Selected Hints for the Exercises

Chapter 1

6. Use Exercise 4.
8. Do it for the case $d = 1$ and then use Exercise 7 to do it in general.
9. Use Exercise 4.
15. Here is a generalization; a is an nth power iff $n \mid \text{ord}_p\, a$ for all primes p.
16. Use Exercise 15.
17. Use Exercise 15 to show that $a^2 = 2b^2$ implies that 2 is the square of an integer.
23. Begin by writing $4(a/2)^2 = (c - b)(c + b)$.
28. Show that $n^5 - n$ is divisible by 2, 3, and 5. Then use Exercise 9.
30. Let s be the largest integer such that $2^s \leq n$, and consider $\sum_{k=1}^{n} 2^{s-1}/k$. Show that this sum can be written in the form $a/b + \frac{1}{2}$ with b odd. Then use Exercise 29.
31. $2 = (1 + i)(1 - i) = -i(1 + i)^2$.
34. Since $\omega^2 = -1 - \omega$ we have $(1 - \omega)^2 = 1 - 2\omega + \omega^2 = -3\omega$, so $3 = -\omega^2(1 - \omega)^2$.

Chapter 2

1. Imitate the classical proof of Euclid.
2. Use $\text{ord}_p(a + b) \geq \min(\text{ord}_p\, a, \text{ord}_p\, b)$.
3. If $p_1, p_2, \ldots, p_t$ were all the primes, then $\phi(p_1 p_2 \cdots p_t) = 1$. Now use the formula for ϕ and derive a contradiction.
5. Consider $2^2 + 1$, $2^4 + 1$, $2^8 + 1, \ldots$. No prime that divides one of these numbers can divide any other, by the previous exercise.
6. Count! Consider the set of pairs (s, t) with $p^s t \leq n$.
12. In each case the summand is multiplicative. Hence evaluate first at prime powers and then use multiplicavity.

17. Use the formula for $\sigma(n)$.
20. If $d\,|\,n$, then n/d also divides n.
22. If $(t, n) = 1$, then $(n - t, n) = 1$, so you can pair those numbers relatively prime to n in such a way that the sum of each pair is n.

Chapter 3

1. Suppose that $p_1, p_2, \ldots, p_t$ are all congruent to -1 modulo 6. Consider $N = 6p_1p_2 \cdots p_t - 1$.
3. 10^k is congruent to 1 modulo 3 and 9 and congruent to $(-1)^k$ modulo 11.
5. If a solution exists, then $x^3 \equiv 2\ (7)$ has a solution. Show that it does not.
10. If n is not a prime power, write $n = ab$ with $(a, b) = 1$. If $n = p^s$ with $s > 1$, then $(n - 1)!$ is divisible by $p \cdot p^{s-1} = p^s = n$. If $n = p^2$ and $p \neq 2$; then $(n - 1)!$ is divisible by $p \cdot 2p = 2n$.
13. Show that $n^p \equiv n\ (p)$ for all n by induction. If $(n, p) = 1$, then one can cancel n and get Fermat's formula.
17. Let x_i be a solution to $f(x) \equiv 0\ (p_i^{a_i})$ and solve the system $x \equiv x_i\ (p_i^{a_i})$.
23. Since $i \equiv -1\ (1 + i)$, we have $a + bi \equiv a - b\ (1 + i)$. Write $a - b = 2c + d$, where $d = 0$ or 1. Then $a + ib \equiv d\ (1 + i)$.
25. Write $\alpha = 1 + \beta\lambda$, cube both sides and take congruence modulo λ^4 to get $\alpha^3 \equiv 1 + (\beta^3 - \omega^2\beta)\lambda^3\ (\lambda^4)$. Then show that the term in parentheses is divisible by λ.

Chapter 4

4. If $(-a)^n \equiv 1$, and n is even, then $p - 1\,|\,n$. If n is odd, then $p - 1\,|\,2n$, which implies that $2\,|\,n$ is a contradiction.
6. This is a bit tricky. If 3 is not a primitive element, show that 3 is congruent to a square. Use Exercise 4 to show there is an integer a such that $-3 \equiv a^2\ (p)$. Now solve $2u \equiv -1 + a(p)$ and show that u has order 3. This would imply that $p = 1\ (3)$, which cannot be true.
7. Use the fact that 2 is not a square modulo p.
9. See Exercise 22 of Chapter 2 and use the fact that $g^{(p-1)/2} \equiv -1\ (p)$ for a primitive root g.
11. Express the numbers between 1 and $p - 1$ as the powers of a primitive root and use the formula for the sum of a geometric progression.
14. If $(ab)^s = e$, then $a^{ns} = 1$, implying that $m\,|\,ns$. Thus $m\,|\,s$. Similarly, $n\,|\,s$. Thus $mn\,|\,s$.
18. Choose a primitive element (e.g., 2) and construct the elements of order 7.
22. Show first that $1 + a + a^2 \equiv 0\ (p)$.
23. Use Proposition 4.2.1.

Chapter 5

3. Use the identity $4(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$.
9. Using $k \equiv -(p - k)\ (p)$, show first that $2 \cdot 4 \cdot \ldots \cdot (p - 1) \equiv (-1)^{(p-1)/2} 1 \cdot 3 \cdot 5 \cdot \ldots \cdot p - 2\ (p)$.
10. Use Exercise 9.

13. If $x^4 - x^2 + 1 \equiv 0\ (p)$, then $(2x^2 - 1)^2 \equiv -3\ (p)$ and $(x^2 - 1)^2 \equiv -x^2\ (p)$. Conclude that $p = 1\ (3)$ and $p = 1\ (4)$ by using quadratic reciprocity.
18. Let $D = p_1 p_2 \cdots p_m$ and suppose that n is a nonresidue modulo p_1. Find a number b such that $b \equiv 1\ (p_i)$ and $b \equiv n\ (p_1)$ for $1 < i \le m$. Then use the definition of the Jacobi symbol to show that $(b/D) = -1$.
23. Since $s^2 + 1 = (s + i)(s - i)$, if p is prime in $\mathbb{Z}[i]$, then either $p \mid s + i$ $p \mid s - i$, but neither alternative is true.
26. To prove (b) notice that $a + b$ is odd, so from $2p = (a + b)^2 + (a - b)^2$ we see that $(2p/a + b) = 1$. Now use the properties of the Jacobi symbol.
29. It is useful to consider the cases $p \equiv 1\ (4)$ and $p \equiv 3\ (4)$ separately.
30. To evaluate the sum notice that $(n(n + 1)/p) = ((2n + 1)^2 - 1/p)$.

Chapter 6

1. Find an equation of degree 4.
2. If $a_0\alpha^s + a_1\alpha^{s-1} + \cdots + a_s = 0$, with $a_i \in \mathbb{Z}$, multiply both sides with a_0^{s-1} and conclude that $a_0\alpha$ is an algebraic integer.
3. Suppose that α and β satisfy monic equations with integer coefficients of degree m and n, respectively. Let γ be a root of $x^2 + \alpha x + \beta$ and show that the $\mathbb{Z}$ module generated by $\alpha^i\beta^j\gamma^k$, where $0 \le i < m$, $0 \le j < n$, and $k = 0$ or 1, is mapped into itself by γ.
10. Use $g_a = (a/p)g$ and the fact that $\sum_a (a/p) = 0$.
11. Remember that $1 + (t/p)$ is the number of solutions to $x^2 \equiv t\ (p)$ and that $\sum_t \zeta^t = 0$.
13. Use Exercise 12.
16. Show that otherwise $f'(\alpha) = 0$ and apply Proposition 6.1.7.
23. Use Exercise 4 to show that it is enough to show that $f(x)$ is irreducible in $\mathbb{Z}[x]$. Then write $f(x) = g(x)h(x)$, reduce modulo p, and use the fact that $F_p[x]$ is a unique factorization domain.

