

Bibliography

- [Abou] M. Abouzaid, *Les nombres de Lucas et Lehmer sans diviseur primitif*, J. Théor. Nombres Bordeaux **18** (2006), 299–313.
- [Abr-Ste] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions*, Dover publications (1972).
- [AGP] R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. **139** (1994), 703–722.
- [Ami] Y. Amice, *Les nombres p -adiques*, SUP/Le Mathématicien **14**, Presses Universitaires de France (1975).
- [Ang] W. Anglin, *The square pyramid puzzle*, American Math. Monthly **97** (1990), 120–124.
- [Ax] J. Ax, *Zeros of polynomials over finite fields*, Amer. J. Math. **86** (1964), 255–261.
- [Bac] G. Bachman, *Introduction to p -adic Numbers and Valuation theory*, Academic paperbacks, Acad. Press (1964).
- [Bak1] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika **13** (1966), 204–216.
- [Bak2] A. Baker, *Transcendental Number Theory*, Cambridge University Press, 1975.
- [Bak-Dav] A. Baker and H. Davenport, *The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = y^2$* , Quart. J. Math. Oxford Ser. (2) **20** (1969), 129–137.
- [Bak-Wus] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. reine angew. Math. **442** (1993), 19–62.
- [BDD] R. Balasubramanian, J.-M. Deshouillers, and F. Dress, *Problème de Waring pour les bicarrés 1 : schéma de la solution, 2 : résultats auxiliaires pour le théorème asymptotique*, C. R. Acad. Sc. Paris **303** (1986), 85–88 and 161–163.
- [Bal-Dar-Ono] A. Balog, H. Darmon, and K. Ono, *Congruences for Fourier coefficients of half-integral weight modular forms and special values of L -functions*, Proceedings of a Conference in honor of H. Halberstam **1** (1996), 105–128.
- [Bar] D. Barsky, *Congruences de coefficients de séries de Taylor (Application aux nombres de Bernoulli–Hurwitz)*, Groupe d’Analyse Ultramétrique **3** (1975–1976), Exp. 17, 1–9, available on the NUMDAM archives.
- [Bat-Oli] C. Batut and M. Olivier, *Sur l’accélération de la convergence de certaines fractions continues*, Séminaire Th. Nombres Bordeaux (1979–1980), exposé **23**.
- [Bel-Gan] K. Belabas and H. Gangl, *Generators and relations for $K_2\mathcal{O}_F$* , K -Theory **31** (2004), 195–231.

- [BBGMS] C. Bennett, J. Blass, A. Glass, D. Meronk, and R. Steiner, *Linear forms in the logarithms of three positive rational numbers*, J. Théor. Nombres Bordeaux **9** (1997), 97–136.
- [Ben1] M. Bennett, *Rational approximation to algebraic numbers of small height: The Diophantine equation $|ax^n - by^n| = 1$* , J. reine angew. Math. **535** (2001), 1–49.
- [Ben2] M. Bennett, *Recipes for ternary Diophantine equations of signature (p, p, k)* , Proc. RIMS Kokyuroku (Kyoto) **1319** (2003), 51–55.
- [Ben3] M. Bennett, *On some exponential Diophantine equations of S. S. Pillai*, Canad. J. Math. **53** (2001), 897–922.
- [Ben-deW] M. Bennett and B. de Weger, *The Diophantine equation $|ax^n - by^n| = 1$* , Math. Comp. **67** (1998), 413–438.
- [Ben-Ski] M. Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), 23–54.
- [Ben-Vat-Yaz] M. Bennett, V. Vatsal, and S. Yazdani, *Ternary Diophantine equations of signature $(p, p, 3)$* , Compositio Math. **140** (2004), 1399–1416.
- [Ber-Eva-Wil] B. Berndt, R. Evans, and K. Williams, *Gauss and Jacobi Sums*, Canadian Math. Soc. series **21**, Wiley (1998).
- [Bha1] M. Bhargava, *Higher composition laws I, II, and III*, Ann. Math. **159** (2004), 217–250, 865–886, 1329–1360.
- [Bha2] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. Math. **162** (2005), 1031–1063.
- [Bha-Han] M. Bhargava and J. Hanke, *Universal quadratic forms and the 290-theorem*, Invent. Math., to appear.
- [Bilu] Yu. Bilu, *Catalan’s conjecture (after Mihailescu)*, Séminaire Bourbaki **909** (2002–2003), 1–25.
- [Bil-Han] Yu. Bilu and G. Hanrot, *Solving Thue equations of high degree*, J. Number Th. **60** (1996), 373–392.
- [Bil-Han-Vou] Yu. Bilu, G. Hanrot, and P. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, with an appendix by M. Mignotte, J. reine angew. Math. **539** (2001), 75–122.
- [Boe-Mis] J. Boéchat and M. Mischler, *La conjecture de Catalan racontée à un ami qui a le temps*, preprint available on the web at the URL <http://arxiv.org/pdf/math.NT/0502350>.
- [Bom] E. Bombieri, *Effective Diophantine approximation on \mathbf{G}_m* , Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **20** (1993), 61–89.
- [Bor-Bai] J. Borwein and D. Bailey, *Mathematics by Experiment*, A. K. Peters (2004).
- [Bor-Bai-Gir] J. Borwein, D. Bailey, and R. Girgensohn, *Experimentation in Mathematics*, A. K. Peters (2004).
- [Bor-Sha] Z. I. Borevitch and I. R. Shafarevitch, *Number Theory*, Academic Press, New York (1966).
- [Bre-Cas] A. Bremner and I. Cassels, *On the equation $Y^2 = X(X^2 + p)$* , Math. Comp. **42** (1984), 257–264.
- [Bre-Mor] A. Bremner and P. Morton, *A new characterization of the integer 5906*, Manuscripta Math. **44** (1983), 187–229.
- [Bre-Tza1] A. Bremner and N. Tzanakis, *Lucas sequences whose 12th or 9th term is a square*, J. Number Th. **107** (2004), 215–227.
- [Bre-Tza2] A. Bremner and N. Tzanakis, *On squares in Lucas sequences*, J. Number Th., to appear.
- [Bre-Tza3] A. Bremner and N. Tzanakis, *Lucas sequences whose n th term is a square or an almost square*, Acta Arith., to appear.

- [BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over \mathbb{Q} : wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.
- [Bri-Eve-Gyo] B. Brindza, J. Evertse, and K. Györy, *Bounds for the solutions of some Diophantine equations in terms of discriminants*, J. Austral. Math. Soc. (Series A) **51** (1991), 8–26.
- [Bru1] N. Bruin, *Chabauty Methods and Covering Techniques Applied to Generalized Fermat Equations*, CWI Tract **133**, CWI, Amsterdam (2002).
- [Bru2] N. Bruin, *The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$* , Compositio Math. **118** (1999), 305–321.
- [Bru3] N. Bruin, *Chabauty methods using elliptic curves*, J. reine angew. Math. **562** (2003), 27–49.
- [Bru4] N. Bruin, *Primitive solutions to $x^3 + y^9 = z^2$* , J. Number theory **111** (2005), 179–189.
- [Bru-Kra] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715–742.
- [Bug] Y. Bugeaud, *Bounds for the solutions of superelliptic equations*, Compositio Math. **107** (1997), 187–219.
- [Bug-Gyo] Y. Bugeaud and K. Györy, *Bounds for the solutions of Thue–Mahler equations and norm form equations*, Acta Arith. **74** (1996), 273–292.
- [Bug-Han] Y. Bugeaud and G. Hanrot, *Un nouveau critère pour l'équation de Catalan*, Mathematika **47** (2000), 63–73.
- [Bug-Mig] Y. Bugeaud and M. Mignotte, *On integers with identical digits*, Mathematika **46** (1999), 411–417.
- [BMS1] Y. Bugeaud, M. Mignotte, and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Annals of Math. **163** (2006), 969–1018.
- [BMS2] Y. Bugeaud, M. Mignotte, and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell equation*, Compositio Math. **142** (2006), 31–62.
- [BMS3] Y. Bugeaud, M. Mignotte, and S. Siksek, *A multi-Frey approach to some multi-parameter families of Diophantine equations*, Canadian J. Math., to appear.
- [Buh-Gro] J. Buhler and B. Gross, *Arithmetic on elliptic curves with complex multiplication II*, Invent. Math. **79** (1985), 11–29.
- [BGZ] J. Buhler, B. Gross, and D. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3*, Math. Comp. **44** (1985), 473–481.
- [Cal] E. Cali, *Points de torsion des courbes elliptiques et quartiques de Fermat*, Thesis, Univ. Paris VI (2005).
- [Can] D. Cantor, *Computing on the Jacobian of a hyperelliptic curve*, Math. Comp., **48** (1987), 95–101.
- [Cas1] J. Cassels, *Local Fields*, London Math. Soc. Student Texts **3**, Cambridge University Press (1986).
- [Cas2] J. Cassels, *Lectures on Elliptic Curves*, London Math. Soc. Student Texts **24**, Cambridge University Press (1991).
- [Cas3] J. Cassels, *On the equation $a^x - b^y = 1$, II*, Proc. Cambridge Phil. Soc. **56** (1960), 97–103.
- [Cas-Fly] J. Cassels and V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, LMS Lecture Note Series **230**, Cambridge University Press (1996).

- [Cas-Frö] J. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, New York (1967).
- [Cat] E. Catalan, *Note extraite d'une lettre adressée à l'éditeur*, J. reine angew. Math. **27**, (1844), 192.
- [Cha] C. Chabauty, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension*, C. R. A. S. Paris, **212** (1941), 1022–1024.
- [Coa-Wil] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251.
- [Coh0] H. Cohen, *A Course in Computational Algebraic Number Theory (4th corrected printing)*, Graduate Texts in Math. **138**, Springer-Verlag (2000).
- [Coh1] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Math. **193**, Springer-Verlag (2000).
- [Coh2] H. Cohen, *Variations sur un thème de Siegel et Hecke*, Acta Arith. **30** (1976), 63–93.
- [Coh3] H. Cohen, *Sums involving L-functions of quadratic characters*, Math. Ann. **217** (1975), 271–285.
- [Coh4] H. Cohen, *Continued fractions for gamma products and $\zeta(k)$* , unfinished postscript preprint available on the author's home page at <http://www.math.u-bordeaux1.fr/~cohen/>.
- [Coh-Fre] H. Cohen and G. Frey, eds., *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman & Hall/CRC press, 2005.
- [Coh-Fri] H. Cohen and E. Friedman, *Raabe's formula for p-adic gamma and zeta functions*, submitted.
- [Coh-Len] H. Cohen and H. W. Lenstra, *Heuristics on class groups of number fields*, Springer Lecture Notes in Math. **1068** (1984), 33–62.
- [Coh-Mar] H. Cohen and J. Martinet, *Class groups of number fields: numerical heuristics*, Math. Comp. **48** (1987), 123–137.
- [Coh-Rhi] H. Cohen and G. Rhin, *Accélération de la convergence de certaines récurrences linéaires*, Séminaire Th. Nombres Bordeaux (1980–1981), exposé **16**.
- [Coh-Vil-Zag] H. Cohen, F. Rodriguez-Villegas, and D. Zagier, *Convergence acceleration of alternating series*, Exp. Math. **9** (2000), 3–12.
- [Cohn1] J. Cohn, *The Diophantine equation $x^2 + C = y^n$* , Acta Arith. **65** (1993), 367–381.
- [Cohn2] J. Cohn, *The Diophantine equation $x^2 + C = y^n$, II*, Acta Arith. **109** (2003), 205–206.
- [Col] R. Coleman, *Effective Chabauty*, Duke Math. J., **52** (1985), 765–780.
- [Colm] P. Colmez, *Arithmétique de la fonction zêta*, Journées mathématiques X-UPS (2002), Publications de l'École Polytechnique, 37–164.
- [Con-Sou] J. B. Conrey and K. Soundararajan, *Real zeros of quadratic Dirichlet L-functions*, Invent. Math. **150** (2002), 1–44.
- [Con] J.-H. Conway, *The Sensual (Quadratic) Form*, Carus Math. Monographs **26**, MAA (1997).
- [Con-Slo] J.-H. Conway and N. Sloane, *Sphere Packings, Lattices and Groups (3rd ed.)*, Grundlehren der math. Wiss. **290**, Springer-Verlag, New York (1999).
- [Cre1] J. Cremona, *Computing the degree of the modular parametrization of a modular elliptic curve*, Math. Comp. **64** (1995), 1235–1250.
- [Cre2] J. Cremona, *Algorithms for Modular Elliptic Curves (2nd ed.)*, Cambridge Univ. Press (1996).

