.
   (c) Prove that the ideal classes of P and Q are equal.
   (d) The Minkowski bound for R is $[\mu] = 3$. Using this fact, determine the ideal class group of R.
4. In each case, determine the ideal class group and draw the possible shapes of the lattices.
   (a) $d = -10$ **(b)** $d = -13$ **(c)** $d = -14$ **(d)** $d = -15$ **(e)** $d = -17$
   (f) $d = -21$
5. Prove that the values of d listed in Theorem (7.7) have unique factorization.
6. Prove Lemma (10.13).
7. Derive Corollary (10.14) from Lemma (10.13).
8. Verify Table (10.24).

11. Real Quadratic Fields

1. Let $R = \mathbb{Z}[\delta]$, $\delta = \sqrt{2}$. Define a size function on R using the lattice embedding (11.2): $\sigma(a + b\delta) = a^2 - 2b^2$. Prove that this size function makes R into a Euclidean domain.
2. Let R be the ring of integers in a real quadratic number field, with $d \equiv 2$ or 3 (modulo 4). According to (6.14), R has the form $\mathbb{Z}[x]/(x^2 - d)$. We can also consider the ring $R' = \mathbb{R}[x]/(x^2 - d)$, which contains R as a subring.
   (a) Show that the elements of R' are in bijective correspondence with points of $\mathbb{R}^2$ in such a way that the elements of R correspond to lattice points.

(b) Determine the group of units of R'. Show that the subset U' of R' consisting of the points on the two hyperbolas $xy = \pm 1$ forms a subgroup of the group of units.
(c) Show that the group of units U of R is a discrete subgroup of U', and show that the subgroup U_0 of units which are in the first quadrant is an infinite cyclic group.
(d) What are the possible structures of the group of units U?

3. Let U_0 denote the group of units of R which are in the first quadrant in the embedding (11.2). Find a generator for U_0 when (a) $d = 3$, (b) $d = 5$.
4. Prove that if d is a square >1 then the equation $x^2 - y^2 d = 1$ has no solution except $x = \pm 1, y = 0$.
5. Draw a figure showing the hyperbolas and the units in a reasonable size range for $d = 3$.

12. Some Diophantine Equations

1. Determine the primes such that $x^2 + 5y^2 = 2p$ has a solution.
2. Express the assertion of Theorem (12.10) in terms of congruence modulo 20.
3. Prove that if $x^2 \equiv -5$ (modulo p) has a solution, then there is an integer point on one of the two ellipses $x^2 + 5y^2 = p$ or $2x^2 + 2xy + 3y^2 = p$.
4. Determine the conditions on the integers a, b, c such that the linear Diophantine equation $ax + by = c$ has an integer solution, and if it does have one, find all the solutions.
5. Determine the primes p such that the equation $x^2 + 2y^2 = p$ has an integer solution.
6. Determine the primes p such that the equation $x^2 + xy + y^2 = p$ has an integer solution.
7. Prove that if the congruence $x^2 \equiv -10$ (modulo p) has a solution, then the equation $x^2 + 10y^2 = p^2$ has an integer solution. Generalize.
8. Find all integer solutions of the equation $x^2 + 2 = y^3$.
9. Solve the following Diophantine equations.
(a) $y^2 + 10 = x^3$ (b) $y^2 + 1 = x^3$ (c) $y^2 + 2 = x^3$

Miscellaneous Problems

1. Prove that there are infinitely many primes congruent 1 modulo 4.
2. Prove that there are infinitely many primes congruent to -1 (modulo 6) by studying the factorization of the integer $p_1 p_2 \cdots p_r - 1$, where $p_1, \ldots, p_r$ are the first r primes.
3. Prove that there are infinitely many primes congruent to -1 (modulo 4).
4. (a) Determine the prime ideals of the polynomial ring $\mathbb{C}[x, y]$ in two variables.
(b) Show that unique factorization of ideals does not hold in the ring $\mathbb{C}[x, y]$.
5. Relate proper factorizations of elements in an integral domain to proper factorizations of principal ideals. Using this relation, state and prove unique factorization of ideals in a principal ideal domain.
6. Let R be a domain, and let I be an ideal which is a product of distinct maximal ideals in two ways, say $I = P_1 \cdots P_r = Q_1 \cdots Q_s$. Prove that the two factorizations are the same, except for the ordering of the terms.
7. Let R be a ring containing $\mathbb{Z}$ as a subring. Prove that if integers m, n are contained in a proper ideal of R, then they have a common integer factor > 1.

*8. (a) Let θ be an element of the group $\mathbb{R}^+/\mathbb{Z}^+$. Use the Pigeonhole Principle [Appendix (1.6)] to prove that for every integer n there is an integer $b \leq n$ such that $|b\theta| \leq 1/bn$.

(b) Show that for every real number r and every $\epsilon > 0$, there is a fraction m/n such that $|r - m/n| \leq \epsilon/n$.

(c) Extend this result to the complex numbers by showing that for every complex number α and every real number $\epsilon > 0$, there is an element of $\mathbb{Z}(i)$, say $\beta = (a + bi)/n$ with $a, b, n \in \mathbb{Z}$, such that $|\alpha - \beta| \leq \epsilon/n$.

(d) Let ϵ be a positive real number, and for each element $\beta = (a + bi)/n$ of $\mathbb{Q}(i)$, $a, b, n \in \mathbb{Z}$, consider the disc of radius ϵ/n about β. Prove that the interiors of these discs cover the complex plane.

(e) Extend the method of Proposition (7.9) to prove the finiteness of the class number for any imaginary quadratic field.

*9. (a) Let R be the ring of functions which are polynomials in $\cos t$ and $\sin t$, with real coefficients. Prove that $R \approx \mathbb{R}[x, y]/(x^2 + y^2 - 1)$.

(b) Prove that R is not a unique factorization domain.

*(c) Prove that $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$ is a principal ideal domain and hence a unique factorization domain.

*10. In the definition of a Euclidean domain, the size function σ is assumed to have as range the set of nonnegative integers. We could generalize this by allowing the range to be some other ordered set. Consider the product ring $R = \mathbb{C}[x] \times \mathbb{C}[y]$. Show that we can define a size function $R - \{0\} \longrightarrow S$, where S is the ordered set $\{0, 1, 2, 3, \ldots; \omega, \omega + 1, \omega + 2, \omega + 3, \ldots\}$, so that the division algorithm holds.

*11. Let φ: $\mathbb{C}[x, y] \longrightarrow \mathbb{C}[t]$ be a homomorphism, defined say by $x \rightsquigarrow x(t), y \rightsquigarrow y(t)$. Prove that if $x(t)$ and $y(t)$ are not both constant, then $\ker \varphi$ is a nonzero principal ideal.