Chapter 7

3. Since $q \equiv 1\ (n)$, there are n solutions to $x^n = 1$. If $\beta^n = \alpha$, then the other solutions to $x^n = \alpha$ are given by $\gamma\beta$, where γ runs through the solutions of $x^n = 1$.
5. $q^n - 1 = (q - 1)(q^{n-1} + \cdots + q + 1)$. Since $q \equiv 1\ (n)$, we have $q^{n-1} + \cdots + q + 1 \equiv n \equiv 0\ (n)$. Thus $n(q - 1)$ divides $q^n - 1$.
7. Let $m = [K:F]$. α is a square in K iff $\alpha^{(q^m-1)/2} = 1$. If α is not a square in F, then $\alpha^{(q-1)/2} = -1$. Show that $\alpha^{(q^m-1)/2} = (-1)^m$. This formula yields the result.
9. Use the method of Exercise 7.
14. One can prove this by exactly the same method as for F_p. Alternatively, suppose that $q = p^m$. Let $f(x) \in F_p[x]$ be an irreducible of degree mn and let $g(x)$ be an irreducible factor of $f(x)$ in $F_q[x]$. Let α be a root of $g(x)$ and show that $F_q \subset F_p(\alpha)$. Conclude that $F_q(\alpha) = F_p(\alpha)$ and that $[F_q(\alpha):F_q] = n$. It follows that $g(x)$ has degree n.

15. If $x^n - 1$ splits into linear factors in E, where $[E:F] = f$, then E has q^f elements and $n \mid q^f - 1$ since the roots of $x^n - 1$ form a subgroup of E^* of order n.
23. If β is a root of $x^p - x - \alpha$, then so are $\beta + 1, \beta + 2, \ldots, \beta + (p - 1)$. Using this, one can show the statement about irreducibility. To prove the final assertion, notice that $\beta^p = \beta + \alpha$ implies that $\beta^{p^2} = \beta^p + \alpha^p = \beta + \alpha + \alpha^p$, etc. Thus $\beta^{p^n} = \beta + \mathrm{tr}(\alpha)$ and so $\beta \in F$ iff $\mathrm{tr}(\alpha) = 0$.

Chapter 8

1. Use the Corollary to Proposition 8.1.3 and Proposition 8.1.4.
4. Make the substitution $t = (k/2)(u + 1)$ and use Exercise 3.
6. It follows from Exercise 5 together with part (d) of Theorem 1, or directly from Exercise 4 by substituting $k = 1$.
8. Use Proposition 8.1.5 and imitate the proof of Exercise 3.
14. Use Proposition 8.3.3.
19. First show that the number of solutions is given by $p^{r-1} + J_0(\chi, \chi, \ldots, \chi)$, where χ is a character of order 2 and there are r components in J_0. Then use Proposition 8.5.1 and Theorem 3. Notice in particular that if r is odd, the answer is simply p^{r-1}.
28. For (a): Write
$$\sum_{x=1}^{p-1} x\chi(x) = \sum_{x=1}^{(p-1)/2} x\chi(x) + \sum_{x=1}^{(p-1)/2} (p - x)\chi(p - x).$$
For (b): Write
$$\sum_{x=1}^{p-1} x\chi(x) = \sum_{x=1}^{(p-1)/2} 2x\chi(2x) + \sum_{x=1}^{(p-1)/2} (p - 2x)\chi(p - 2x).$$
For (c) and (d): Equate (a) and (b).

Chapter 9

3. Use the fact that $N\gamma = a^2 - ab + b^2 \equiv 3(m + n) + 1\ (9)$.
4. Rewrite γ as $3(m + n) - 1 - 3n\lambda$. Thus $\gamma \equiv 3(m + n) - 1 (3\lambda)$.
5. Remember that $3 = -\omega^2\lambda^2$.
7. $2 + 3\omega$, $-7 - 3\omega$, and $-4 - 3\omega$.
10. $D/5D$ has 25 elements. Thus $x^{24} - 1$ factors completely into linear factors in D.
13. Use Exercise 9 to show that the elements listed represent all the cubes in $D/5D$.
15. Remember that every element in $D/\pi D$ is represented by a rational integer.
19. Use Exercise 18, the law of cubic reciprocity, and induction on the number of primary primes dividing γ.
23. Let $p = \pi\bar{\pi}$, where π is primary. By Exercise 15 $x^3 \equiv 3\ (p)$ is solvable iff $\chi_\pi(3) = 1$. By Exercise 5 $\chi_\pi(3) = \omega^{2n}$, where $\pi = a + b\omega$ and $b = 3n$. It follows that $x^3 \equiv 3\ (p)$ is solvable iff $9 \mid b$.

24. (c) Use cubic reciprocity with $\pi \equiv b\omega\,(a)$.
(d) Write $(a + b) = (a + b)\omega \cdot \omega^{-1}$ and note that $a + b\omega \equiv a(1 - \omega)\,(\pi)$.
25. (a) Use Exercise 18 and the corollary to Proposition 9.3.4 to show that $\chi_{a+b}(b) = 1$. Note that $\pi \equiv -b(1 - \omega)\,(a + b)$.
(b) $\chi_{a+b}(1 - \omega) = (\chi_{a+b}(1 - \omega)^2)^2$
$= (\chi_{a+b}(-3\omega))^2$ etc.
39. Combine Exercises 6 and 27 of Chapter 8 with Proposition 9.6.1.
40. See the hint to the previous exercise.
43. Use Exercise 23, Chapter 6.

Chapter 10

2. Map $[x_0, x_1, \ldots, x_{n-1}]$ to $[0, x_0, x_1, \ldots, x_{n-1}]$.
3. Since the number of points in $A^n(F)$ is q^n, the decomposition of $P^n(F)$ shows that the number of points in $P^n(F)$ is q^n plus the number of points in $P^{n-1}(F)$. One now proceeds by induction.
4. It is no loss of generality to assume that $a_0 \neq 0$. If $[x_0, x_1, \ldots, x_n]$ is a solution, map it to the point $[x_1, x_2, \ldots, x_n]$ of $P^{n-1}(F)$. Show this map is well defined, one to one, and onto.
5. Substitute, "dehomogenize," and use the fact that a polynomial of degree n has at most n roots.
9. The kth partial derivative is $ma_k x_k^{m-1}$. Since each $a_k \neq 0$ and m is prime to the characteristic, the only common zero of all the partial derivatives has all its components zero. This, however, does not correspond to a point of projective space.
12. The "homogenized" equation is $t^2x^2 + t^2y^2 + x^2y^2 = 0$. Setting $t = 0$ we see that the points at infinity are (0, 0, 1) and (0, 1, 0). Calculating partial derivatives and substituting shows that both these points are singular.
14. Consider the associated homogeneous equation and calculate the three partial derivatives. Assuming that a common solution exists, show that $4a^3 + 27b^2 = 0$.
19. The trace is identically zero on F_p iff $p \mid n$.
20. Consider the mapping $h(x) = x^p - x$ from F_q to F_q. Prove that it is a homomorphism and that its image has q/p elements. Prove also that the image of h is contained in the kernel of the trace mapping. Show that the latter map has less than or equal to q/p elements in its kernel. The result follows.
21. Count the number of such maps.
23. Substitute and calculate.