- [Cre-Pri-Sik] J. Cremona, M. Prickett, and S. Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number theory **116** (2006), 42–68.
- [Dar] H. Darmon, *Rational Points on Modular Elliptic Curves*, CBMS Regional Conference Series in Mathematics **101** (2004), American Math. Soc.
- [Dar-Gra] H. Darmon and A. Granville, *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$* , Bull. London Math. Soc. **27** (1995), 513–543.
- [Dar-Mer] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat’s Last Theorem*, J. reine angew. Math. **490** (1997), 81–100.
- [Dem1] V. Dem’yanenko, *О Суммах четырех кубов (On sums of four cubes)*, Izv. Visch. Outch. Zaved. Matematika **54** (1966), 64–69.
- [Dem2] V. Dem’yanenko, *Rational points on a class of algebraic curves*, Amer. Math. Soc. Transl. **66** (1968), 246–272.
- [Dem3] V. Dem’yanenko, *The indeterminate equations $x^6 + y^6 = az^2$, $x^6 + y^6 = az^3$, $x^4 + y^4 = az^4$* , Amer. Math. Soc. Transl. **119** (1983), 27–34.
- [Den] P. Dénes, *Über die Diophantische Gleichung $x^\ell + y^\ell = cz^\ell$* , Acta Math. **88** (1952), 241–251.
- [DeW1] B. de Weger, *Solving exponential Diophantine equations using lattice basis reduction algorithms*, J. Number Th. **26** (1987), 325–367.
- [DeW2] B. de Weger, *A hyperelliptic Diophantine equation related to imaginary quadratic number fields with class number 2*, J. reine angew. Math. **427** (1992), 137–156.
- [Dia1] J. Diamond, *The p -adic log gamma function and p -adic Euler constants*, Trans. Amer. Math. Soc. **233** (1977), 321–337.
- [Dia2] J. Diamond, *On the values of p -adic L -functions at positive integers*, Acta Arith. **35** (1979), 223–237.
- [Dia-Kra] F. Diamond and K. Kramer, *Modularity of a family of elliptic curves*, Math. Res. Lett. **2** (1995), No. 3, 299–304.
- [Dok] T. Dokchitser, *Computing special values of motivic L -functions*, Exp. Math. **13** (2004), 137–149.
- [Duq1] S. Duquesne, *Rational Points on Hyperelliptic Curves and an Explicit Weierstrass Preparation Theorem*, Manuscripta Math. **108:2** (2002), 191–204.
- [Duq2] S. Duquesne, *Calculs effectifs des points entiers et rationnels sur les courbes*, Thesis, Univ. Bordeaux I (2001).
- [Edw] J. Edwards, *Platonic solids and solutions to $x^2 + y^3 = dz^r$* , Thesis, Univ. Utrecht (2005).
- [Elk1] N. Elkies, *ABC implies Mordell*, Internat. Math. Res. Notices **7** (1991), 99–109.
- [Elk2] N. Elkies, \mathbb{Z}^{28} in $E(\mathbb{Q})$, Internet announcement on the number theory listserver (May 3rd, 2006).
- [Ell] W. Ellison and M. Mendès France, *Les nombres premiers*, Hermann (1975).
- [Erd-Wag] P. Erdős and S. Wagstaff, *The fractional parts of the Bernoulli numbers*, Illinois J. Math. **24** (1980), 104–112.
- [Eva] R. Evans, *Congruences for Jacobi sums*, J. Number Theory **71** (1998), 109–120.
- [Fal] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.
- [Fer-Gre] B. Ferrero and R. Greenberg, *On the behaviour of p -adic L -functions at $s = 0$* , Invent. Math. **50** (1978), 91–102.

- [Fly] V. Flynn, *A flexible method for applying Chabauty's Theorem*, Compositio Math. **105** (1997), 79–94.
- [Fly-Wet1] V. Flynn and J. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Math. **100** (1999), 519–533.
- [Fly-Wet2] V. Flynn and J. Wetherell, *Covering collections and a challenge problem of Serre*, Acta Arith. **98** (2001), 197–205.
- [Fre] E. Freitag, *Hilbert Modular Forms*, Springer-Verlag (1990).
- [Frö-Tay] A. Fröhlich and M. Taylor, *Algebraic Number Theory*, Cambridge Studies in Adv. Math. **27**, Cambridge Univ. Press (1991).
- [Gel] A. O. Gel'fond, *On the approximation of transcendental numbers by algebraic numbers*, Doklady Akad. Nauk SSSR **2** (1935), 177–182.
- [Gou] F. Gouvêa, *p -adic Numbers: An Introduction*, Universitext, Springer-Verlag (1993).
- [Gra-Sou] A. Granville and K. Soundararajan, *Large character sums: pre-tentious characters and the Polya–Vinogradov theorem*, Journal of the American Math. Soc., to appear.
- [Gran] D. Grant, *A curve for which Coleman's effective Chabauty bound is sharp*, Proc. Amer. Math. Soc. **122** (1994), 317–319.
- [Gras] G. Gras, *Class Field Theory: From Theory to Practice*, Springer monographs in mathematics (2003).
- [Gre-Tao] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. Math., to appear.
- [Gri-Riz] G. Grigorov and J. Rizov, *Heights on elliptic curves and the Diophantine equation $x^4 + y^4 = cz^4$* , Sophia Univ. preprint (1998).
- [Gro] B. Gross, *Heegner points on $X_0(N)$* , in Modular forms, edited by R. Rankin (1984), 87–105.
- [Gro-Kob] B. Gross and N. Koblitz, *Gauss sums and the p -adic Γ -function*, Ann. Math. **109** (1979), 569–581.
- [Guy] R. K. Guy, *Unsolved Problems in Number Theory (3rd edition)*, Problem books in math. **1**, Springer-Verlag (2004).
- [Hal-Kra1] E. Halberstadt and A. Kraus, *Sur les modules de torsion des courbes elliptiques*, Math. Ann. **310** (1998), 47–54.
- [Hal-Kra2] E. Halberstadt and A. Kraus, *Courbes de Fermat : résultats et problèmes*, J. reine angew. Math. **548** (2002), 167–234.
- [Har-Wri] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers (5th ed.)*, Oxford University Press (1979).
- [Hay] Y. Hayashi, *The Rankin's L -function and Heegner points for general discriminants*, Proc. Japan. Acad. **71** (1995), 30–32.
- [Her] G. Herglotz, *Über die Kroneckersche Grenzformel für reelle quadratische Körper I, II*, Gesam. Schr. (ed. H. Schwerdtfeger), Vandenhoeck and Ruprecht (1979), 466–484.
- [Hul] W. Hulsbergen, *Conjectures in Arithmetic Algebraic Geometry*, Aspects of math., Vieweg (1992).
- [Ire-Ros] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory (2nd ed.)*, Graduate Texts in Math. **84**, Springer-Verlag (1982).
- [Ivo1] W. Ivorra, *Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$* , Acta Arith. **108** (2003), 327–338.
- [Ivo2] W. Ivorra, *Equations diophantiennes ternaires de type $(p, p, 2)$ et courbes elliptiques*, Thesis, Univ. Paris VI (2004).
- [Ivo-Kra] W. Ivorra and A. Kraus, *Quelques résultats sur les équations $ax^p + by^p = cz^2$* , Can. J. Math., to appear.

- [Iwa-Kow] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Colloquium Publications **53**, American Math. Soc. (2004).
- [Jan] G. Janusz, *Algebraic Number Fields*, Pure and applied math. **55**, Academic Press (1973).
- [Kap] I. Kaplansky, *Ternary positive quadratic forms that represent all odd positive integers*, Acta Arith. **70** (1995), 209–214.
- [Kat1] N. Katz, *On a theorem of Ax*, Amer. J. Math. **93** (1971), 485–499.
- [Kat2] N. Katz, *The congruences of Clausen–von Staudt and Kummer for Bernoulli–Hurwitz numbers*, Math. Ann. **216** (1975), 1–4.
- [Kea] J. Keating, talk in Bordeaux, 2005.
- [Kel-Ric] W. Keller and J. Richstein, *Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$* , Math. Comp. **74** (2005), 927–936.
- [Kna] A. Knapp, *Elliptic Curves*, Math. Notes **40**, Princeton University press (1992)
- [Ko] Ko Chao, *On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$* , Sci. Sinica **14** (1965), 457–460.
- [Kob1] N. Koblitz, *p -adic Numbers, p -adic Analysis, and Zeta-Functions (2nd edition)*, Graduate Texts in Math. **58**, Springer-Verlag (1984).
- [Kob2] N. Koblitz, *An Introduction to Elliptic Curves and Modular Forms (2nd edition)*, Graduate Texts in Math. **97**, Springer-Verlag (1993).
- [Kra1] A. Kraus, *Sur l'équation $a^3 + b^3 = c^p$* , Experimental Math. **7** (1998), 1–13.
- [Kra2] A. Kraus, *On the equation $x^p + y^q = z^r$: a survey*, Ramanujan Journal **3** (1999), 315–333.
- [Kra3] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Can. J. Math. **49** (1997), 1139–1161.
- [Kra-Oes] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.
- [Kul] L. Kulesz, *Application de la méthode de Dem'janenko–Manin à certaines familles de courbes de genre 2 et 3*, J. Number Theory **76** (1999), 130–146.
- [Lan0] S. Lang, *Algebra*, Addison-Wesley, Reading, MA (1965).
- [Lan1] S. Lang, *Algebraic Number Theory (2nd ed.)*, Graduate Texts in Math. **110**, Springer-Verlag (1994).
- [Lau] M. Laurent, *Linear form in two logarithms and interpolation determinants*, Acta Arith. **66** (1994), 181–199.
- [Lau-Mig-Nes] M. Laurent, M. Mignotte, and Yu. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory **55** (1995), 255–265.
- [Leb] V. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$* , Nouv. Ann. Math. **9** (1850), 178–181.
- [Lem] F. Lemmermeyer, *Kronecker–Weber via Stickelberger*, preprint.
- [Ma] D.-G. Ma, *An elementary proof of the solution to the Diophantine equation $6y^2 = x(x+1)(2x+1)$* , Sichuan Daxue Xuebao **4** (1985) 107–116.
- [Man] Yu. Manin, *The p -torsion of elliptic curves is uniformly bounded*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 459–465; Amer. Math. Soc. Transl. 433–438.
- [Mar] J. Martinet, *Perfect Lattices in Euclidean Spaces*, Grundlehren der math. Wiss. **327**, Springer (2003).
- [Marc] D. A. Marcus, *Number Fields*, Springer-Verlag, New York (1977).
- [Mart] G. Martin, *Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$* , J. Number Theory **112** (2005), 298–331.

- [Mat] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125–180. English transl. in Izv. Math. **64** (2000), 1217–1269.
- [Maz] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
- [McC] W. McCallum, *On the method of Coleman and Chabauty*, Math. Ann. **299** (1994), 565–596.
- [Mes-Oes] J.-F. Mestre and J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m -ième*, J. reine angew. Math. **400** (1989), 173–184.
- [Mig] M. Mignotte, *A note on the equation $ax^n - by^n = c$* , Acta Arith. **75** (1996), 287–295.
- [Mig-Weg] M. Mignotte and B. de Weger, *On the Diophantine equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$* , Glasgow Math. J. **38** (1996), 77–85.
- [Mom] F. Momose, *Rational points on the modular curves $X_{split}(p)$* , Compositio Math. **52** (1984), 115–137.
- [Mon-Vau] H. Montgomery and R. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math. **43** (1977), 69–82.
- [Mord] L. Mordell, *Diophantine Equations*, Pure and applied Math. **30**, Academic Press (1969).
- [Mori] M. Mori, *Developments in the double exponential formula for numerical integration*, in Proceedings ICM 1990, Springer-Verlag (1991), 1585–1594.
- [Morit1] Y. Morita, *A p -adic analogue of the Γ -function*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **22** (1975), 255–266.
- [Morit2] Y. Morita, *On the Hurwitz–Lerch L -functions*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **24** (1977), 29–43.
- [Nak-Tag] Y. Nakajima and Y. Taguchi, *A generalization of the Chowla–Selberg formula*, J. reine angew. Math. **419** (1991), 119–124.
- [New] D. Newman, *Analytic Number Theory (2nd corrected printing)*, Graduate Texts in Math. **177**, Springer-Verlag (2000).
- [Pap] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3*, J. Number Theory **44** (1993), 119–152.
- [Poo-Sch-Sto] B. Poonen, E. Schaefer, and M. Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$* , Duke Math. J., to appear.
- [Poo-Wil] A. van der Poorten and K. Williams, *Values of the Dedekind eta function at quadratic irrationalities*, Canadian Jour. Math. **51** (1999), 176–224, corrigendum **53** (2001), 434–448.
- [Rap-Sch-Sch] M. Rapoport, N. Schappacher, and P. Schneider, *Beilinson’s Conjectures on Special Values of L -Functions*, Perspectives in Math. **4** (1988), Academic Press.
- [Rib1] K. Ribet, *On modular representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms*, Invent. Math. **100** (1990), 431–476.
- [Rib2] K. Ribet, *On the equation $a^p + 2b^p + c^p = 0$* , Acta Arith. **LXXIX.1** (1997), 7–15.
- [Rob1] A. Robert, *A Course in p -adic Analysis*, Graduate Texts in Math. **198**, Springer-Verlag (2000).
- [Rob2] A. Robert, *The Gross–Koblitz formula revisited*, Rend. Sem. Math. Univ. Padova **105** (2001), 157–170.

- [Rod-Zag] F. Rodriguez-Villegas and D. Zagier, *Which primes are sums of two cubes?*, Canadian Math. Soc. Conference proceedings **15** (1995), 295–306.
- [Ruc] H.-G. Rück, *A note on elliptic curves over finite fields*, Math. Comp. **49** (1987), 301–304.
- [Rud] W. Rudin, *Real and Complex Analysis*, Mc Graw Hill (1970).
- [Sam] P. Samuel, *Théorie Algébrique des Nombres*, Hermann, Paris (1971).
- [Sch] E. Shaefer, *2-descent on the Jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), 219–232.
- [Sch-Sto] E. Schaefer and M. Stoll, *How to do a p -descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), 1209–1231.
- [Scho] R. Schoof, *Class groups of real cyclotomic fields of prime conductor*, Math. Comp. **72** (2003), 913–937 (see also the errata on Schoof's home page).
- [Sel1] E. S. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$* , Acta Math. **85** (1951), 203–362.
- [Sel2] E. S. Selmer, *Completion of the tables*, Acta Math. **92** (1954), 191–197.
- [Ser1] J.-P. Serre, *Cours d'arithmétique*, P.U.F., Paris (1970). English translation: Graduate Texts in Math. **7**, Springer-Verlag (1973).
- [Ser2] J.-P. Serre, *Corps locaux (2nd ed.)*, Hermann, Paris (1968). English translation: Graduate Texts in Math. **67**, Springer-Verlag (1979).
- [Ser3] J.-P. Serre, *Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Math. J. **54** (1987) 179–230.
- [Ser4] J.-P. Serre, *Abelian ℓ -adic Representations and Elliptic Curves*, W. A. Benjamin, New York, 1968.
- [Ses] J. Sesanio, *Books IV to VII of Diophantus's Arithmetica in the Arabic Translation Attributed to Qusta ibn Luqa*, Sources in the History of Mathematics and Physical Sciences **3**, Springer-Verlag (1982).
- [Shi] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwami Shoten (1971).
- [Sho-Tij] T. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics **87**, Cambridge University Press (1986).
- [Sik] S. Siksek, *On the Diophantine equation $x^2 = y^p + 2^k z^p$* , Journal de Théorie des Nombres de Bordeaux **15** (2003), 839–846.
- [Sik-Cre] S. Siksek and J. Cremona, *On the Diophantine equation $x^2 + 7 = y^m$* , Acta Arith. **109** (2003), 143–149.
- [Sil1] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer-Verlag (1986).
- [Sil2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math. **151**, Springer-Verlag (1994).
- [Sil3] J. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), 723–743.
- [Sil4] J. Silverman, *Rational points on certain families of curves of genus at least 2*, Proc. London Math. Soc. **55** (1987), 465–481.
- [Sil-Tat] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Math., Springer-Verlag (1992).
- [Sim1] D. Simon, *Solving quadratic equations using reduced unimodular quadratic forms*, Math. Comp. **74** (2005), 1531–1543.
- [Sim2] D. Simon, *Computing the rank of elliptic curves over a number field*, LMS J. Comput. Math. **5** (2002), 7–17.