Chapter 11

4. In F_q there are $2q + 1$ points at infinity and q^2 finite points. Thus $N_s = 3p^{2s} - p^s - 1$.

7. The number of lines in $P^n(F)$ is equal to the number of planes $A^{n+1}(F)$ which pass through the origin. The answer is $(q^{n+1} - 1)(q^{n+1} - q)(q^2 - 1)^{-1}(q^2 - q)^{-1}$.
9. There is one point at infinity. For $x = 0$ there is only one point $(0, 0)$ on the curve. If $x \neq 0$, let $t = y/x$ and consider $t^2 = x + 1$. This has $p - 2$ solutions with $x \neq 0$. Altogether there are p solutions in F_p. Similarly, there are q solutions in F_q. Thus the answer is $(1 - pu)^{-1}$.
12. To begin with, calculate the number of solutions to $u^2 - v^4 = 4D$.
16. The important facts are that $N_{F_s/F}$ is a homomorphism which is onto, and that the group of multiplicative characters of a finite field is cyclic.
18. Use the relation between Gauss sums and Jacobi sums and the Hasse–Davenport relation.
19. After expanding the terms of the product into geometric series, the result reduces to the fact that every monic polynomial is the product of monic irreducible polynomials in a unique way.
20. Use the identity $1 - T^s = \prod_{k=0}^{s-1} (1 - \zeta^k T)$, where $\zeta = e^{2\pi i/s}$.

Chapter 12

7. $21 = (1 + 2\sqrt{-5})(1 + 2\sqrt{-5})$.
8. Write $\det(\omega_i^{(j)})$ as $P - N$, where P is the sum of terms corresponding to the even permutations and N is the corresponding sum for odd permutations. Then notice that $(P - N)^2 = (P + N)^2 - 4PN$. A standard argument shows that $P + N$ and PN are integers.
9. Use Proposition 12.1.4 and elementary symmetric functions.
14. Consider $\zeta + \zeta^{-1}$ where ζ is a primitive seventh root of unity.
21–23. See Part 2, Section 5.
26. Choose a primitive g for the residue field. Lift it to D and consider the corresponding minimal polynomial over the fixed field of the decomposition group (see [207], p. 223).

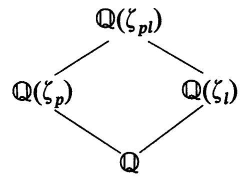
Chapter 13

1. Show that $\phi(n)$ is even if $n > 2$.
2. Use Proposition 13.1.3.
3. $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$.
24. The discriminant of a quadratic field is 0 or 1 modulo 4.
27. The order of σ_p cannot be 4. See Theorem 2.

Chapter 14

1. (a) Use the definition of $J(\chi, \psi)$, the binomial theorem and Exercise 11, Chapter 4. See also Lemma 1, Chapter 9.
12. See Exercise 17(e).
14. Let P be a prime ideal dividing p. Show $(\alpha/P)(\alpha/\bar{P}) = 1$. See [166], Satz 1034.

17. (b) Examine the ramification of l in the diagram



(c) Note that $\zeta_l^{\sigma_t} = \zeta_l^t = (1 - (1 - \zeta_l))^t$.
(e) Use Theorem 1, Chapter 8 and the fact that $g(\chi_P^t) = g(\chi_P)^{\sigma_t}$.

Chapter 15

2. Use Theorem 3.
3. Use Theorem 3 and Proposition 15.2.4.
9. As a function of a complex variable $(e^t - 1)^{-1}$ is analytic for $|t| < 2\pi$.
13. Use Exercise 12.
21. Set $F = 2$ in Exercise 19.

Chapter 16

4. For another evaluation note that $\int_0^1 t^{3k}(1 - t)\,dt = 1/[(3k + 1)(3k + 2)]$.
7. Show that if $p \nmid m$ and $p \mid \Phi_m(N)$ for an integer N then $p \equiv 1\ (m)$.
11. For an integer m choose a prime $p \equiv 1\ (m)$ and consider subfields of $\mathbb{Q}(\zeta_p)$.
12. If $p \equiv t\ (m)$ then $p \mid f(\zeta^p) = f(\zeta^t)$ where ζ is a primitive mth root of unity and $f(x) \in \mathbb{Z}[x]$, $f(\zeta) = 0$.
14. Use Theorem 1, Chapter 6.

Chapter 17

2. $y^2 + 4 = x^3 - 27$.
3. Imitate the proof of Proposition 17.8.1 ([60], Theorem 121).
8. $(y + 2i)(y - 2i) = x^3$.
12. Consider $(x_1 + y_1\sqrt{d})^2$ for a solution (x_1, y_1) of $x^2 - dy^2 = -1$.
13. $1^3 + 2^3 + \cdots + n^3 = (n(n + 1)/2)^2$.
16. Consider the map

$$(x_1, x_2, x_3, x_4) \to \left(\frac{x_1 + x_2}{2}, \frac{x_1 - x_2}{2}, \frac{x_3 + x_4}{2}, \frac{x_3 - x_4}{2}\right).$$

18. $\binom{4}{2} = 6$.
19. Consider the hint for Problem 16.

Chapter 18

4. If t is the order of the torsion subgroup of E then for $p \equiv 2\ (3)$, $p \equiv -1\ (t)$. The density of the set of primes $\equiv -1\ (t)$ is $1/\phi(t)$ while the density of primes $p \equiv 2\ (3)$ is $\frac{1}{2}$.

8. (a) Prove first for $\mathfrak{A} = P$ using $(N(P) - 2)(N(P)) = (N(P) - 1)^2 - 1$.
   (b) See Exercise 4, Chapter 14. For $|u(a, b)| = 1$, apply σ_{-1} (cf. Lemma 4, Section 5, Chapter 14).
   (c) Show that $\hat{u}$ is invariant under the action of the appropriate Galois group.
12. (a) See Chapter 11.
   (b) See Exercise 4.
   (c) See Exercise 17.