- [Sma] N. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Math. Soc. Student Texts **41** (1998).
- [Sta1] H. Stark, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. **23** (1974), 135–152.
- [Sta2] H. Stark, *Class numbers of complex quadratic fields*, in Modular Forms in One Variable I, Springer Lecture Notes in Math **320** (1973), 153–174.
- [Sto] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), 245–277.
- [Sug] T. Sugatani, *Rings of convergent power series and Weierstrass preparation theorem*, Nagoya Math. J. **81** (1981), 73–78.
- [Swd] H.-P.-F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory*, London Math. Soc. Student Texts **50**, Cambridge University Press (2001).
- [Tak-Mor] H. Takashi and M. Mori, *Double exponential formulas for numerical integration*, Publications of RIMS, Kyoto University (1974), 9:721–741.
- [Tay] P. Taylor, *On the Riemann zeta function*, Quart. J. Math., Oxford Ser. **16** (1945), 1–21.
- [Tay-Wil] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.
- [Ten] S. Tengely, *On the Diophantine equation $F(x) = G(y)$* , Acta Arith. **110** (2003), 185–200.
- [Tij] R. Tijdeman, *On the equation of Catalan*, Acta Arith. **29** (1976), 197–209.
- [Tun] J. Tunnell, *A classical Diophantine problem and modular forms of weight $3/2$* , Invent. Math. **72** (1983), 323–334.
- [Tza-Weg] N. Tzanakis and B. de Weger, *On the practical solution of the Thue Equation*, J. Number Th. **31** (1989), 99–132.
- [Vel] J. Vélú, *Isogénies entre courbes elliptiques*, Comptes Rendus Acad. Sc. Paris Sér. A **273** (1971), 238–241.
- [Wald1] M. Waldschmidt, *Minorations de combinaisons linéaires de logarithmes de nombres algébriques*, Canadian J. Math. **45** (1993), 176–224.
- [Wald2] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups*, Grundlehren der math. Wiss. **326** (2000), Springer-Verlag.
- [Wals] P. G. Walsh, *A quantitative version of Runge’s theorem on Diophantine equations*, Acta Arith. **62** (1992), 157–172.
- [Was] L. Washington, *Introduction to Cyclotomic Fields (2nd ed.)*, Graduate Texts in Math. **83**, Springer-Verlag (1997).
- [Watk] M. Watkins, *Real zeros of real odd Dirichlet L -functions*, Math. Comp. **73** (2004), 415–423.
- [Wats] G. Watson, *A Treatise on the Theory of Bessel Functions (2nd ed.)*, Cambridge Univ. Press (1966).
- [Wet] J. Wetherell, *Bounding the Number of Rational Points on Certain Curves of High Rank*, PhD thesis, Univ. California Berkeley (1997).
- [Wil] A. Wiles, *Modular elliptic curves and Fermat’s last theorem*, Annals of Math. **141** (1995), 443–551.
- [Yam] Y. Yamamoto, *Real quadratic number fields with large fundamental units*, Osaka J. Math. **8** (1971), 261–270.
- [Zag] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), 372–384.

Index of Notation

Page numbers in Roman type refer to the current volume, while italicized page numbers refer to the complementary volume.

Symbols

$\ \cdot \ $	an absolute value on a field, or a norm, 183
$ \cdot $	usually a \mathfrak{p} -adic absolute value, 183
$\mathbf{1}$	the constant arithmetic function 1, 152

A

$]a, b[$	open interval with endpoints a and b , ix, <i>ix</i>
$(a, b)_p$	local Hilbert symbol at $p \leq \infty$, 295
$[a, b[,]a, b]$	half-open intervals with endpoints a and b , ix, <i>ix</i>
$a * b$	arithmetic convolution of a and b , 152
AGM	arithmetic–geometric mean, 486
$A_p(t)$	set linked to $y^2 = x^p + t$, 411
$\text{Arg}(z)$	principal determination of the argument of z , 169

B

$B(a, b)$	beta function, 93
$\binom{a}{k}$	generalized binomial coefficient, ix, <i>ix</i>
$B_k(\chi)$	χ -Bernoulli number, 43
$B_{k,p}$	p -adic Bernoulli numbers, 308
$B_k(x), B_k$	Bernoulli polynomial, number, 3

C

$\lceil x \rceil$	ceiling of x , ix, <i>ix</i>
c_ℓ	Fourier coefficient of a newform, 498
$\text{III}(E)$	Tate–Shafarevich group of E , 479, 522, 555
$\chi(n)$	often a Dirichlet character at n , 156
$\chi_D(n)$	Kronecker–Legendre symbol $\left(\frac{D}{n}\right)$, 317
χ^-	$\chi^-(n) = \chi(-n)$, 43
$\text{Cl}(K)$	class group of K , 131

$Cl_T(K)$	T -class group of K , 550
C_n	cyclic group of order n , 114
\mathbb{C}_p	the completion of the algebraic closure of \mathbb{Q}_p , 260
$c_p(E)$	Tamagawa number, 522
$\langle g \rangle$	cyclic group generated by g , 145

D

$d(n)$	number of divisors of n , 157
$\delta(n)$	Kronecker's δ function, 156
$\delta_{k,1}$	1 if $k = 1$, 0 otherwise, 4
$\langle x \rangle$	$x/\omega_v(x)$, diamond of x , 229
$\text{disc}(E)$	discriminant of elliptic curve E , 466
$\mathfrak{d}(L/K)$	relative discriminant of L/K , 130
$d(\Lambda, \mathbf{y})$	distance from \mathbf{y} to the nearest vector of Λ distinct from \mathbf{y} , 58
$d \mid n$	d is a positive divisor of n , ix, ix, 152
$d \parallel n$	$d \mid n$ and $\text{gcd}(d, n/d) = 1$, ix, ix, 155
$D_{\pi, f}(X)$	Dwork power series generalized to p^f , 256
$D_{\pi}(X)$	Dwork power series, 255
$D(\mathfrak{P}/\mathfrak{p})$	decomposition group of $\mathfrak{P}/\mathfrak{p}$, 134

E

E^0	noncompact component of $E(\mathbb{R})$, 485
$E_1(x)$	exponential integral, 574
e_1, e_2, e_3	roots of $4X^3 - g_2X - g_3 = 0$, 484
E^{gg}	the egg, compact component of $E(\mathbb{R})$, 485
$e(\mathfrak{P}/\mathfrak{p})$	ramification index of $\mathfrak{P}/\mathfrak{p}$, 132
$\varepsilon((a_1, \dots, a_n))$	ε -invariant of a quadratic form, 300
$\varepsilon(E)$	sign of the functional equation, root number, 521
$E_p(X)$	Artin–Hasse exponential, 217
$E \sim_p f$	E arises modulo p from f , 498
$\eta(\tau)$	Dedekind's eta function, 215
$\exp_{\mathfrak{p}}(x)$	\mathfrak{p} -adic exponential, 211

F

E, \mathbb{F}	general finite fields, sometimes their algebraic closure, x, x
$f(\chi), f$	conductor of Dirichlet character χ , 25
$\mathcal{F}(f), \widehat{f}$	Fourier transform of f , 104, 107
$\lfloor x \rfloor$	floor of x , ix, ix
F_n	usually the Fibonacci sequence, 421
$f(\mathfrak{P}/\mathfrak{p})$	residual degree of $\mathfrak{P}/\mathfrak{p}$, 132
$\{x\}$	$x - \lfloor x \rfloor$, fractional part of x , ix, ix

G

G	usually a group, also Catalan's constant, 127
g	sometimes the genus of a curve, 90, 441
g	sometimes the number of prime ideals above \mathfrak{p} , 134
G_0	group of points reducing to a nonsingular point, 507
G_1	group of points reducing to \overline{O} , 508
$g_2(\Lambda)$	g_2 -invariant of lattice Λ , 483
$g_3(\Lambda)$	g_3 -invariant of lattice Λ , 483
γ	usually Euler's constant, 33
$\Gamma_p(s)$	p -adic gamma function at s , 368
$\Gamma_r(s, x)$	higher incomplete gamma function, 574
$\gamma(s)$	$\pi^{-s/2}\Gamma(s/2)$, 172
$\Gamma(s, x)$	incomplete gamma function, 573
$\Gamma(x)$	gamma function at x , 78
$\gamma_p(\chi)$, γ_p	p -adic Euler constants, 308
$\gcd(a, b)$, GCD	greatest common divisor, viii, viii
$\gcd(a, b^\infty)$	limit of $\gcd(a, b^n)$, ix, ix
G_N	group of points of level $\geq N$, 508
$G(\tau, s)$	nonholomorphic Eisenstein series, 211

H

H^\perp	orthogonal of H in V , 286
$h(D)$	class number of quadratic order of discriminant D , 318
$h(E)$	height of the elliptic curve E , 603
H_k	$\sum_{1 \leq j \leq k} 1/j$, harmonic sum, 110
$h(K)$, h	class number of K , 131
H_n	$\sum_{1 \leq k \leq n} 1/k$, 85
H_n	harmonic sum $\sum_{1 \leq j \leq n} 1/j$, 128
HNF	Hermite normal form, 16, 340
$h(P)$	naïve height of a point $P \in E(\mathbb{Q})$, 530
$\widehat{h}(P)$	canonical height of $P \in E(\mathbb{Q})$, 530
h_p	class number of $\mathbb{Q}(\zeta_p)$, 432
h_{p^k}	class number of $\mathbb{Q}(\zeta_{p^k})$, 148
$h_{p^k}^-$	minus class number of p^k th cyclotomic field, 149
$h_{p^k}^+$	class number of maximal totally real subfield, 148
$H(p, t)$, $H(t)$	conditions for $y^2 = x^p + t$, 411

I

$\Im(s)$	imaginary part of s , ix, ix
$I(\mathfrak{P}/\mathfrak{p})$	inertia group of $\mathfrak{P}/\mathfrak{p}$, 134
$I_s(m)$, I_s	Stickelberger ideal, 160

J

$J(\chi_1, \chi_2)$	Jacobi sum associated with two characters, 82
$j(E)$	j -invariant of elliptic curve E , 467
$J_k(\chi_1, \dots, \chi_k)$	Jacobi sum, 79

K

K	usually a number field, x, x
\mathcal{K}	a general \mathfrak{p} -adic field, $x, x, 235$
$K_n(F)$	higher K -groups, 244
$K_{\mathfrak{p}}$	completion of K at the prime ideal \mathfrak{p} , $x, x, 195$
$K(T, 2)$	same as $S_T(K)$, 551

L

L	usually a number field, x, x
$\Lambda(\chi, s)$	completed L -function for χ , 172
$\Lambda(E, s)$	completed L -function of an elliptic curve, 521
$\Lambda(n)$	von Mangoldt's function, 159
$\lambda(N)$	Carmichael's function of N , 93
$L(a, s)$	Dirichlet series associated with a , 151
\mathcal{L}	a general \mathfrak{p} -adic field, x, x
$L(\chi, s)$	L -series of character χ , 162
$\text{lcm}(a, b)$, LCM	least common multiple, viii, viii
$L(E_D, s)$	L -function of elliptic curve E twisted by D , 590
$\left(\frac{a}{p}\right), \left(\frac{m}{n}\right), \left(\frac{a}{b}\right)$	Legendre, Jacobi, or Kronecker symbol, 33
$\left(\frac{a}{b}\right)_m$	m th power reciprocity symbol, 166
$\mathcal{L}(f)$	Laplace transform of f , 108
$\mathcal{L}_F(E)$	space of F -linear maps from E to E , 118
$\text{Log}\Gamma_p(x)$	Diamond's log gamma function for $x \in \mathbb{Z}_p$, 330
$\text{Log}\Gamma_p(\chi, x)$	Morita's log gamma function for $x \in \mathbb{Z}_p$, 337
$\text{Log}\Gamma(s)$	complex log gamma function at s , 81
L^H	fixed field of L by H , 104
Li_2	dilogarithm function, 278, 404
Li_k	polylogarithm function, 278
$\text{Li}(x)$	logarithm integral, 257
$[L : K]$	the degree of L over K , or the index of K in L , 107
L_n	usually the Lucas sequence, 421
$\log_{\mathfrak{p}}(x)$	\mathfrak{p} -adic logarithm, 211
$L_p(\chi, s)$	p -adic L -function of character χ , 301

M

$\mathcal{M}(f)$	Mellin transform of f , 107
$\mu(n)$	Möbius function of n , 153
μ_n	group of roots of unity of order n , 18
$\mu_n = \mu_n(K)$	subgroup of n th roots of unity in K , 112
$\mu_{\mathfrak{p}}$	group of $(\mathcal{N}_{\mathfrak{p}} - 1)$ st roots of unity in $K_{\mathfrak{p}}$, 228

N

- $\lfloor x \rfloor$ nearest integer to x , ix, *ix*
- $\mathcal{N}\mathfrak{p}$ the absolute norm of a prime ideal \mathfrak{p} , 191
- $\left[\begin{smallmatrix} n \\ x \end{smallmatrix} \right]$ $1 \cdot 2 \cdots n / (x(x+1) \cdots (x+n))$, 281