Bibliography

First Bibliography

1. A. Albert. *Fundamental Concepts of Higher Algebra.* Chicago: University of Chicago Press, 1956.
2. E. Artin. *The Collected Papers of Emil Artin.* Reading, Mass.: Addison-Wesley, 1965.
3. J. Ax. Zeros of polynomials over finite fields. *Am. J. Math.*, **86** (1964), 255–261.
4. P. Bachman. *Niedere Zahlentheorie*, Vol. 1. Leipzig, 1902, p. 83.
5. P. Bachman. *Die Lehre von der Kreisteilung.* Leipzig, 1872.
6. P. Bachman. Über Gauss' Zahltheoretische Arbeiten. *Gott. Nach.* (1911), 455–508.
7. A. Beck, M. N. Bleicher, and D. W. Crowe. *Excursions into Mathematics.* New York: Worth, 1969.
8. H. Bilharz. Primdivisor mit vorgegebener Primitivwurzel. *Math. Ann.*, **114** (1937), 476–492.
9. Z. I. Borevich and I. R. Shafarevich. *Number Theory.* Transl. by N. Greenleaf. New York: Academic Press, 1966.
10. L. Carlitz. The arithmetic of polynomials in a Galois field. *Am. J. Math.*, **54** (1932), 39–50.
11. L. Carlitz. Some applications of a theorem of Chevalley. *Duke Math. J.*, **18** (1951), 811–819.
12. L. Carlitz. Some problems involving primitive roots in a finite field. *Proc. Nat. Acad. Sci. U.S.A.*, **38** (1952), 314–318.
13. L. Carlitz. Kloosterman sums and finite field extensions. *Acta Arithmetica*, **16** (1969), 179–193.
14. P. Cartier. Sur une généralisation des symboles de Legendre–Jacobi. *L'Enseignement Math.*, **15** (1970), 31–48.
15. J. W. S. Cassels. On Kummer sums. *Proc. London Math. Soc.*, **21**, no. 3 (1970), 19–27.
16. C. Chevalley. Démonstration d'une hypothèse de M. Artin. *Abhand. Math. Sem. Hamburg*, **11** (1936), 73–75.
17. S. Chowla. The last entry in Gauss' diary. *Proc. Nat. Acad. Sci. U.S.A.*, **35** (1949), 244–246.

18. S. Chowla. *The Riemann Hypothesis and Hilbert's Tenth Problem*. New York: Gordon & Breach, 1965.
19. S. Chowla. A note on the construction of finite Galois fields $GF(p^n)$. *J. Math. Anal. Appl.*, **15** (1966), 53–54.
20. S. Chowla. An algebraic proof of the law of quadratic reciprocity. *Norske Vid. Selsk. Forh. (Trondheim)*, **39** (1966), 59.
21. H. Davenport. On the distribution of quadratic residues mod *p*. *London Math. Soc. J.*, **5–6** (1930–1931), 49–54.
22. H. Davenport. *The Higher Arithmetic*. London: Hutchinson, 1968.
23. H. Davenport and H. Hasse. Die Nullstellen der Kongruenz Zetafunktion in gewissen zyklischen Fällen. *J. Reine und Angew. Math.*, **172** (1935), 151–182.
24. M. Deuring. The zeta functions of algebraic curves and varieties. *Indian J. Math.* (1955), 89–101.
25. L. Dickson. *Linear Algebraic Groups and an Exposition of the Galois Field Theory. 1900*. New York: Dover, 1958.
26. B. Dwork. On the rationality of the zeta function. *Am. J. Math.*, **82** (1959), 631–648.
27. G. Eisenstein. Beiträge zur Kreisteilung. *J. Reine und Angew. Math.* (1844), 269–278.
28. G. Einstein. Beweis des Reciprocitätssatzes für die kubischen Reste . . . . *J. Reine und Angew. Math.* (1844), 289–310.
29. G. Eisenstein. Nachtrag zum kubischen Reciprocitätssatze. *J. Reine und Angew. Math.*, **28** (1844), 28–35.
30. G. Eisenstein. Beiträge zur Theorie der elliptischen Funktionen. *J. Reine und Angew. Math.*, **35** (1847), 135–274.
31. P. Erdös. Some recent advances and current problems in number theory. *Lectures in Modern Mathematics*, Vol. 3. New York: Wiley, 1965.
32. A. Frankel. Integers and the theory of numbers. *Scripta Math. Studies*, **5**, 1955.
33. E. Galois. *Oeuvres Mathematiques*. Paris: Gauthier-Villars, 1897.
34. C. F. Gauss. *Arithmetische Untersuchungen*. New York: Chelsea, 1965.
35. L. Goldstein. Density questions in algebraic number theory. *Am. Math. Monthly*, **78** (April 1971), 342–351.
36. R. Graham. On quadruples of consecutive *k*th power residues. *Proc. Am. Math. Soc.* (1964), 196–197.
37. M. Greenberg. *Forms in Many Variables*. Menlo Park, Calif.: W. A. Benjamin, 1969.
38. G. H. Hardy. *Prime Numbers*. Manchester: British Association, 1915, pp. 350–354 and *Collected Papers*, Vol. 2.
39. G. H. Hardy. An introduction to the theory of numbers. *Bull. Am. Math. Soc.*, **35** (1929), 778–818.
40. G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. 4th ed., New York: Oxford University Press, 1960.
41. H. Hasse. *Vorlesungen über Zahlentheorie*. Berlin: Springer-Verlag, 1964.
42. H. Hasse. *The Riemann Hypothesis in Function Fields*. Philadelphia: Pennsylvania State University Press, 1969.
43. A. Hausner. On the law of quadratic reciprocity. *Archiv der Math.*, **12** (1961), 182–183.
44. E. Hecke. *Algebraische Zahlentheorie*. Leipzig: 1929. Reprinted by Chelsea Publishing Company, Inc., New York.
45. L. Holzer. *Zahlentheorie*. Leipzig: Teubner Verlagsgesellschaft, 1958.
46. C. Hooley. On Artin's conjecture. *J. Reine und Angew. Math.*, **225** (1967), 209–220.
47. C. Jacobi. Über die Kreisteilung . . . . *J. Reine und Angew. Math.* (1846), 254–274.
48. E. Jacobsthal. Über die Darstellung der Primzahlen der Form $4n + 1$ als Summe zweier Quadrate. *J. Reine und Angew. Math.*, **132** (1907), 238–245.

49. C. Jordan. *Traite des substitutions.* Paris: 1870.
50. H. Kornblum. Uber die Primfunktionen in einer Arithmetischen Progression. *Math. Z.*, **5** (1919), 100–111.
51. E. Kummer. Über die allgemeinen Reciprocitatsgesetz . . . . *Math. Abh. Akad. Wiss. zu Berlin* (1859), 19–160.
52. E. Landau, *Elementary Number Theory.* 2nd ed. New York: Chelsea, 1966.
53. S. Lang. Some theorems and conjectures on diophantine equations. *Bull. Am. Math. Soc.*, **66** (1960), 240–249.
54. D. H. Lehmer. A note on primitives. *Scripta Mathematica*, **26** (1963), 117–119.
55. E. Lehmer. On the quintic character of 2 and 3, *Duke Math. J.*, **18** (1951), 11–18.
56. E. Lehmer. Criteria for cubic and quartic residuacity. *Mathematika*, **6** (1958), 20–29.
57. P. Leonard. On constructing quartic extensions of *GF(p)*. *Norske Vid. Selsk. Forh. (Trondheim)*, **40** (1967), 41–52.
58. H. B. Mann. *Introduction to Number Theory.* Columbus, Ohio: Ohio State University Press, 1955.
59. W. H. Mills. Bounded consecutive residues and related problems. *Proc. Symp. Pure Math.*, **8** (1965).
60. T. Nagell. *Introduction to Number Theory.* New York: Wiley, 1951. Reprinted by Chelsea Publishing Company, Inc., New York.
61. I. Niven and H. S. Zuckerman. *An Introduction to the Theory of Numbers.* 2nd ed. New York: Wiley, 1966.
62. C. Pisot. Introduction à la theorie des nombres algébriques. *L'Enseignement Math.*, **8**, no. 2 (1962), 238–251.
63. H. Pollard and H. Diamond. *The Theory of Algebraic Numbers.* New York: Wiley, 1950. 2nd ed., 1975.
64. H. Rademacher. *Lectures on Elementary Number Theory.* Lexington, Mass.: Xerox College Publishing, 1964.
65. H. Rademacher and O. Toeplitz. *The Enjoyment of Mathematics.* Princeton, N.J.: Princeton University Press, 1951.
66. G. Rieger. *Die Zahlentheorie bei C. F. Gauss.* From *Gauss Gedenkband.* Berlin: Haude and Sperner, 1960.
67. P. Samuel. Unique factorization. *Am. Math. Monthly*, **75** (1968), 945–952.
68. P. Samuel. *Théorie Algébrique des Nombres.* Paris: Hermann & Cie, 1967.
69. J. P. Serre. *Compléments d'Arithmétiques, Rédigés par J. P. Ramis et G. Ruget.* Paris: Ecoles Normales Supérieures, 1964. English version, Springer-Verlag, 1973.
70. D. Shanks. *Solved and Unsolved Problems in Number Theory.* New York: Spartan Books, 1962.
71. W. Sierpinski. *A Selection of Problems in the Theory of Numbers.* Oxford: Pergamon Press, 1964.
72. H. J. S. Smith. *Report on the Theory of Numbers*, 1894. Reprinted by Chelsea Publishing Company, Inc., New York, 1965.
73. H. Stark, *An Introduction to Number Theory.* Cambridge, Mass.: M.I.T. Press, 1979.
74. T. Storer. *Cyclotomy and Difference Sets.* Chicago: Markham, 1967.
75. R. Swan. Factorization of polynomials over finite fields. *Pacific J. Math.*, **12** (1962), 1099–1106.
76. E. Vegh. Primitive roots modulo a prime as consecutive terms of an arithmetic progression. *J. Reine und Angew. Math.*, **235** (1969), 185–188.
77. I. M. Vinogradov. *Elements of Number Theory.* Transl. by S. Kravetz. New York: Dover, 1954.
78. E. Warning. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. *Agh. Math. Sem. Hamburg*, **11** (1936), 76–83.