O

- \mathcal{O} identity element of an elliptic curve, 473
- $\Omega(n)$ number of prime divisors of n with multiplicity, 156
- ω Teichmüller character, 391
- $\omega(n)$ number of distinct prime divisors of n , 156
- $\omega_{\mathfrak{P}}(x)$ $(q-1)$ st root of 1 congruent to $x \pmod{\mathfrak{P}}$, 152
- $\omega_v(a)$ extension of Teichmüller character to \mathbb{Q}_p^* , 281
- $\omega(x)$ Teichmüller character of x , 227, 228
- $\langle x \rangle$ $x/\omega(x) \in U_1$, 229
- ord_P order of the point P , 443

P

- $\Phi f(x, y)$ $(f(x) - f(y))/(x - y)$, 277
- $\phi(n)$ Euler's ϕ function, 141
- Π a uniformizer of a prime ideal in an extension, 432
- π either a uniformizer of a prime ideal, or 3.14... , 432
- PID principal ideal domain, 106, 129
- $\prod^{(p)}$ product over integers prime to p , 302
- ψ_b $x \mapsto \zeta_p^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(bx)}$, 75
- $\psi_p(x)$ $\text{Log}\Gamma'_p(x)$, Diamond's p -adic ψ function, 331
- $\psi(x)$ logarithmic derivative of $\Gamma(x)$, 76
- $\wp(z)$ Weierstrass \wp function, 482

Q

- \mathbb{Q}_p completion of \mathbb{Q} at p , the field of p -adic numbers, 195

R

- r_1 number of real embeddings of a number field, 107
- r_2 half the number of nonreal embeddings of a number field, 107
- $R(A, B)$ resultant of polynomials A and B , 143
- $\text{rad}(N)$ radical of the integer or polynomial N , 483
- $R(E)$ regulator of the elliptic curve E , 522, 601
- $\Re(s)$ real part of s , ix, *ix*
- $r_k(n)$ number of representations of n as a sum of k squares, 317
- $r_Q(n)$ number of representations of n by Q , 215

S

$S^1(X)$, $S^1(\mathbb{Z}_p)$	strictly differentiable functions, 277
$S_2(E)$	2-Selmer group of E , 555
$S(a, b; p)$	Kloosterman sum, 100
$s \setminus p$	$(s - a_0(s))/p$, essentially $\lfloor s/p \rfloor$, 365
$\sigma(n)$	sum of divisors of n , 157
$\sigma_k(n)$	sum of k th powers of divisors of n , 157, 317
$s(N)$	sometimes the squarefree part of N , 541
$s_p(n)$, $s(n)$	sum of the digits of n in base p , 155, 207
$S_T(K)$	T -Selmer group of number field K , 551
$\sum^{(p)}$	sum over integers prime to p , 302

T

τ	often an element of the upper half-plane \mathcal{H} , 586
$\tau(\chi)$, $\tau(\chi, a)$	Gauss sum for multiplicative character χ , 31
$\tau(\chi, \psi)$	Gauss sum with additive character ψ , 75
$\tau(n)$	Ramanujan τ function, 159
$\tau_q(r)$	Gauss sum associated with a Dwork character, 386
$\theta(\chi, \tau)$	theta function of character χ , 170
$t(n)$	product of factorials of digits of n in base p , 155

U

U_0	the group of \mathfrak{p} -adic units, 226
U_1	group of \mathfrak{p} -adic units congruent to 1 mod \mathfrak{p} , 228
U_i	group of \mathfrak{p} -adic units congruent to 1 mod \mathfrak{p}^i , 228
$U(K)$	unit group of K , 131
$U_T(K)$	T -unit group of K , 550
$\langle u \rangle$	distance from u to the nearest integer, 58

W

$W(\chi)$	root number of modulus 1, 49
W_Q	Atkin–Lehner operator, 596

Z

$\mathbb{Z}_{\geq 0}$	nonnegative integers, ix, ix
ζ	usually a primitive p th root of unity, 432
$\zeta_C(T)$	zeta function of a curve or variety C , 91
$\zeta_K(s)$	Dedekind zeta function of a number field, 216
$\zeta_p(s, x)$	p -adic Hurwitz zeta function, 283
$\zeta_Q(s)$	Epstein zeta function for the quadratic form Q , 215
$\zeta(s)$	Riemann zeta function, 72, 153
$\zeta(s, z)$	Hurwitz zeta function, 71, 168, 190
$\mathbb{Z}_{> 0}$	strictly positive integers, ix, ix

$\mathbb{Z}_K, \mathbb{Z}_L$	ring of algebraic integers of K, L , <i>x, x</i> , 128
$\mathbb{Z}_{\leq 0}$	negative or zero integers, <i>ix, ix</i>
$\mathbb{Z}_{< 0}$	strictly negative integers, <i>ix, ix</i>
ζ_n	a primitive n th root of unity, 17
$\mathbb{Z}_p, \mathbb{Z}_{\mathfrak{p}}$	the ring of p -adic or \mathfrak{p} -adic integers, 195
$z(\mathfrak{p})$	$\lfloor e(\mathfrak{p}/p)/(p-1) \rfloor + 1$, 229
ζ_π	p th root of 1 congruent to $1 + \pi \pmod{\mathfrak{p}^2}$, 256
$\zeta_p(s)$	Kubota–Leopoldt p -adic zeta function, 301

Index of Names

Page numbers in Roman type refer to the current volume, while italicized page numbers refer to the complementary volume.

A

Abel, N., 30, 200, 251, 256
Abouzaid, M., *417*
Adams, J., 67, 325
Alford, R., *94*
Almkvist, G., 69
Alpern, D., *384*
Amice, Y., 276
Apéry, R., 99, 141
Apostol, T., *94*
Arnold, V., 121
Artin, E., *70, 115, 167, 217, 219*
Atkin, O., *565, 596, 613*
Ax, J., *73*

B

Baker, A., viii, *viii, 2, 411, 414, 424, 424, 517, 519, 600, 603*
Balasubramanian, R., *4*
Balog, A., 133
Barnes, E., 135
Batut, C., 11, 99
Beck, M., *380*
Beilinson, A., 245
Belabas, K., x, *x*
Belyi, G., 478
Bender, C., 99
Bennett, M., x, *x, 339, 416, 423, 490, 523*
Bernardi, D., x, *x*

Bernoulli, J., 3, 264
Bessel, F., 111
Beukers, F., 275, 400, 463
Beurling, A., 137
Bhargava, M., *107, 313*
Bilu, Yu., viii, *viii, 3, 413, 417, 436, 442, 483, 529, 532*
Binet, J., 125
Birch, B., vi, *vi, 3, 245, 452, 518, 522, 528, 586*
Blichfeldt, H., *63*
Bloch, S., 245
Boéchat, J., viii, *viii, 442, 529*
Borel, A., 244
Borevich, Z., x, *x*
Bourbaki, N., 21
Brauer, R., 242
Bremner, A., *410, 462, 608, 614*
Breuil, C., 2, 242, 498
Brindza, B., 437
Bruin, N., 456, 486, 489
Brumer, A., 501
Buchmann, J., *357*
Bugeaud, Y., viii, *viii, 411, 424, 518*
Bump, D., 262

C

Cantor, D., 447
Cardano, G., *561*
Carlitz, L., 326

Carmichael, R., 93
 Cassels, I., *x, x, 2, 283, 311, 330, 359, 443, 465, 609, 614*
 Catalan, E., 2, 127, 428, 442
 Cauchy, A.-L., 188, 269, 440
 Čebotarev, N., 325, 514
 Čebyshev, P., 276
 Chabauty, C., 452, 489
 Chein, E., 445
 Chen, I., 490
 Chevalley, C., 72
 Chowla, S., 223
 Clausen, T., 63, 325
 Coates, J., 245, 522
 Cohen, H., 41, 99, 140, 195, 198
 Cohn, J., 410, 424
 Coleman, R., 452
 Colliot-Thélène, J.-L., 327
 Colmez, P., 275, 276, 301, 346
 Conrad, B., 2, 242, 259, 498
 Conrey, B., 137, 239
 Conway, J., 51
 Cremona, J., *x, x, 476, 488, 498, 523, 555, 557, 596, 598*

D

Dénes, P., 506
 Darmon, H., 133, 465, 482, 490, 504, 506, 509
 Davenport, H., 82, 173, 174, 182, 311, 394, 424, 427, 493
 David, S., 517, 603
 Dedekind, R., 117, 127, 131, 215, 216
 Delaunay, C., *x, x, 584, 598*
 Deligne, P., 4, 11, 92, 160, 240, 335, 496, 498
 Delone, B., 386
 Dem'yanenko, V., 376, 381, 408, 450
 Deshouillers, J.-M., 4
 Deuring, M., 497, 588
 Diamond, F., 2, 242, 498, 501
 Diamond, J., 281, 330

Dirac, P., 22, 178
 Dirichlet, P.-G. Lejeune, 1, 138, 237
 Dress, F., 4
 Dupuy, B., 532
 Duquesne, S., viii, viii, *x, x, 441, 459*
 Dwork, B., 217, 240, 255, 375, 388

E

Edwards, J., 463, 480
 Eichler, M., 198
 Eisenstein, G., 159, 170, 193, 201, 211, 264, 434
 Elkies, N., 55, 276, 378, 385, 482, 518, 565
 Ellenberg, J., 424, 490
 Epstein, P., 210, 215
 Erdős, P., 246
 Euler, L., 6, 19, 21, 77, 141, 154, 267, 338, 387
 Evertse, J., 437

F

Faltings, G., vii, vii, 2, 92, 368, 449, 482, 498, 518, 521
 Fel'dman, N., 411
 Fermat, P., 55, 314, 338, 415, 424, 427, 482, 503, 517, 518
 Ferrero, B., 389
 Fibonacci, L., 421
 Fisher, T., 369, 557
 Flynn, V., 409, 449, 453, 456, 460
 Fourier, J., 45, 104, 148, 269
 Frey, G., 2, 495, 503
 Fricke, R., 587
 Friedman, E., 275, 287, 395
 Frobenius, G., 69, 180, 498
 Fubini, G., 28
 Furtwängler, P., 434

G

Galois, E., 101

Gauss, C.-F., 2, 31, 75, 124, 149,
245, 315, 338, 347, 406
 Germain, S., 430
 Glaisher, J., 133
 Goldbach, C., 455
 Goldfeld, D., 139, 523
 Grant, D., 452
 Granville, A., 94, 268, 482
 Gras, G., 321
 Green, B., 238
 Greenberg, R., 389
 Gross, B., 139, 245, 383, 386, 522,
571, 583, 588, 590
 Grothendieck, A., 3, 463, 478
 Guy, R., 455
 Györy, K., 437

H

Hadamard, J., 52, 85, 246, 248
 Halberstadt, E., 506, 521
 Hall, P., 493
 Hanke, J., 313
 Hanrot, G., viii, viii, 411, 413, 417,
436
 Hardy, G. H., 4
 Hasse, H., 6, 82, 91, 98, 173, 174,
182, 217, 305, 318, 326, 394, 494
 Hayashi, Y., 591
 Hecke, E., 193, 217, 242
 Heegner, K., 528, 584, 586
 Hellegouarch, Y., 2, 495, 503
 Henniart, G., 521
 Hensel, K., v, v, 5, 199, 202
 Herbrand, J., 245
 Herglotz, G., 271
 Hermite, C., 54, 70
 Hilbert, D., vii, vii, 4, 118, 193
 Houriet, J., 312, 330, 331
 Hurwitz, A., 71, 168, 198, 264
 Huxley, M., 182
 Hyrö, S., 448

I

Ireland, K., x, x, 64

Iwaniec, H., 246, 254
 Iwasawa, K., 264, 346

J

Jacobi, C. G., 36
 Jacobstahl, E., 381
 Jaulent, J.-F., x, x, 144

K

Kaneko, M., 119
 Kato, K., 245
 Katz, N., 73, 383
 Kazandzidis, G., 381
 Klein, F., 478, 489
 Kloosterman, H., 100
 Knapp, A., 494
 Ko, Chao, 445, 517
 Koblitz, N., 383, 386, 450
 Kodaira, K., 597
 Kohlen, W., 195
 Kolyvagin, V., 245, 522
 Korobov, N., 250
 Kowalski, E., 246
 Kramer, K., 501
 Krasner, M., 189, 238, 267, 269,
346
 Kraus, A., x, x, 429, 430, 490, 499,
506, 511, 513, 514, 523
 Kronecker, L., 36, 128, 140, 145,
146, 167, 213, 229
 Kubota, T., 301
 Kummer, E., 1, 68, 133, 324, 338,
436

L

Lagrange, J.-L., 4, 315
 Landau, E., 314
 Langlands, R., 167, 242
 Laplace, P.-S., 28, 104, 108
 Laurent, M., 414
 Laurent, P.-A., 13
 Lebesgue, H., 106
 Lebesgue, V.-A., 418
 Lech, C., 283

Legendre, A.-M., 2, 33, 245, 347
 Lehner, J., 596, 613
 Lemmermeyer, F., 181
 Lenstra, A., 56
 Lenstra, H. W., 3, 56, 140, 180,
 607
 Leopoldt, H., 301
 Lerch, M., 223
 Lichtenbaum, S., 244
 Lind, C., 328
 Liouville, J., 264, 413, 483
 Lipschitz, R., 277
 Littlewood, J., 4
 Ljunggren, W., 424
 Lovasz, L., 56
 Lucas, E., 11, 421, 424
 Lutz, E., 524

M

Ma, D.-G., 426
 MacLaurin, C., 19, 21
 Mahler, K., 221, 283, 375
 von Mangoldt, H., 159
 Manin, Yu., 358, 450, 457, 494,
 586
 Marcus, D., 218
 Martinet, J., x, x, 51
 Mason, R., 491
 Masser, D., 482
 Matiyasevich, Yu., vii, vii
 Mazur, B., 501, 511, 513, 528
 McCallum, W., 452
 Mellin, R., 104, 107
 Merel, L., 490, 504, 506, 509
 Mertens, F., 268
 Mestre, J.-F., 518, 521, 565, 566,
 608
 Meurman, A., 69
 Meyer, C., 271
 Mignotte, M., viii, viii, 283, 411,
 414, 420, 424, 518
 Mihăilescu, P., viii, viii, 2, 428,
 442, 483, 531
 Minkowski, H., 63, 305

Mischler, M., viii, viii, 442, 483,
 529
 Möbius, A., 153
 de Moivre, A., 143
 Momiyama, H., 119
 Montgomery, H., 200
 Mordell, L., 2, 92, 159, 368, 384,
 449, 452, 455, 482, 498, 517, 518,
 538, 554
 Mori, M., 37
 Morita, Y., 330, 336, 364
 Morton, P., 410
 Mumford, D., 446
 Muzzafar, H., 271

N

Nagell, T., 273, 444, 524
 Nakayama, T., 231
 Newman, D., 246, 250
 Noether, E., 110

O

Oesterlé, J., 482, 499
 Olivier, M., 99
 Ono, K., 133
 Ostrowski, A., 190

P

Padé, H., 141
 Pascal, B., 118
 Pell, J., 229, 354
 Pethő, A., 417
 Pfister, A., 329
 Picard, É., 445
 Pine, E., 380
 Plana, G., 30
 Poisson, S., 45
 Pólya, G., 198
 Pomerance, C., 94
 Poonen, B., 489

R

Raabe, C., 103
 Ramakrishnan, D., 490

Ramanujan, S., 26, 153, 159, 241, 496
 Rhin, G., 99
 Ribet, K., viii, *viii*, 2, 335, 339, 424, 489, 490, 498, 500, 504, 521
 Riccati, J., 611
 Riemann, B., 106, 153, 159, 245, 442, 465, 473
 Rivat, J., 137
 Robert, A., 383
 Roch, G., 442, 465
 Rodriguez-Villegas, F., x, *x*, 41, 275, 277, 375, 378
 Rosen, M., x, *x*, 64
 Roth, K., 432
 Rubin, K., 245, 522
 Runge, C., 439

S

Saias, E., 94
 Sansone, G., 609
 Schaefer, E., 489
 Schinzel, A., 384, 437
 Schlömilch, O., 148
 Scholl, T., 245
 Schoof, R., viii, *viii*, 150, 387, 442, 443, 529, 565, 609
 Schreier, O., 70, 115
 Schwartz, L., 177
 Seidel, P., 11
 Selberg, A., 137, 223, 243, 246
 Selmer, E., 359, 368, 551, 555
 Serre, J.-P., x, *x*, 346, 409, 456, 501, 511
 Shafarevich, I., x, *x*, 306, 479, 498, 522, 555
 Shanks, D., 34, 357, 565, 566
 Shimura, G., 195, 270, 497, 518, 521, 588, 589
 Shorey, T., 414, 423
 Siegel, C. L., 139, 193, 194, 218, 239, 437, 517–519
 Siksek, S., viii, *viii*, 328, 332, 339, 424, 490, 495, 518

Silverman, J., 465, 596
 Simon, D., x, *x*, 347, 553
 Skinner, C., 490, 523
 Skolem, T., 385
 Sloane, N., 51
 Smart, N., 517, 600, 603
 Sondow, J., 140, 260
 Soundararajan, K., 200, 239
 Stark, H., 95, 193, 245, 273, 528
 von Staudt, K., 63, 325
 Stein, W., 495
 Stickelberger, L., 155, 162, 259, 390, 391
 Stieltjes, T., 99, 251
 Stirling, J., 34, 82, 125, 222, 268, 282
 Stoll, M., 328, 367, 489, 493
 Strassmann, R., 266
 Swan, R., 259
 Swinnerton-Dyer, P., vi, *vi*, 3, 245, 452, 518, 522, 528

T

Takahashi, H., 37
 Tamagawa, T., 508, 522, 554
 Taniyama, T., 497, 518, 521
 Tao, T., 238
 Tarrant, W., 380
 Tate, J., x, *x*, 218, 242, 306, 465, 479, 499, 506, 508, 522, 555, 597
 Tauber, A., 253
 Taylor, B., 21
 Taylor, R., viii, *viii*, 2, 242, 339, 424, 428, 490, 498
 Teichmüller, O., 152, 228
 Thaine, F., viii, *viii*, 3, 163, 553
 Thue, A., 414, 424, 437
 Tijdeman, R., 2, 414, 429, 437
 Tonelli, L., 34
 Tunnell, J., 3, 242, 395, 453
 Tzanakis, N., 462, 600, 608

V

Vélu, J., 474

de la Vallée Poussin, C.-J., 246

Vandiver, H., 438

Vatsal, V., 523

Vaughan, R., 200

Vinogradov, A. I., 198

Vinogradov, I. M., 4, 250

Volkenborn, A., 276, 277

Voronoi, G., 66, 182

Voutier, P., 413, 417

W

Waldschmidt, M., 411, 414

Waldspurger, J.-L., 195

Walsh, G., 439

Waring, E., 4, 376, 455

Warning, E., 72

Washington, L., x, *x*, 150, 301

Watkins, M., 139, 383, 384, 566,
598

Weber, H., 140, 145, 167

Wedderburn, J., 65

de Weger, B., 59, 387, 417, 420,
423, 600

Zorn, M., 262

Weierstrass, K., 270, 465, 482, 586

Weil, A., 3, 11, 90, 92, 100, 335,
445, 497, 497, 518, 521

Wendt, E., 430

Wetherell, J., 409, 455, 456, 460

Wieferich, A., 430, 435

Wiles, A., viii, *viii*, 2, 242, 245,
339, 424, 428, 489, 490, 498, 518,
521, 522

Wilson, J., 368, 405

Witt, E., 290, 293

Wolstenholme, J., 97, 383

Y

Yamamoto, Y., 139

Yarbrough, K., 380

Yazdani, S., 523

Z

Zagier, D., 8, 41, 122, 139, 195,
198, 239, 245, 246, 261, 270, 378,
463, 522, 571, 583, 590

General Index

Page numbers in Roman type refer to the current volume, while italicized page numbers refer to the complementary volume.

Symbols

290-theorem, *313*

A

abc conjecture, 482

Abel–Plana formula, 30

Abelian extension, 167

abelian group

– finite, *14*

– finitely generated, *11*

abscissa

– of absolute convergence, 160

– of convergence, 162, 259

absolute norm, *109*

absolute trace, *109*

absolute value, *183*

– Archimedean, *184*

– equivalent, *184*

– extension, *237*

– non-Archimedean, *184*

– normalization, *191*

– trivial, *184*

absolutely irreducible, *468*

additive character, *74*

additive number theory, *4*

additive reduction, *472*

affine curve, *90*

AGM, *483, 486*

algebraic geometry, *7*

algebraic integer, *126*

algebraic number theory, *6*

algebraic rank, *522*

Almkvist–Meurman theorem, 70,

133, 327

analytic p -adic function, *205*

analytic element, *189*

analytic number theory, 151

analytic rank, *522*

approximate functional equation,
176

approximation of linear forms, *60*

Archimedean absolute value, *184*

arithmetic

– convolution, 152

– function, 151

arithmetic geometry, *7*

arithmetic surface, *7*

arithmetic–geometric mean, *483, 486*

Artin’s conjecture, 167, 219

Artin–Hasse exponential, *217*

Artin–Schreier polynomial, *115*

Artin–Schreier subgroup, *70*

Artin–Schreier theory, *115*

asymptotic expansion, 19

Atkin–Lehner operator, *596*

automorphism

– Frobenius, *498*

B

baby-step giant-step algorithm, *357, 565*

bad reduction, 506
 basic CM elliptic curve, 571
 basis
 – orthogonal, 288
 Bernoulli
 – χ , 43
 – number, 3
 – polynomial, 3, 118
 Bernoulli–Euler triangle, 121
 Bernoulli–Hurwitz number, 264
 Bessel functions, 111
 beta function, 93
 birational transformation, 475
 Birch–Swinnerton-Dyer conjecture,
 vi, vi, 3, 245, 452, 522
 BSD conjecture, vi, vi, 245, 452,
 479, 522

C

cannonball problem, 424, 425
 canonical coordinates, 506
 canonical height, 530
 Carmichael number, 93
 Carmichael’s function, 93
 CAS: computer algebra system, v,
 v
 Cassels–Sansone number, 609
 Catalan’s constant, 127
 Catalan’s equation, 2, 428, 442
 Cauchy sequence, 192
 Cauchy’s formula, 188, 440
 Čebotarev density theorem, 325,
 514
 character
 – additive, 74
 – conductor of, 25
 – Dirichlet, 25
 – Dwork, 388
 – even, 171
 – group, 18
 – multiplicative, 74
 – odd, 171
 – orthogonality, 20, 29
 – primitive, 25
 – real primitive, 43
 – trivial, 18
 characteristic of a field, 65
 characteristic polynomial of an el-
 ement, 109
 Chevalley–Warning theorem, 72, 204
 χ -Bernoulli number, polynomial, 43
 Chowla–Selberg formula, 223
 circle method, 4
 circle problem, 182
 class group, 131, 338
 – T , 550
 class number, 131
 class number formula, 138
 Clay foundation, 3
 CM point, 586
 cocycle condition, 110
 compact representation, 357
 complementary law, 35
 complete field, 192
 completely multiplicative function,
 154
 completion, 194
 complex cubic field, 108
 complex multiplication, 265, 484,
 588
 complex multiplication field, 149
 conductor
 – of a character, 25
 – of an elliptic curve, 521
 congruent number, 3, 393, 450
 conjecture
 – Artin, 167
 – Birch–Swinnerton-Dyer (BSD),
 vi, vi, 3, 245, 452, 522
 – Catalan, 2
 – congruent number, 3
 – Fermat (FLT), 1
 – Mordell, 2, 498
 – Ramanujan, 496
 – Shafarevich, 498
 – Taniyama–Shimura–Weil, 2, 497,
 521
 – Waring, 4, 376

- Weil, 3
 - constant term
 - in Euler–MacLaurin, 26
 - content of a polynomial, 124
 - contiguity relation, 149
 - contiguous bases, 288
 - continued fraction method, 357
 - convex set, 63
 - convolution, 104
 - arithmetic, 152
 - coordinates
 - canonical, 506
 - covariant, 478
 - covolume of a lattice, 51
 - critical strip, 243
 - curve, 7
 - affine, 90
 - elliptic, 2, 452
 - hyperelliptic, 442
 - projective, 90
 - cuspidal, 469
 - cyclic cubic field, 109
 - cyclotomic field, 144
 - cyclotomic polynomial, 201
 - cyclotomic unit, 142
- D**
- decomposition group, 134
 - Dedekind domain, 131
 - Dedekind eta function, 215
 - Dedekind independence theorem, 117
 - Dedekind zeta function, v , v , 216
 - degree
 - of an isogeny, 474
 - degree of a divisor, 444
 - descent, 387, 391
 - infinite, 338, 373
 - second, 546
 - 2-descent
 - general, 548
 - with 2-torsion, 532
 - 3-descent
 - with rational 3-torsion, 557
 - dessin d’enfant, 478
 - determinant of a lattice, 51
 - diagonal form, 293
 - diagonal hypersurface, 177
 - diamond of x , 229
 - dilogarithm, 278, 404
 - dimension, 6
 - Diophantine m -tuple, 424
 - Diophantine equation, 1
 - Dirichlet character, 25
 - Dirichlet series, 160
 - formal, 151
 - Dirichlet’s class number formula, 138
 - Dirichlet’s theorem on primes, 27, 237
 - discrete logarithm, 93
 - discrete valuation ring, 196
 - discriminant
 - fundamental, 43
 - of a quadratic form, 286
 - of an elliptic curve, 466
 - prime, 48
 - relative, 130
 - distribution formula
 - for Γ_p , 372
 - for $\text{Log}\Gamma_p$, 331, 340
 - for $\text{Log}\Gamma_p(\chi)$, 338
 - for ψ_p , 331
 - for $\psi_p(\chi)$, 338
 - for ζ_p , 286, 292
 - for $\zeta_p(\chi)$, 295
 - for Bernoulli polynomials, 5
 - for complex gamma, 88
 - for fractional part, 171
 - for higher gamma, 135
 - for Hurwitz zeta, 77
 - for sum of digits, 171
 - division algebra, 65
 - divisor
 - degree, 444
 - effective, 444
 - group, 444
 - on a curve, 444

- rational, 445
- reduced, 446
- semireduced, 446
- suitable, 363
- divisor problem, 182
- dot product, 286
- double point, 469
- doubly exponential numerical integration, 37
- dual group, 18
- dual isogeny, 474
- duplication formula
 - for Γ_p , 372
 - for complex gamma, 88
 - for Hurwitz zeta, 77
- Dwork character, 388
- Dwork power series, 255

E

- E arises from f , 498
- effective divisor, 444
- egg, 485
- Egyptian number, 463
- Eisenstein
 - criterion, 201
 - polynomial, 201, 253
- Eisenstein series, 264
 - holomorphic, 159
 - nonholomorphic, 211
- Eisenstein's reciprocity law, 170, 434
- elementary divisor theorem, 12, 13
- elementary number theory, 151
- elliptic curve, 2, 452
 - basic CM, 571
 - rank, 452
 - supersingular, 498
- elliptic logarithm, 425, 483, 603
- Epstein zeta function, 210, 215
- equation
 - Catalan, 428
 - Diophantine, 1
 - Pell–Fermat, 354
 - Thue, 414, 437

- Weierstrass, 465
- equivalence
 - Kummer, 114
- equivalent absolute values, 184
- equivalent ideals, 131
- equivalent norms, 235
- equivalent quadratic forms, 291
- ERH, 238
- eta function
 - Dedekind, 215
- Euler number, 6, 267
- Euler polynomial, 121
- Euler product, 154
- Euler's totient function, 141
- Euler–MacLaurin summation formula, 19
- Eulerian number, 126
- Eulerian polynomial, 126
- even character, 171
- exact hexagon lemma, 244
- expansion
 - asymptotic, 19
- exponent of a group, 93
- exponential
 - \mathfrak{p} -adic, 211
 - Artin–Hasse, 217
 - formal, 504
- exponential generating function, 3, 8
- exponential integral, 574
- extended Riemann hypothesis, 238
- extension
 - Galois, 103
 - Kummer, 179
 - maximal unramified, 242
 - normal, 103
 - of \mathfrak{p} -adic fields, 235
 - of absolute values, 237
 - tamely ramified, 240
 - totally ramified, 240, 253
 - unramified, 240, 249
- extraneous zero, 177