79. W. Waterhouse. The sign of the Gauss sum. *J. Number Theory*, **2**, no. 3 (1970), 363.
80. A. Weil. Number of solutions of equations in a finite field. *Bull. Am. Math. Soc.*, **55** (1949), 497–508.
81. A. Weil. Jacobi sums as "Grössencharaktere." *Trans. Am. Math. Soc.*, **73** (1952), 487–495.
82. K. Yamamoto. On a conjecture of Hasse concerning multiplicative relations of Gauss sums. *J. Combin. Theory*, **1** (1966), 476–489.
83. A. Yokoyama. On the Gaussian sum and the jacobi sum with its applications. *Tohoku Maths. J.* (2), **16** (1964), 142–153.

Second Bibliography

84. W. W. Adams and L. J. Goldstein. *Introduction to Number Theory*. Englewood Cliffs, N.J.: Prentice-Hall, 1976.
85. L. Ahlfors. *Complex Analysis*. 2nd ed. New York: McGraw-Hill, 1966.
86. N. C. Ankeny, E. Artin, and S. Chowla. The class numbers of real quadratic fields. *Ann. Math.* (2), **56** (1952), 479–493.
87. N. Arthaud, On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication. *Comp. Math.*, **37**, Fasc. 2 (1978), 209–232.
88. R. Ayoub. Euler and the zeta function. *Am. Math. Monthly*, **81** (1974), 1067–1086.
89. A. Baker. *Transcendental Number Theory*. Cambridge: Cambridge University Press, 1975.
90. A. Baker. On the class number of imaginary quadratic fields. *Bull. Amer. Math. Soc.*, **77** (1971), 678–684.
91. G. Bergmann. Über Eulers Beweis des grossen Fermatschen Satzes für den Exponenten 3. *Math. Ann.*, **164** (1966), 159–175.
92. B. C. Berndt. Sums of Gauss, Jacobi and Jacobsthal. *J. Number Theory*, **11** (1979), 349–398.
93. B. C. Berndt and R. J. Evans. The determination of Gauss Sums. *Bull. Am. Math. Soc.*, **5** (2) (1981), 107–129.
94. B. C. Berndt. Classical theorems on quadratic residues. *L'Enseignement Math.* **22**, fasc. 3–4 (1976).
95. B. C. Berndt and R. C. Evans. Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer. *Ill. Math.*, **23**, no. 3 (1979), 374–437.
96. B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves, I. *J. Reine und Angew. Math.*, **212** (1963), 7–25; II, **218** (1965), 79–108.
97. B. J. Birch. Conjectures on elliptic curves. In: *Theory of Numbers*, Amer. Math. Soc., Proc. of Symposia in Pure Math., Vol. 8. Pasadena, 1963.
98. E. Bombieri. Counting points on Curves over Finite Fields (d'après S. A. Stepanov) Sem. Bourbaki, Vol. 1972–73, Exposé 430. *Lecture Notes in Mathematics*, Vol. 383, pp. 234–241. New York: Springer-Verlag, 1974.
99. E. Brown. The first proof of the quadratic reciprocity law, revisited. *Am. Math. Monthly*, **88** (1981), 257–264.
100. A. Brumer and K. Kramer. The rank of elliptic curves. *Duke Math. J.*, **44** (1977), 715–742.
101. W. K. Bühler. *Gauss*. New York: Springer-Verlag, 1981.
102. K. Burde. Ein rationales biquadratisches Reciprozitätsgesetz. *J. Reine und Angew. Math.*, **235** (1969), 175–184.
103. H. S. Butts and L. Wade. Two criteria for Dedekind domains. *Am. Math. Monthly*, **73** (1966), 14–21.