F

- factor basis, 357

- Fermat prime, 512
 - Fermat triangle, 482, 514
 - Fermat's last theorem, 1, 427
 - Fibonacci number, 420
 - Fibonacci sequence, 421
 - field
 - characteristic, 65
 - complete, 192
 - completion, 194
 - complex cubic, 108
 - cyclic cubic, 109
 - cyclotomic, 144
 - finite, 7, 65
 - fixed, 104
 - global, 7
 - imaginary quadratic, 108
 - number, 106
 - p -adic, 7, 183
 - perfect, 101
 - place, 190
 - prime, 65
 - pure cubic, 108
 - quadratic, 136
 - real quadratic, 108
 - regular, 232
 - residue, 7, 189
 - skew, 65
 - totally real cubic, 108
 - filtration (p -adic), 509
 - finite abelian group structure, 14
 - finite field, 7, 65
 - finitely generated abelian group, 11
 - first case of FLT, 428
 - fixed field, 104
 - FLT, 1, 427, 503
 - FLT I, 428
 - FLT II, 435
 - formal Dirichlet series, 151
 - formal Euler product, 154
 - formal exponential, 504
 - formal group, 503
 - formal logarithm, 504
 - Fourier
 - coefficient, 45, 496
 - inversion formula, 105
 - series, 45
 - transform, 46, 104, 148
 - fractional part, 16
 - Frey curve, 503
 - Fricke involution, 587
 - Frobenius automorphism
 - elliptic curves, 498
 - finite fields, 69
 - unramified p -adic extension, 250
 - Frobenius homomorphism
 - elliptic curves, 495
 - number fields, 180
 - function
 - L , v , v
 - arithmetic, 151
 - Bessel, 111
 - beta, 93
 - Dedekind zeta, v , v
 - kernel, 104
 - Möbius, 153
 - multiplicative, 154
 - theta, 169
 - zeta, v , v
 - function tending rapidly to 0, 163
 - functional equation
 - approximate, 176
 - of L -function, 172
 - of theta function, 171
 - fundamental discriminant, 43
 - fundamental parallelogram, 483
 - fundamental parallelotope, 51
 - fundamental unit, 132, 338
- G**
- Galois extension, 103
 - Galois representation, 2
 - Galois theory, 101
 - gamma function
 - p -adic, 368
 - complex, 80
 - higher, 192

- real, 78
- Gauss sum, 31, 75
- Gauss’s lemma on contents, 124
- generating function
 - exponential, 3, 8
 - ordinary, 3, 8
- genus of a curve, 90
- geometry
 - algebraic, 7
 - arithmetic, 7
 - projective, 90
- global field, 7
- global solution, v , v
- Goldbach’s conjecture, 455
- good reduction, 506, 520
- Gram matrix, 51
- Gram–Schmidt basis, 52
- Gross–Koblitz formula, 151, 386
- Gross–Zagier theorem, 590
- group
 - class, 338
 - dual, 18
 - formal, 503
 - Picard, 445
 - Tate–Shafarevich, 306
 - unit, 338
- group character, 18
- group of units of a ring, 20

H

- Hadamard product, 85, 248
- Hadamard’s inequality, 52
- half-system, 39
- harmonic sum, 128, 142
- Hasse interval, 497
- Hasse norm principle, 318
- Hasse principle, 6, 326
- Hasse–Davenport relation
 - lifting, 174, 182
 - product, 82, 173, 394
- Hasse–Minkowski theorem, 305
- Hasse–Weil zeta function, 91, 497
- Hecke–Eisenstein series, 193
- Heegner point, 586

- Heegner point method, 528, 584
- height
 - canonical, 530
 - naïve, 530
- height pairing matrix, 531, 601
- Hellegouarch–Frey curve, 503
- Hensel lifting, v , v
- Hensel’s lemma, 199, 202
- Herbrand quotient, 245
- Hermite normal form, 16, 340
- Hermite’s inequality, 54
- higher gamma function, 192
- Hilbert modular form, 193
- Hilbert symbol, 295
- Hilbert’s tenth problem, vii, vii
- Hilbert’s Theorem 90, 118
- holomorphic Eisenstein series, 159
- Hurwitz zeta function, 71, 168, 190
- hyperbolic plane, 287
- hyperbolic quadratic form, 292
- hyperelliptic curve, 442, 514
- hypergeometric series, 149, 406

I

- ideal
 - primitive, 363
- ideal class group, 131
- imaginary quadratic field, 108
- incomplete gamma function, 172, 573
- inequality
 - Pólya–Vinogradov, 198
 - triangle, 183
 - ultrametric, 188
- inertia group, 134
- infinite descent, 373, 391
- infrastructure, 357
- integral quadratic form, 311
- invariant differential, 501
- inverse binomial symbol, 281
- inverse limit, 224
- inversion formula
 - Möbius, 153
- irreducible

- absolutely, 468
- irregular prime, 69, 432
- isogenous elliptic curves, 473
- isogeny, 473
 - degree, 474
 - dual, 474
- isogeny conjecture, 521
- isotropic
 - subspace, 287
 - vector, 287
- Iwasawa logarithm, 264

J

- Jacobi sum, 79
- Jacobi symbol, 36
- Jacobian, 408, 479
- Jacobian variety, 445
- Jacobstahl–Kazandzidis congruence, 381

K

- Kash, v , v , 338
- K -automorphism, 102
- K -embedding, 102
- kernel function, 104
- Klein form, 478
- Klein quartic curve, 489
- Kloosterman sum, 100
- Kodaira type, 597
- Krasner analytic function, 267, 269, 346
- Krasner’s lemma, 238
- Kronecker limit formula, 213
- Kronecker symbol, 36
- Kronecker’s Jugendtraum, 146
- Kronecker–Weber theorem, 140, 145, 167
- Kummer congruence, 67, 324
- Kummer equivalence, 114
- Kummer extension, 179
- Kummer theory, 436

L

- L -function, v , v

- functional equation, 172
- Λ -function, 242
- Langlands program, 167, 242
- Laplace
 - inversion formula, 109
 - transform, 28, 104, 108
- large sieve inequality, 139
- lattice, 51
 - covolume, 51
 - determinant, 51
 - fundamental parallelotope, 51
 - minimum, 54
- Legendre symbol, 33
- level of a p -adic point, 508
- level-lowering, 490, 498, 500
- Lichtenbaum’s conjecture, 244
- Lipschitz-continuous, 277
- LLL algorithm, 58
- LLL-reduced basis, 56
- local ring, 189
- local solution, v , v
- local to global principle, 326
- local-to-global principle, v , v
- log gamma function
 - complex $\text{Log}\Gamma$, 81
 - Diamond’s $\text{Log}\Gamma_p$, 330
 - Morita’s $\text{Log}\Gamma_p(\chi)$, 337
- logarithm
 - p -adic, 211
 - discrete, 93
 - elliptic, 425, 483, 603
 - formal, 504
- Lucas number, 420
- Lucas sequence, 421

M

- magma, v , v , 338, 495
- Mahler coefficient, 221
- Mahler’s theorem, 220
- von Mangoldt’s function, 159
- Manin constant, 586
- Mason’s theorem, 491
- matrix
 - Gram, 51

- orthogonal, 51
- matrix-integral quadratic form, 311
- maximal unramified extension, 242
- Mazur's theorem, 528
- Mellin
 - inversion formula, 107
 - transform, 104, 107
- Mersenne prime, 512
- Mertens's theorem, 268
- method
 - infinite descent, 338, 373, 391
 - stationary phase, 117
 - steepest descent, 117
- minimal model, 506, 519
- minimal polynomial, 106
- minimum of a lattice, 54
- Minkowski's convex body theorem, 63
- minus class number, 149
- Möbius
 - function, 141, 153, 156
 - inversion formula, 153
- model
 - minimal, 506, 519
- modular form, 2, 159, 172
 - Hilbert, 193
- modular parametrization, 586
- modularity theorem, 497
- Mordell's conjecture, 2, 92, 482, 498
- Mordell's theorem, 538, 554
- morphism (of quadratic modules), 286
- multiplication
 - complex, 484
- multiplicative character, 74
- multiplicative function, 154
- multiplicative quadratic form, 329
- multiplicative reduction, 472
- Mumford's representation, 446
- mwr*ank, 479

N

Nagell–Lutz theorem, 524

naïve height, 530

Nakayama's lemma, 231

newform, 496

- rational, 497

Noether's theorem, 110

non-Archimedean absolute value, 184

nondegenerate

- quadratic form, 287
- quadratic module, 287

nonholomorphic Eisenstein series, 211

nonsingular

- equation, 203
- solution, 73, 203

nonsplit multiplicative reduction, 472

nontrivial zero, 177

norm

- absolute, 109
- equivalent, 235
- relative, 109

norm on a vector space, 235

normal basis theorem, 120, 251

normal extension, 103

normal form

- Hermite, 16, 340
- Smith, 15

normalization of absolute values, 191

number

- Bernoulli, 3
- congruent, 393, 450
- Egyptian, 463
- Euler, 6, 267
- Eulerian, 126
- Fermat, 512
- Fibonacci, 420, 424
- Lucas, 420, 424
- Mersenne, 512
- Stirling, 125, 222, 268
- tangent, 6

number field, 106

number theory

- additive, 4
- algebraic, 6
- analytic, 151
- elementary, 151

O

- obstruction, 306
- odd character, 171
- order of a point on a curve, 443
- orthogonal
 - basis, 288
 - direct sum, 286
 - elements, 286
 - of a subset, 286
- orthogonal matrix, 51
- orthogonality of characters, 20, 29
- Ostrowski's theorem, 190

P

- \mathfrak{p} -adic exponential, 211
- \mathfrak{p} -adic field, v, v, 7, 183
- p -adic gamma function, 368
- \mathfrak{p} -adic integer, 196
- \mathfrak{p} -adic logarithm, 211
- p -adic number, v, v
- p -adic regulator, 458
- p -adic root, 202
- \mathfrak{p} -adic unit, 226
- pairing (perfect), 112
- Pari/GP, v, v, 338, 495
- Pascal's triangle, 118
- Pell–Fermat equation, 354
 - Kronecker's solution, 229
- perfect field, 101
- perfect pairing, 112
- Picard group, 445
- place of a number field, 190
- PNT, 245
- point
 - rational, 465
- point on a curve, 90
- Poisson summation formula, 45
- Pólya–Vinogradov inequality, 198
- polylogarithm, 192, 278

- polynomial
 - Artin–Schreier, 115
 - Bernoulli, 3, 118
 - characteristic, 109
 - cyclotomic, 201
 - Eisenstein, 201, 253
 - separable, 101
- power basis, 107
- p th power-free, 360
- preparation theorem, 270
- primary algebraic number, 169
- prime fundamental discriminant, 48
- prime number theorem, 245
- prime subfield, 65
- primes in arithmetic progression, 237
- primitive character, 25
- primitive element theorem, 106
- primitive ideal, 363
- primitive root, 23
- principal ideal problem, 338
- principle
 - local-to-global, v, v
- product
 - dot, 286
- product formula, 191
- profinite completion, 70
- profinite group, 70
- projective curve, 90
- projective geometry, 90
- projective limit, 224
- projective point, 90
- pure cubic field, 108
- Pythagorean triangle, 3, 451, 482
- Pythagorean triple, 352

Q

- quadratic field, 108, 136
- quadratic form, 286, 305
 - integral, 311
 - matrix-integral, 311
 - multiplicative, 329
 - universal, 312
- quadratic module, 286

quadratic reciprocity law, 35
 quadratic twist, 489, 499, 589
 quotient
 – Herbrand, 245

R

Raabe's formula
 – for $\text{Log}\Gamma_p$, 335
 – for $\text{Log}\Gamma_p(\chi)$, 344
 – for ζ_p , 287
 – for $\zeta_p(\chi)$, 297
 – for complex gamma, 103
 radical
 – of a polynomial, 491
 – of an integer, 483
 radical (of a quadratic module), 286
 radius of convergence, 206
 Ramanujan τ function, 159, 259
 Ramanujan sum, 153
 Ramanujan's conjecture, 160, 241, 496
 ramification index, 132
 rank
 – algebraic, 452, 522
 – analytic, 522
 rational cuboid problem, 456
 rational divisor, 445
 rational newform, 497
 rational point, 465
 rational subgroup, 557
 real primitive character, 43
 real quadratic field, 108
 reciprocity law, 35
 – Shimura, 589
 reduced divisor, 446
 reduction
 – additive, 472
 – bad, 506
 – good, 506, 520
 – nonsplit multiplicative, 472
 – split multiplicative, 472
 reflection formula
 – for Γ_p , 371

– for $\text{Log}\Gamma_p$, 331
 – for $\text{Log}\Gamma_p(\chi)$, 338
 – for ψ_p , 331
 – for $\psi_p(\chi)$, 338
 – for ζ_p , 286
 – for $\zeta_p(\chi)$, 295
 – for complex gamma, 89
 regular \mathfrak{p} -adic field, 232
 regular prime, 69, 432
 regulator
 – p -adic, 458
 – of a real quadratic field, 138
 – of an elliptic curve, 601
 relative
 – discriminant, 130
 – norm, 109
 – trace, 109
 representation
 – Galois, 2
 residual degree, 132
 residue field, 7, 189
 resultant of two polynomials, 143, 180
 RH, 162
 Ribet's level-lowering, 500
 Riccati differential equation, 611
 Riemann hypothesis, 159, 162
 – extended, 238
 – for curves, 91
 Riemann zeta
 – function, 153
 – series, 153
 Riemann–Lebesgue lemma, 106
 root
 – primitive, 23
 root number, 49, 521

S

SEA algorithm, 565
 second case of FLT, 435
 second descent, 546
 Selberg zeta function, 243
 Selmer group
 – T , 551

- of an elliptic curve, 555
 - semireduced divisor, 446
 - separable polynomial, 101
 - series
 - Eisenstein, 264
 - Shafarevich conjecture, 498
 - Shimura’s reciprocity law, 589
 - Siegel zero, 239
 - sign of quadratic Gauss sums, 45
 - signature of a number field, 107
 - singular modulus, 571
 - singular series, 4
 - skew field, 65
 - Skolem’s equation, 385
 - Smith normal form, 15
 - SMK equation, 511
 - solution
 - global, v , v
 - local, v , v
 - Sondow’s formula, 140
 - special value, 243
 - special values of L -function, 186
 - split (totally), 135
 - split multiplicative reduction, 472
 - square pyramid problem, 424
 - squarefree integer, 156
 - squarefree part, 541
 - Stark’s conjectures, 193
 - stationary phase, 117
 - steepest descent, 117
 - Stickelberger ideal, 160
 - Stickelberger’s congruence, 155, 390
 - Stickelberger’s ideal theorem, 162
 - Stickelberger’s theorem, 390, 391
 - Stirling number
 - first kind, 222, 268
 - second kind, 125
 - Stirling transform, 282
 - Stirling’s formula, 34, 82
 - complex, 85
 - Strassmann’s theorem, 266, 387
 - strictly differentiable, 277
 - structure
 - class group, 131
 - unit group, 131
 - structure of finite abelian groups, 14
 - Sturm’s algorithm, 107
 - suitable divisor, 363
 - sum
 - Gauss, 31
 - Jacobi, 79
 - Ramanujan, 153
 - summation formula
 - Euler–MacLaurin, 19
 - generalized Poisson, 178
 - Poisson, 45
 - supersingular elliptic curve, 498, 512
 - surface, 7
 - algebraic, 7
 - arithmetic, 7
 - symbol
 - Hilbert, 295
 - symmetric set, 63
 - system of fundamental units, 338
- T**
- Tamagawa number, 508, 554
 - tamely ramified extension, 240
 - tangent number, 6
 - tanh-sinh numerical integration, 37
 - Taniyama–Shimura–Weil conjecture, 2, 497, 521
 - Tate’s algorithm, 499
 - Tate–Shafarevich group, 306, 479, 555
 - Tauberian theorem, 253
 - T -class group, 550
 - Teichmüller character, 152, 228
 - Teichmüller representative, 249
 - theta function, 169, 170
 - functional equation, 171
 - Thue equation, 414, 424, 437
 - totally discontinuous, 197
 - totally ramified extension, 240, 253
 - totally real cubic field, 108
 - totally split, 135

totient function, 141
 trace
 – absolute, 109
 – relative, 109
 transform
 – Fourier, 104
 – Laplace, 104, 108
 – Mellin, 104, 107
 triangle
 – Fermat, 482, 514
 – Pythagorean, 3, 451
 triangle inequality, 183
 triangular number, 331
 trigonometric sum, 4
 trivial character, 18
 trivial zero, 177
 T -Selmer group, 551
 T -unit group, 550
 Tunnell's theorem, 453
 T -virtual square, 551
 twin prime conjecture, 455
 twisted projective equivalence, 392

U

ultrametric inequality, 188
 unimodular matrix, 15
 unit, 126
 – cyclotomic, 142
 – fundamental, 132
 – p -adic, 226
 unit group, 131, 338
 – T , 550
 unit group of a ring, 20
 unit group structure, 131
 unit in \mathbb{Z}_K , 131
 universal quadratic form, 312
 unramified extension, 240, 249

V

Vandiver's conjecture, 438
 virtual square

– T , 551

Volkenborn integral, 277

W

Waring's problem, 4, 376, 455
 Wedderburn's theorem, 65
 Weierstrass \wp -function, 482
 Weierstrass equation, 465
 Weierstrass's preparation theorem, 270
 Weil conjectures, 3, 92, 335
 Weil representation, 148
 Weil's bounds, 90, 335
 Weil's conjectures, 178
 Wieferich's criterion, 435
 Wiles's theorem, 521
 Wilson prime, 405
 Wilson's theorem, 368
 Witt's theorem, 290, 293
 Wolstenholme prime, 383, 407
 Wolstenholme's congruence, 97, 406

Z

zero
 – extraneous, 177
 – nontrivial, 177
 – Siegel, 239
 – trivial, 177
 zeta function, v , v
 – Dedekind, 216
 – diagonal hypersurface, 177
 – Epstein, 210, 215
 – Hasse–Weil, 91, 497
 – Hurwitz, 71, 168, 190
 – Hurwitz p -adic, 283
 – χ -Hurwitz p -adic, 291
 – Kubota–Leopoldt p -adic, 301
 – of a curve, 91
 – Riemann, 153
 – Selberg, 243
 Zorn's lemma, 262

Graduate Texts in Mathematics

(continued from page ii)

- 64 EDWARDS. Fourier Series. Vol. I. 2nd ed.
65 WELLS. Differential Analysis on Complex Manifolds. 2nd ed.
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. 2nd ed.
72 STILLWELL. Classical Topology and Combinatorial Group Theory. 2nd ed.
73 HUNGERFORD. Algebra.
74 DAVENPORT. Multiplicative Number Theory. 3rd ed.
75 HOCHSCHILD. Basic Theory of Algebraic Groups and Lie Algebras.
76 ITAKA. 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. 2nd ed.
81 FORSTER. Lectures on Riemann Surfaces.
82 BOTT/TU. Differential Forms in Algebraic Topology.
83 WASHINGTON. Introduction to Cyclotomic Fields. 2nd ed.
84 IRELAND/ROSEN. A Classical Introduction to Modern Number Theory. 2nd ed.
85 EDWARDS. Fourier Series. Vol. II. 2nd ed.
86 VAN LINT. Introduction to Coding Theory. 2nd ed.
87 BROWN. Cohomology of Groups.
88 PIERCE. Associative Algebras.
89 LANG. Introduction to Algebraic and Abelian Functions. 2nd ed.
90 BRØNDSTED. An Introduction to Convex Polytopes.
91 BEARDON. On the Geometry of Discrete Groups.
92 DIESTEL. Sequences and Series in Banach Spaces.
93 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part I. 2nd ed.
94 WARNER. Foundations of Differentiable Manifolds and Lie Groups.
95 SHIRYAEV. Probability. 2nd ed.
96 CONWAY. A Course in Functional Analysis. 2nd ed.
97 KOBLITZ. Introduction to Elliptic Curves and Modular Forms. 2nd ed.
98 BRÖCKER/TOM DIECK. Representations of Compact Lie Groups.
99 GROVE/BENSON. Finite Reflection Groups. 2nd ed.
100 BERG/CHRISTENSEN/RESSEL. Harmonic Analysis on Semigroups: Theory of Positive Definite and Related Functions.
101 EDWARDS. Galois Theory.
102 VARADARAJAN. Lie Groups, Lie Algebras and Their Representations.
103 LANG. Complex Analysis. 3rd ed.
104 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part II.
105 LANG. $SL_2(\mathbf{R})$.
106 SILVERMAN. The Arithmetic of Elliptic Curves.
107 OLVER. Applications of Lie Groups to Differential Equations. 2nd ed.
108 RANGE. Holomorphic Functions and Integral Representations in Several Complex Variables.
109 LEHTO. Univalent Functions and Teichmüller Spaces.
110 LANG. Algebraic Number Theory.
111 HUSEMÖLLER. Elliptic Curves. 2nd ed.
112 LANG. Elliptic Functions.
113 KARATZAS/SHREVE. Brownian Motion and Stochastic Calculus. 2nd ed.
114 KOBLITZ. A Course in Number Theory and Cryptography. 2nd ed.
115 BERGER/GOSTIAUX. Differential Geometry: Manifolds, Curves, and Surfaces.
116 KELLEY/SRINIVASAN. Measure and Integral. Vol. I.
117 J.-P. SERRE. Algebraic Groups and Class Fields.
118 PEDERSEN. Analysis Now.
119 ROTMAN. An Introduction to Algebraic Topology.
120 ZIEMER. Weakly Differentiable Functions: Sobolev Spaces and Functions of Bounded Variation.

- 121 LANG. Cyclotomic Fields I and II. Combined 2nd ed.
- 122 REMMERT. Theory of Complex Functions. *Readings in Mathematics*
- 123 EBBINGHAUS/HERMES et al. Numbers. *Readings in Mathematics*
- 124 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications Part III.
- 125 BERENSTEIN/GAY. Complex Variables: An Introduction.
- 126 BOREL. Linear Algebraic Groups. 2nd ed.
- 127 MASSEY. A Basic Course in Algebraic Topology.
- 128 RAUCH. Partial Differential Equations.
- 129 FULTON/HARRIS. Representation Theory: A First Course. *Readings in Mathematics*
- 130 DODSON/POSTON. Tensor Geometry.
- 131 LAM. A First Course in Noncommutative Rings. 2nd ed.
- 132 BEARDON. Iteration of Rational Functions.
- 133 HARRIS. Algebraic Geometry: A First Course.
- 134 ROMAN. Coding and Information Theory.
- 135 ROMAN. Advanced Linear Algebra. 2nd ed.
- 136 ADKINS/WEINTRAUB. Algebra: An Approach via Module Theory.
- 137 AXLER/BOURDON/RAMEY. Harmonic Function Theory. 2nd ed.
- 138 COHEN. A Course in Computational Algebraic Number Theory.
- 139 BREDON. Topology and Geometry.
- 140 AUBIN. Optima and Equilibria. An Introduction to Nonlinear Analysis.
- 141 BECKER/WEISPFENNING/KREDEL. Gröbner Bases. A Computational Approach to Commutative Algebra.
- 142 LANG. Real and Functional Analysis. 3rd ed.
- 143 DOOB. Measure Theory.
- 144 DENNIS/FARB. Noncommutative Algebra.
- 145 VICK. Homology Theory. An Introduction to Algebraic Topology. 2nd ed.
- 146 BRIDGES. Computability: A Mathematical Sketchbook.
- 147 ROSENBERG. Algebraic K -Theory and Its Applications.
- 148 ROTMAN. An Introduction to the Theory of Groups. 4th ed.
- 149 RATCLIFFE. Foundations of Hyperbolic Manifolds.
- 150 EISENBUD. Commutative Algebra with a View Toward Algebraic Geometry.
- 151 SILVERMAN. Advanced Topics in the Arithmetic of Elliptic Curves.
- 152 ZIEGLER. Lectures on Polytopes.
- 153 FULTON. Algebraic Topology: A First Course.
- 154 BROWN/PEARCY. An Introduction to Analysis.
- 155 KASSEL. Quantum Groups.
- 156 KECHRIS. Classical Descriptive Set Theory.
- 157 MALLIAVIN. Integration and Probability.
- 158 ROMAN. Field Theory.
- 159 CONWAY. Functions of One Complex Variable II.
- 160 LANG. Differential and Riemannian Manifolds.
- 161 BORWEIN/ERDÉLYI. Polynomials and Polynomial Inequalities.
- 162 ALPERIN/BELL. Groups and Representations.
- 163 DIXON/MORTIMER. Permutation Groups.
- 164 NATHANSON. Additive Number Theory: The Classical Bases.
- 165 NATHANSON. Additive Number Theory: Inverse Problems and the Geometry of Sumsets.
- 166 SHARPE. Differential Geometry: Cartan's Generalization of Klein's Erlangen Program.
- 167 MORANDI. Field and Galois Theory.
- 168 EWALD. Combinatorial Convexity and Algebraic Geometry.
- 169 BHATIA. Matrix Analysis.
- 170 BREDON. Sheaf Theory. 2nd ed.
- 171 PETERSEN. Riemannian Geometry. 2nd ed.
- 172 REMMERT. Classical Topics in Complex Function Theory.
- 173 DIESTEL. Graph Theory. 2nd ed.
- 174 BRIDGES. Foundations of Real and Abstract Analysis.
- 175 LICKORISH. An Introduction to Knot Theory.
- 176 LEE. Riemannian Manifolds.
- 177 NEWMAN. Analytic Number Theory.
- 178 CLARKE/LEDYAEV/ STERN/WOLENSKI. Nonsmooth Analysis and Control Theory.
- 179 DOUGLAS. Banach Algebra Techniques in Operator Theory. 2nd ed.
- 180 SRIVASTAVA. A Course on Borel Sets.