104. L. Carlitz. Arithmetic properties of generalized Bernoulli numbers. *J. Reine und Angew. Math.*, **201–202** (1959), 173–182.
105. L. Carlitz. A note on irregular primes. *Proc. Am. Math. Soc.*, **5** (1954), 329–331.
106. L. Carlitz. A characterization of algebraic number fields with class number two. *Proc. Am. Math. Soc.*, **11** (1960), 391–392.
107. J. W. S. Cassels. Arithmetic on an elliptic curve. Proceedings of the International Congress of Mathematics. Stockholm, 1962. pp. 234–246.
108. J. W. S. Cassels. On Kummer sums. *Proc. London Math. Soc.* (3), **21** (1970), 19–27.
109. J. W. S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, **41** (1966), 193–291.
110. J. W. S. Cassels and A. Frölich. Algebraic number theory. Proceedings of an International Congress by the London Mathematical Society, 1967. Washington, D.C.: Thompson.
111. F. Châtelet. Les corps quadratiques. *Monographies de l'Enseignement Mathématique*, Vol. 9. Genève: 1962.
112. K. Chandrasekharan. *Introduction to Analytic Number Theory.* New York: Springer-Verlag, 1968.
113. S. Chowla. On Gaussian sums. *Proc. Nat. Acad. Sci. U.S.A.*, **48** (1962), 1127–1128.
114. J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, **39** (1977), 223–251.
115. H. Cohn. *A Second Course in Number Theory.* New York: Wiley, 1962.
116. M. J. Collison. The origins of the cubic and biquadratic reciprocity laws. *Arch. Hist. Exact Sci.*, **17**, no. 1 (1977), 63–69.
117. A. Czogla. Arithmetic characterization of algebraic number fields with small class numbers. *Math. Z.* (1981), 247–253.
118. H. Davenport. The work of K. E. Roth. Proc. Int. Cong. Math., 1958, LVII–LX. Cambridge: Cambridge University Press, 1960.
119. H. Davenport. *Multiplicative Number Theory.* New York: Springer-Verlag, 1980.
120. D. Davis and O. Shisha. Simple proofs of the fundamental theorem of arithmetic. *Math. Mag.*, **54**, no. 1 (1981), 18.
121. R. Dedekind. *Mathematische Werke,* Vols. I and II. New York: Chelsea, 1969.
122. P. G. L. Dirichlet. Sur l'equation $t^2 + u^2 + v^2 + w^2 = 4m$. In: *Dirichlet's Werke,* Vol. 2, pp. 201–208. New York: Chelsea, 1969.
123. P. G. L. Dirichlet. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression . . . . In: *Mathematische Werke,* pp. 313–342. New York: Chelsea, 1969.
124. P. G. L. Dirichlet. Recherches sur diverses applications de l'analyse infinitésimale a la théorie des nombres. In: *Dirichlet's Werke,* pp. 401–496. New York: Chelsea, 1969.
125. P. G. L. Dirichlet. *Werke.* 2 vols. in one. New York: Chelsea, 1969.
126. P. G. L. Dirichlet. Sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires. In: *Dirichlet's Werke,* pp. 345–350. New York: Chelsea, 1969.
127. P. G. L. Dirichlet. Dedekind, *Vorlesungen über Zahlentheorie.* New York: Chelsea, 1968.
128. H. M. Edwards. *Fermat's Last Theorem, A Genetic Introduction to Algebraic Number Theory.* New York: Springer-Verlag, 1977.
129. H. M. Edwards. The background of Kummers proof of Fermat's Last Theorem for regular exponent. *Arch. Hist. Exact Sci.*, **14** (1974), 219–326. See also postscript to the above **17** (1977), 381–394.
130. G. Eisenstein. Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste. In: *Mathematische Werke,* Band I, pp. 223–245. New York: Chelsea, 1975.
131. G. Eisenstein. Lois de réciprocité. In: *Mathematische Werke,* Band I, pp. 53–67. New York: Chelsea, 1975.

132. G. Eisenstein. Beweis des allgemeinsten Reciprocitätsgesetze zwischen reelen und complexen Zahlen. In: *Mathematische Werke*, Band II, pp. 189–198. New York: Chelsea, 1975.
133. P. Erdös. On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. *Proc. Nat. Acad. Sci. U.S.A.*, **35** (1949), 374–384.
134. H. Flanders. Generalization of a theorem of Ankeny and Rogers. *Ann. Math.*, **57** (1953), 392–400.
135. W. Fulton. *Algebraic Curves*. New York: W. A. Benjamin, 1969.
136. C. F. Gauss. *Disquisitiones Arithmeticae*. Transl. by A. A. Clarke. New Haven, Conn.: Yale University Press, 1966.
137. C. F. Gauss. *Mathematisches Tagebuch, 1796–1814*. Edited by K.-R. Biermann. Ostwalds Klassiker 256.
138. M. Gerstenhaber. The 152nd proof of the law of quadratic reciprocity. *Am. Math. Monthly*, **70** (1963), 397–398.
139. L. J. Goldstein. A history of the prime number theorem. *Am. Math. Monthly*, **80** (1973), 599–615.
140. L. J. Goldstein. *Analytic Number Theory*. Princeton, N. J.: Prentice-Hall, 1971.
141. D. Goss. A simple approach to the analytic continuation and values at negative integers for Riemann's zeta function. *Proc. Am. Math. Soc.*, **81**, no. 4 (1981), 513–517.
142. B. H. Gross and D. E. Rohrlich. Some results on the Mordell–Weil group of the Jacobian of the Fermat curve. *Invent. Math.*, **44** (1978), 201–224.
143. T. Hall. *Carl Friedrich Gauss, a Biography*. Transl. by A. Froderberg. Cambridge, Mass.: M.I.T. Press, 1970.
144. R. Hartshorne. *Algebraic Geometry*. New York: Springer-Verlag, 1977.
145. P. G. Hartung. On the Pellian equation. *J. Number Theory*, **12** (1980), 110–112.
146. T. L. Heath. *Diophantus of Alexandria: A Study in the History of Greek Algebra*, New York: Dover, 1964.
147. D. R. Heath Brown and S. J. Patterson. The distribution of Kummer sums at prime arguments. *J. Reine und Angew. Math.*, **310** (1979), 111–136.
148. L. Heffter. Ludwig Stickelberger. *Deutsche Math. Jahr.*, **47** (1937), 79–86.
149. J. Herbrand. Sur les classes des corp circulaires. *J. Math. Pures et Appl.*, **ii** (1932), 417–441.
150. I. Herstein. *Topics in Algebra*. Lexington, Mass.: Xerox College, 1975.
151. D. Hilbert. Die Theorie der algebraischen Zahlkörper. In: *Gesammelte Abhandlungen*, Vol. 1, pp. 63–363. New York: Chelsea, 1965.
152. J. E. Hofmann. Über Zahlentheoretische Methoden Fermats und Eulers, ihre Zusammenhänge und ihre Bedeutung. *Arch. Hist. Exact Sci.* (1960–62), 122–159.
153. A. Hurwitz. Einige Eigenschaften der Dirichlet'schen Funktion $F(s) = \sum(D/n)1/n^s$, etc. . . . . In: A Hurwitz: *Mathematische Werke*, Band I, pp. 72–88, Basel and Stuttgart: Birkhäuser-Verlag, 1963.
154. A. Hurwitz. *Mathematische Werke*, Band II. Basel und Stuttgart: Birkhäuser-Verlag, 1963.
155. K. Iwasawa. Lectures on p-adic L-functions. *Ann. Math. Studies*. Princeton Press, 1974.
156. K. Iwasawa. A note on Jacobi sums. *Symp. Math.*, **15** (1975), 447–459.
157. K. Iwasawa. A note on cyclotomic fields. *Invent. Math.* **36** (1976), 115–123.
158. S. Iyanaga (Ed.). *Theory of Numbers*. Amsterdam: North-Holland, 1975.
159. W. Johnson. Irregular primes and cyclotomic invariants. *Math. Comp.*, **29** (1975), 113–120.
160. J. R. Joly. Equations et variétés algébriques sur un corps fini. *L'Enseignement Math.*, **19** (1973), 1–117.