- 181 KRESS. Numerical Analysis.
- 182 WALTER. Ordinary Differential Equations.
- 183 MEGGINSON. An Introduction to Banach Space Theory.
- 184 BOLLOBAS. Modern Graph Theory.
- 185 COX/LITTLE/O'SHEA. Using Algebraic Geometry. 2nd ed.
- 186 RAMAKRISHNAN/VALENZA. Fourier Analysis on Number Fields.
- 187 HARRIS/MORRISON. Moduli of Curves.
- 188 GOLDBLATT. Lectures on the Hyperreals: An Introduction to Nonstandard Analysis.
- 189 LAM. Lectures on Modules and Rings.
- 190 ESMONDE/MURTY. Problems in Algebraic Number Theory. 2nd ed.
- 191 LANG. Fundamentals of Differential Geometry.
- 192 HIRSCH/LACOMBE. Elements of Functional Analysis.
- 193 COHEN. Advanced Topics in Computational Number Theory.
- 194 ENGEL/NAGEL. One-Parameter Semigroups for Linear Evolution Equations.
- 195 NATHANSON. Elementary Methods in Number Theory.
- 196 OSBORNE. Basic Homological Algebra.
- 197 EISENBUD/HARRIS. The Geometry of Schemes.
- 198 ROBERT. A Course in p -adic Analysis.
- 199 HEDENMALM/KORENBLUM/ZHU. Theory of Bergman Spaces.
- 200 BAO/CHEHN/SHEN. An Introduction to Riemann–Finsler Geometry.
- 201 HINDRY/SILVERMAN. Diophantine Geometry: An Introduction.
- 202 LEE. Introduction to Topological Manifolds.
- 203 SAGAN. The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions.
- 204 ESCOFIER. Galois Theory.
- 205 FÉLIX/HALPERIN/THOMAS. Rational Homotopy Theory. 2nd ed.
- 206 MURTY. Problems in Analytic Number Theory.
Readings in Mathematics
- 207 GODSIL/ROYLE. Algebraic Graph Theory.
- 208 CHENEY. Analysis for Applied Mathematics.
- 209 ARVESON. A Short Course on Spectral Theory.
- 210 ROSEN. Number Theory in Function Fields.
- 211 LANG. Algebra. Revised 3rd ed.
- 212 MATOUŠEK. Lectures on Discrete Geometry.
- 213 FRITZSCHE/GRAUERT. From Holomorphic Functions to Complex Manifolds.
- 214 JOST. Partial Differential Equations.
- 215 GOLDSCHMIDT. Algebraic Functions and Projective Curves.
- 216 D. SERRE. Matrices: Theory and Applications.
- 217 MARKER. Model Theory: An Introduction.
- 218 LEE. Introduction to Smooth Manifolds.
- 219 MACLACHLAN/REID. The Arithmetic of Hyperbolic 3-Manifolds.
- 220 NESTRUEV. Smooth Manifolds and Observables.
- 221 GRÜNBAUM. Convex Polytopes. 2nd ed.
- 222 HALL. Lie Groups, Lie Algebras, and Representations: An Elementary Introduction.
- 223 VRETBLAD. Fourier Analysis and Its Applications.
- 224 WALSHAP. Metric Structures in Differential Geometry.
- 225 BUMP. Lie Groups.
- 226 ZHU. Spaces of Holomorphic Functions in the Unit Ball.
- 227 MILLER/STURMFELS. Combinatorial Commutative Algebra.
- 228 DIAMOND/SHURMAN. A First Course in Modular Forms.
- 229 EISENBUD. The Geometry of Syzygies.
- 230 STROOCK. An Introduction to Markov Processes.
- 231 BJÖRNER/BRENTI. Combinatorics of Coxeter Groups.
- 232 EVEREST/WARD. An Introduction to Number Theory.
- 233 ALBIAC/KALTON. Topics in Banach Space Theory.
- 234 JORGENSON. Analysis and Probability.
- 235 SEPANSKI. Compact Lie Groups.
- 236 GARNETT. Bounded Analytic Functions.
- 237 MARTÍNEZ-AVENDAÑO/ROSENTHAL. An Introduction to Operators on the Hardy-Hilbert Space.

Graduate Texts in Mathematics

(continued from page ii)

- 64 EDWARDS. Fourier Series. Vol. I. 2nd ed.
65 WELLS. Differential Analysis on Complex Manifolds. 2nd ed.
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. 2nd ed.
72 STILLWELL. Classical Topology and Combinatorial Group Theory. 2nd ed.
73 HUNGERFORD. Algebra.
74 DAVENPORT. Multiplicative Number Theory. 3rd ed.
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. 2nd ed.
81 FORSTER. Lectures on Riemann Surfaces.
82 BOTT/TU. Differential Forms in Algebraic Topology.
83 WASHINGTON. Introduction to Cyclotomic Fields. 2nd ed.
84 IRELAND/ROSEN. A Classical Introduction to Modern Number Theory. 2nd ed.
85 EDWARDS. Fourier Series. Vol. II. 2nd ed.
86 VAN LINT. Introduction to Coding Theory. 2nd ed.
87 BROWN. Cohomology of Groups.
88 PIERCE. Associative Algebras.
89 LANG. Introduction to Algebraic and Abelian Functions. 2nd ed.
90 BRØNDSTED. An Introduction to Convex Polytopes.
91 BEARDON. On the Geometry of Discrete Groups.
92 DIESTEL. Sequences and Series in Banach Spaces.
93 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part I. 2nd ed.
94 WARNER. Foundations of Differentiable Manifolds and Lie Groups.
95 SHIRYAEV. Probability. 2nd ed.
96 CONWAY. A Course in Functional Analysis. 2nd ed.
97 KOBLITZ. Introduction to Elliptic Curves and Modular Forms. 2nd ed.
98 BRÖCKER/TOM DIECK. Representations of Compact Lie Groups.
99 GROVE/BENSON. Finite Reflection Groups. 2nd ed.
100 BERG/CHRISTENSEN/RESSEL. Harmonic Analysis on Semigroups: Theory of Positive Definite and Related Functions.
101 EDWARDS. Galois Theory.
102 VARADARAJAN. Lie Groups, Lie Algebras and Their Representations.
103 LANG. Complex Analysis. 3rd ed.
104 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part II.
105 LANG. $SL_2(\mathbf{R})$.
106 SILVERMAN. The Arithmetic of Elliptic Curves.
107 OLVER. Applications of Lie Groups to Differential Equations. 2nd ed.
108 RANGE. Holomorphic Functions and Integral Representations in Several Complex Variables.
109 LEHTO. Univalent Functions and Teichmüller Spaces.
110 LANG. Algebraic Number Theory.
111 HUSEMÖLLER. Elliptic Curves. 2nd ed.
112 LANG. Elliptic Functions.
113 KARATZAS/SHREVE. Brownian Motion and Stochastic Calculus. 2nd ed.
114 KOBLITZ. A Course in Number Theory and Cryptography. 2nd ed.
115 BERGER/GOSTIAUX. Differential Geometry: Manifolds, Curves, and Surfaces.
116 KELLEY/SRINIVASAN. Measure and Integral. Vol. I.
117 J.-P. SERRE. Algebraic Groups and Class Fields.
118 PEDERSEN. Analysis Now.
119 ROTMAN. An Introduction to Algebraic Topology.
120 ZIEMER. Weakly Differentiable Functions: Sobolev Spaces and Functions of Bounded Variation.

- 121 LANG. Cyclotomic Fields I and II. Combined 2nd ed.
- 122 REMMERT. Theory of Complex Functions. *Readings in Mathematics*
- 123 EBBINGHAUS/HERMES et al. Numbers. *Readings in Mathematics*
- 124 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications Part III.
- 125 BERENSTEIN/GAY. Complex Variables: An Introduction.
- 126 BOREL. Linear Algebraic Groups. 2nd ed.
- 127 MASSEY. A Basic Course in Algebraic Topology.
- 128 RAUCH. Partial Differential Equations.
- 129 FULTON/HARRIS. Representation Theory: A First Course. *Readings in Mathematics*
- 130 DODSON/POSTON. Tensor Geometry.
- 131 LAM. A First Course in Noncommutative Rings. 2nd ed.
- 132 BEARDON. Iteration of Rational Functions.
- 133 HARRIS. Algebraic Geometry: A First Course.
- 134 ROMAN. Coding and Information Theory.
- 135 ROMAN. Advanced Linear Algebra. 2nd ed.
- 136 ADKINS/WEINTRAUB. Algebra: An Approach via Module Theory.
- 137 AXLER/BOURDON/RAMEY. Harmonic Function Theory. 2nd ed.
- 138 COHEN. A Course in Computational Algebraic Number Theory.
- 139 BREDON. Topology and Geometry.
- 140 AUBIN. Optima and Equilibria. An Introduction to Nonlinear Analysis.
- 141 BECKER/WEISPFENNING/KREDEL. Gröbner Bases. A Computational Approach to Commutative Algebra.
- 142 LANG. Real and Functional Analysis. 3rd ed.
- 143 DOOB. Measure Theory.
- 144 DENNIS/FARB. Noncommutative Algebra.
- 145 VICK. Homology Theory. An Introduction to Algebraic Topology. 2nd ed.
- 146 BRIDGES. Computability: A Mathematical Sketchbook.
- 147 ROSENBERG. Algebraic K -Theory and Its Applications.
- 148 ROTMAN. An Introduction to the Theory of Groups. 4th ed.
- 149 RATCLIFFE. Foundations of Hyperbolic Manifolds. 2nd ed.
- 150 EISENBUD. Commutative Algebra with a View Toward Algebraic Geometry.
- 151 SILVERMAN. Advanced Topics in the Arithmetic of Elliptic Curves.
- 152 ZIEGLER. Lectures on Polytopes.
- 153 FULTON. Algebraic Topology: A First Course.
- 154 BROWN/PEARCY. An Introduction to Analysis.
- 155 KASSEL. Quantum Groups.
- 156 KECHRIS. Classical Descriptive Set Theory.
- 157 MALLIAVIN. Integration and Probability.
- 158 ROMAN. Field Theory.
- 159 CONWAY. Functions of One Complex Variable II.
- 160 LANG. Differential and Riemannian Manifolds.
- 161 BORWEIN/ERDÉLYI. Polynomials and Polynomial Inequalities.
- 162 ALPERIN/BELL. Groups and Representations.
- 163 DIXON/MORTIMER. Permutation Groups.
- 164 NATHANSON. Additive Number Theory: The Classical Bases.
- 165 NATHANSON. Additive Number Theory: Inverse Problems and the Geometry of Sumsets.
- 166 SHARPE. Differential Geometry: Cartan's Generalization of Klein's Erlangen Program.
- 167 MORANDI. Field and Galois Theory.
- 168 EWALD. Combinatorial Convexity and Algebraic Geometry.
- 169 BHATIA. Matrix Analysis.
- 170 BREDON. Sheaf Theory. 2nd ed.
- 171 PETERSEN. Riemannian Geometry. 2nd ed.
- 172 REMMERT. Classical Topics in Complex Function Theory.
- 173 DIESTEL. Graph Theory. 2nd ed.
- 174 BRIDGES. Foundations of Real and Abstract Analysis.
- 175 LICKORISH. An Introduction to Knot Theory.
- 176 LEE. Riemannian Manifolds.
- 177 NEWMAN. Analytic Number Theory.
- 178 CLARKE/LEDYAEV/ STERN/WOLENSKI. Nonsmooth Analysis and Control Theory.
- 179 DOUGLAS. Banach Algebra Techniques in Operator Theory. 2nd ed.
- 180 SRIVASTAVA. A Course on Borel Sets.
- 181 KRESS. Numerical Analysis.

- 182 WALTER. Ordinary Differential Equations.
- 183 MEGGINSON. An Introduction to Banach Space Theory.
- 184 BOLLOBAS. Modern Graph Theory.
- 185 COX/LITTLE/O'SHEA. Using Algebraic Geometry. 2nd ed.
- 186 RAMAKRISHNAN/VALENZA. Fourier Analysis on Number Fields.
- 187 HARRIS/MORRISON. Moduli of Curves.
- 188 GOLDBLATT. Lectures on the Hyperreals: An Introduction to Nonstandard Analysis.
- 189 LAM. Lectures on Modules and Rings.
- 190 ESMONDE/MURTY. Problems in Algebraic Number Theory. 2nd ed.
- 191 LANG. Fundamentals of Differential Geometry.
- 192 HIRSCH/LACOMBE. Elements of Functional Analysis.
- 193 COHEN. Advanced Topics in Computational Number Theory.
- 194 ENGEL/NAGEL. One-Parameter Semigroups for Linear Evolution Equations.
- 195 NATHANSON. Elementary Methods in Number Theory.
- 196 OSBORNE. Basic Homological Algebra.
- 197 EISENBUD/HARRIS. The Geometry of Schemes.
- 198 ROBERT. A Course in p -adic Analysis.
- 199 HEDENMALM/KORENBLUM/ZHU. Theory of Bergman Spaces.
- 200 BAO/CHERN/SHEN. An Introduction to Riemann–Finsler Geometry.
- 201 HINDRY/SILVERMAN. Diophantine Geometry: An Introduction.
- 202 LEE. Introduction to Topological Manifolds.
- 203 SAGAN. The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions.
- 204 ESCOFIER. Galois Theory.
- 205 FÉLIX/HALPERIN/THOMAS. Rational Homotopy Theory. 2nd ed.
- 206 MURTY. Problems in Analytic Number Theory.
Readings in Mathematics
- 207 GODSIL/ROYLE. Algebraic Graph Theory.
- 208 CHENEY. Analysis for Applied Mathematics.
- 209 ARVESON. A Short Course on Spectral Theory.
- 210 ROSEN. Number Theory in Function Fields.
- 211 LANG. Algebra. Revised 3rd ed.
- 212 MATOUŠEK. Lectures on Discrete Geometry.
- 213 FRITZSCHE/GRAUERT. From Holomorphic Functions to Complex Manifolds.
- 214 JOST. Partial Differential Equations. 2nd ed.
- 215 GOLDSCHMIDT. Algebraic Functions and Projective Curves.
- 216 D. SERRE. Matrices: Theory and Applications.
- 217 MARKER. Model Theory: An Introduction.
- 218 LEE. Introduction to Smooth Manifolds.
- 219 MACLACHLAN/REID. The Arithmetic of Hyperbolic 3-Manifolds.
- 220 NESTRUEV. Smooth Manifolds and Observables.
- 221 GRÜNBAUM. Convex Polytopes. 2nd ed.
- 222 HALL. Lie Groups, Lie Algebras, and Representations: An Elementary Introduction.
- 223 VRETBLAD. Fourier Analysis and Its Applications.
- 224 WALSHAP. Metric Structures in Differential Geometry.
- 225 BUMP. Lie Groups.
- 226 ZHU. Spaces of Holomorphic Functions in the Unit Ball.
- 227 MILLER/STURMFELS. Combinatorial Commutative Algebra.
- 228 DIAMOND/SHURMAN. A First Course in Modular Forms.
- 229 EISENBUD. The Geometry of Syzygies.
- 230 STROOCK. An Introduction to Markov Processes.
- 231 BJÖRNER/BRENTI. Combinatorics of Coxeter Groups.
- 232 EVEREST/WARD. An Introduction to Number Theory.
- 233 ALBIAC/KALTON. Topics in Banach Space Theory.
- 234 JORGENSON. Analysis and Probability.
- 235 SEPANSKI. Compact Lie Groups.
- 236 GARNETT. Bounded Analytic Functions.
- 237 MARTÍNEZ-AVENDAÑO/ROSENTHAL. An Introduction to Operators on the Hardy-Hilbert Space.
- 238 AIGNER, A Course in Enumeration.
- 239 COHEN, Number Theory, Vol. I.
- 240 COHEN, Number Theory, Vol. II.