161. N. Katz. An Overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields. Proc. of Symposia in Pure Math., Vol. 28, pp. 275–305. Providence, R.I.: Am. Math. Society, 1976.
162. N. Koblitz. *P-adic Numbers, p-adic Analysis, and Zeta-Functions*, New York: Springer-Verlag, 1977.
163. E. E. Kummer. De residuis cubicis disquisitiones nonnullae analyticae. *J. Reine und Angew Math.*, **32** (1846), 341–359 (*Collected Papers*, Vol. 1, pp. 145–163. New York: Springer-Verlag, 1975.
164. E. E. Kummer. *Collected Papers*, Vol. 1. New York: Springer-Verlag, 1975.
165. E. Landau. *Einführung in die elementare und analytische theorie der algebraischen zahlen und der ideale* . . . . New York: Chelsea, 1949.
166. E. Landau, *Vorlesungen über Zahlentheorie*, Vols. 1–3. Leipzig, 1927.
167. S. Lang. *Cyclotomic Fields*. New York: Springer-Verlag, 1978.
168. S. Lang. *Algebraic Number Theory*. Reading, Mass: Addison-Wesley, 1970.
169. S. Lang. *Elliptic Functions*. Reading, Mass.: Addison-Wesley, 1973.
170. S. Lang. *Diophantine Geometry*. New York: Wiley-Interscience, 1962.
171. S. Lang. *Cyclotomic Fields*, II. New York: Springer-Verlag, 1980.
172. S. Lang. Review of L. J. Mordell's diophantine equations. *Bull. Am. Math. Soc.*, **76** (1970), 1230–1234.
173. S. Lang. Higher dimensional diophantine problems. Bull. Am. Math. Soc., **80**, no. 5 (1974), 779–787.
174. E. Lehmer. On Euler's criterion. *J. Aust. Math. Soc.* (1959/61), Part 1, 67–70.
175. E. Lehmer. Rational reciprocity laws. *Am. Math. Monthly*, **85** (1978), 467–472.
176. E. Lehmer. On the location of Gauss sums. *Math. Comp.*, **10** (1956), 194–202.
177. P. A. Leonard and S. Williams. Jacobi sums and a theorem Brewer. *Rocky Mountain. J. Math.*, **5**, no. 2 (Spring, 1975).
178. A. W. Leopoldt. Eine Verallgemeinerung der Bernoullischen Zahlen. *Abhand. Math. Sem. Hamburg*, **22** (1958), 131–140.
179. W. J. LeVeque. *Fundamentals of Number Theory*. Reading, Mass.: Addison-Wesley, 1977.
180. W. J. LeVeque. A brief survey of diophantine equations. *M.A.A. Studies in Mathematics*, **6** (1969), 4–24.
181. H. von Lienen, Reele kubishe und biquadratische Legendre Symbole. *Reine und Angew. Math.*, **305** (1979), 140–154.
182. J. H. Loxton. Some conjectures concerning Gauss sums. *J. Reine und Angew. Math.*, **297** (1978), 153–158.
183. D. A. Marcus. *Number Fields*. New York: Springer-Verlag, 1977.
184. J. M. Masley, Where are number fields with small class number?, *Lecture Notes in Mathematics*, Vol. 751, pp. 221–242. New York: Springer-Verlag, 1979.
185. J. Masley. Class groups of abelian number fields. Proc. Queen's Number Theory Conference, 1979. Edited by P. Ribenboim. Kingston, Ontario: Queen's University.
186. C. R. Matthews. Gauss sums and elliptic functions. I: The Kummer sum. *Invent. Math.*, **52** (1979), 163–185; II: The Quartic Case, **54** (1979), 23–52.
187. B. Mazur. Rational points on modular curves. In: Modular Functions of One Variable, V. *Lecture Notes in Mathematics*, Vol. 601. New York: Springer-Verlag, 1976.
188. T. Metsänkylä. Distribution of irregular prime members. *J. Reine und Angew. Math.*, **282** (1976), 126–130.
189. L. J. Mordell. *Diophantine Equations*. New York: Academic Press, 1969.
190. L. J. Mordell. Review of S. Lang's diophantine geometry. *Bull. Am. Math. Soc.*, **70** (1964), 491–498.
191. L. J. Mordell. The infinity of rational solutions of $y^2 = x^3 + k$. *J. London Math. Soc.*, **41** (1966), 523–525.

192. B. Morlaye. Demonstration élémentaire d'un théoreme de Davenport et Hasse. *L'enseignement Math.*, **18** (1973), 269–276.
193. Leo Moser. A thorem on quadratic residues. *Proc. Am. Math. Soc.*, **2** (1951), 503–504.
194. J. B. Muskat. Reciprocity and Jacobi sums. *Pacific J. Math.*, **20** (1967), 275–280.
195. T. Nagell. Sur les restes et nonrestes cubiques. *Arkiv Math.*, **1** (1952), 579–586.
196. W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Warsaw: Polish Scientific Publications, 1974.
197. J. von Neumann and H. H. Goldstine. A numerical study of a conjecture of Kummer. *MTAC*, **7** (1953), 133–134.
198. D. J. Newman. Simple analytic proof of the prime number theorem. *Am. Math. Monthly*, **87** (1980), 693–696.
199. N. Nielson. *Traité Élémentaire des Nombres Bernoulli*. Paris: 1923.
200. L. D. Olson. The trace of Frobenius for elliptic curves with complex multiplication. *Lecture Notes in Mathematics*, Vol. 732, pp. 454–476. New York: Springer-Verlag, 1979.
201. L. D. Olson. Points of finite order on elliptic curves with complex multiplication. *Manuscripta Math.*, **14** (1974), 195–205.
202. L. D. Olson. Hasse invariants and anomolous primes for elliptic curves with complex multiplication. *J. Number Theory*, **8** (1976), 397–414.
203. H. Poincaré. Sur les propriétés des courbes algebriques planes. *J. Liouville* (v), **7** (1901), 161–233.
204. H. Rademacher. *Topics in Analytic Number Theory*. Die Grundlehren der Mathematischen, Wissenschaften. New York: Springer-Verlag, 1964.
205. H. Reichardt. Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen. *J. Reine Angew. und Math.*, **184** (1942), 12–18.
206. P. Ribenboim. 13 Lectures on Fermat's Last Theorem. New York: Springer-Verlag, 1979.
207. P. Ribenboim. *Algebraic Numbers*. New York: Wiley, 1972.
208. K. Ribet. A modular construction of unramified p-extensions of $Q(\mu_p)$. *Invent. Math.*, **34** (1976), 151–162.
209. G. J. Rieger. Die Zahlentheorie bei C. F. Gauss. In: C. F. Gauss, *Leben und Werk*. pp. 38–77. Berlin: Haude & Spenersche Verlagsbuchhandlung, 1960.
210. A. Robert. Elliptic curves. *Lecture Notes in Mathematics*, Vol. 326. New York: Springer-Verlag, 1973.
211. M. I. Rosen and J. Kraft. Eisenstein reciprocity and nth power residues. *Am. Math. Monthly*, **88** (1981), 269–270.
212. M. I. Rosen. Abel's theorem on the lemniscate. *Am. Math. Monthly*, **88** (1981), 387–395.
213. P. Samuel. *Théorie Algébrique des Nombres*. Hermann: Paris, 1967. Transl. by A. Silberger. Boston: Houghton Mifflin, 1970.
214. P. Samuel and O. Zariski. *Commutative Algebra*, Vol. 1, New York: Springer-Verlag, 1975–1976.
215. A. Selberg. An elementary proof of the prime number theorem. *Ann. Math.*, **50** (1949), 305–319.
216. E. S. Selmer. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, **85** (1951), 203–362.
217. W. M. Schmidt. Diophantine approximation. *Lecture Notes in Mathematics*, Vol. 785. New York: Springer-Verlag, 1980.
218. W. M. Schmidt. Equations over finite fields: an elementary approach. *Lecture Notes in Mathematics*, Vol. 536. New York: Springer-Verlag, 1976.
219. I. R. Shafarevich. *Basic Algebraic Geometry*. Grundlehren der Mathematischen Wissenschaften 213. Transl. by K. A. Hirsch. New York: Springer-Verlag, 1977.
220. D. E. Smith. *Source Book in Mathematics*, Vols. 1 and 2. New York: Dover, 1959.

221. H. M. Stark. On the Riemann hypothesis in hyperelliptic function fields. *A.M.S. Proc. Symp. Pure Math.*, **24** (1973), 285–302.
222. S. A. Stepanov. Rational points on algebraic curves over finite fields (in Russian). Report of a 1972 Conference on Analytic Number Theory in Minsk, U.S.S.R., pp. 223–243.
223. N. M. Stephens. The diophantine equation $x^3 + y^3 = dz^3$ and the conjectures of Birch and Swinnerton-Dyer. *J. Reine und Angew. Math.*, 231.
224. L. Stickelberger. Über eine Verallgemeinerung von der Kreistheilung. *Math. Ann.*, **37** (1890), 321-367.
225. K. B. Stolarsky. *Algebraic Numbers and Diophantine Approximation.* New York: Dekker, 1974.
226. H. P. F. Swinnerton-Dyer. The conjectures of Birch and Swinnerton-Dyer and of Tate. In: *Proceedings of a Conference on Local Fields.* Berlin–Heidelberg–New York: Springer-Verlag, 1967.
227. J. Tate. The arithmetic of elliptic curves. *Invent. Math.*, **23** (1974), 179–206.
228. A. D. Thomas. *Zeta Functions: An Introduction to Algebraic Geometry.* London, San Francisco: Pitman, 1977.
229. E. Trost. *Primzahlen.* Basel and Stuttgart: Birhäuser-Verlag, 1953.
230. J. V. Uspensky and M. A. Heaslet, New York: McGraw-Hill, 1939.
231. H. S. Vandiver. Fermat's last theorem. *Am. Math. Monthly*, **53** (1946), 555–578.
232. H. S. Vandiver. On developments in an arithmetic theory of the Bernoulli and allied numbers. *Scripta Math.*, **25** (1961), 273–303.
233. A. van der Poorten. A proof that Euler missed . . . Apery's proof of the irrationality of $\zeta(3)$: An informal report. *The Mathematical Intelligencer*, **1**, no. 1 (1978) 195–203.
234. S. Wagstaff. The irregular primes to 125,000. *Math. Comp.*, **32**, no. 142 (1978), 583–591.
235. A. Weil. Two lectures on number theory: Past and present. *L'Enseignement Math.*, **XX** (1973), 81–110. Also in: A. Weil, *Oeuvres Scientifiques*, Vol. III, pp. 279–302. New York: Springer-Verlag, 1979.
236. A. Weil. Sommes de Jacobi et caractéres de Hecke. *Gött. Nach.* (1974), 1–14. Also in: A. Weil, *Oeuvres Scientifiques*, Vol. III, pp. 329–342. New York: Springer-Verlag, 1979.
237. A. Weil. Sur les sommes de trois et quatre carrés. *L'Enseignement Math.*, **20** (1974), 303–310. Also in: A. Weil, *Oeuvres Scientifiques*, Vol. III, New York: Springer-Verlag, 1979.
238. A. Weil. La cyclotomie jadis et naguére. *L'Enseignement Math.*, **20** (1974), 247–263. Also in: A. Weil, *Oeuvres Scientifiques*, Vol. III, pp. 311–327. New York: Springer-Verlag, 1979.
239. A. Weil. Review of "Mathematische Werke, by Gotthold Eisenstein". In: A. Weil, *Oeuvres Scientifiques*, Vol. III, pp. 398–403. New York: Springer-Verlag, 1979.
240. A. Weil. Fermat et l'équation de Pell. In: *Oeuvres Scientifiques*, Vol. III, pp. 413–419. New York: Springer-Verlag, 1979.
241. A. Weil. *Oeuvres Scientifiques, Collected Papers*, 3 vols. Corrected second printing. New York: Springer-Verlag, 1980.
242. A. Wiles. Modular curves and the class group of $\mathbb{Q}(\zeta_p)$. *Invent. Math.*, **58** (1980), 1–35.
243. K. S. Williams. On Euler's criterion for cubic nonresidues. *Proc. Am. Math. Soc.*, **49** (1975), 277–283.
244. K. S. Williams. Note on Burde's rational biquadratic reciprocity law. *Can. Math. Bull.*, (1) **20** (1977), 145–146.
245. K. S. Williams. On Eisenstein's supplement to the law of cubic reciprocity. *Bull. Cal. Math. Soc.*, **69** (1977), 311–314.

246. B. F. Wyman. What is a reciprocity law?. *Am. Math. Monthly*, **79** (1972), 571–586.
247. H. Yokoi. On the distribution of irregular primes. *J. Number Theory*, **7** (1975), 71–76.
248. Zeta Functions. In: *Encyclopedic Dictionary of Mathematics*. Edited by S. Iyanaga and Y. Kawada. Cambridge, Mass.: M.I.T. Press, 1977. pp. i372–i393.

Index

H

I

J

K

L

M

N

O

P

Q

R

S

Graduate Texts in Mathematics

Soft and hard cover editions are available for each volume up to Vol. 14, hard cover only from Vol. 15.

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFFER. Topological Vector Spaces.
4 HILTON/STAMMBACH. A Course in Homological Algebra.
5 MACLANE. Categories for the Working Mathematician.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory. 2nd printing, revised.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book.
20 HUSEMOLLER. Fibre Bundles. 2nd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis. 4th printing.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra I.
29 ZARISKI/SAMUEL. Commutative Algebra II.
30 JACOBSON. Lectures in Abstract Algebra I: Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II: Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III: Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 WERMER. Banach Algebras and Several Complex Variables. 2nd ed.
36 KELLEY/NAMIOKA. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory.

42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory. 4th ed. Vol. 1.
46 LOÈVE. Probability Theory. 4th ed. Vol. 2.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory. Vol. 1: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics.
61 WHITEHEAD. Elements of Homotopy Theory.
62 KARGAPOLOV/MERZIJAKOV. Fundamentals of the Theory of Groups.
63 BOLLOBAS. Graph Theory—An Introductory Course.
64 EDWARDS. Fourier Series. 2nd ed. Vol. 1.
65 WELLS. Differential Analysis on Complex Manifolds.
66 WATERHOUSE. Introduction to Affine Group Schemes.
67 SERRE. Local Fields.
68 WEIDMANN. Linear Operators in Hilbert Spaces.
69 LANG. Cyclotomic Fields II.
70 MASSEY. Singular Homology Theory.
71 FARKAS/KRA. Riemann Surfaces.
72 STILLWELL. Classical Topology and Combinatorial Group Theory.
73 HUNGERFORD. Algebra.
74 DAVENPORT. Multiplicative Number Theory.
75 HOCHSCHILD. Basic Theory of Algebraic Groups and Lie Algebras.
76 IITAKA. Algebraic Geometry.
77 HECKE. Lectures on the Theory of Algebraic Numbers.
78 BURRIS/SANKAPPANAVAR. A Course in Universal Algebra.
79 WALTERS. An Introduction to Ergodic Theory.
80 ROBINSON. A Course in the Theory of Groups.
81 FORSTER. Lectures on Riemann Surfaces.
82 BOTT/TU. Differential Forms in Algebraic Topology.
83 WASHINGTON. Introduction to Cyclotomic Fields.
84 IRELAND/ROSEN. A Classical Introduction to Modern Number Theory.