
References

- [1] MFIPS 186-2. *Digital signature standard*. Federal Information Processing Standards Publication 186. U. S. Dept. of Commerce/National Institute of Standards and Technology, 2000.
- [2] M. Abdalla, M. Bellare, and P. Rogaway. The Oracle Diffie-Hellman assumption and an analysis of DHIES. *Topics in cryptology - CT RSA 01*. volume 2020 of *Lecture Notes in Computer Science*, Springer, Berlin, 2001, pages 143–158.
- [3] L. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over $\text{GF}(q)$. *Theoret. Comput. Sci.*, 226(1-2): 7–18, 1999.
- [4] L. V. Ahlfors. *Complex analysis*. McGraw-Hill Book Co., New York, third edition, 1978. An introduction to the theory of analytic functions of one complex variable, International Series in Pure and Applied Mathematics.
- [5] W. S. Anglin. The square pyramid puzzle. *Amer. Math. Monthly*, 97(2): 120–124, 1990.
- [6] M. F. Atiyah and C. T. C. Wall. Cohomology of groups. In *Algebraic number theory (Proc. Instructional Conf., Brighton, 1965)*, pages 94–115. Thompson, Washington, D.C., 1967.
- [7] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.
- [8] A. O. L. Atkin and F. Morain. Finding suitable curves for the elliptic curve method of factorization. *Math. Comp.*, 60(201):399–405, 1993.
- [9] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *J. Cryptology*, 11(2):141–145, 1998.
- [10] J. Belding. A Weil pairing on the p -torsion of ordinary elliptic curves over $K[\epsilon]$. *J. Number Theory* (to appear).
- [11] D. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. *Asiacrypt 2007* (to appear).
- [12] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*.

- Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.
- [13] D. Boneh. The decision Diffie-Hellman problem. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 48–63. Springer-Verlag, Berlin, 1998.
 - [14] D. Boneh and N. Daswani. Experimenting with electronic commerce on the PalmPilot. In *Financial Cryptography '99*, volume 1648 of *Lecture Notes in Comput. Sci.*, pages 1–16. Springer-Verlag, Berlin, 1999.
 - [15] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In *Advances in cryptology, Crypto 2001 (Santa Barbara, CA)*, volume 2139 of *Lecture Notes in Comput. Sci.*, pages 213–229. Springer-Verlag, Berlin, 2001.
 - [16] A. I. Borevich and I. R. Shafarevich. *Number theory*. Translated from the Russian by N. Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York, 1966.
 - [17] J. M. Borwein and P. B. Borwein. *Pi and the AGM*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons Inc., New York, 1987. A study in analytic number theory and computational complexity, A Wiley-Interscience Publication.
 - [18] W. Bosma and H. W. Lenstra, Jr. Complete systems of two addition laws for elliptic curves. *J. Number Theory*, 53(2):229–240, 1995.
 - [19] R. P. Brent, R. E. Crandall, K. Dilcher, and C. van Halewyn. Three new factors of Fermat numbers. *Math. Comp.*, 69(231):1297–1304, 2000.
 - [20] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.
 - [21] K. S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. Corrected reprint of the 1982 original.
 - [22] D. G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987.
 - [23] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.
 - [24] C. H. Clemens. *A scrapbook of complex curve theory*. Plenum Press, New York, 1980. The University Series in Mathematics.
 - [25] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

- [26] H. Cohen, A. Miyaji, and T. Ono. Efficient elliptic curve exponentiation using mixed coordinates. In *Advances in cryptology—ASIACRYPT'98 (Beijing)*, volume 1514 of *Lecture Notes in Comput. Sci.*, pages 51–65. Springer-Verlag, Berlin, 1998.
- [27] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography* Chapman & Hall/CRC, Boca Raton, 2005.
- [28] I. Connell. Addendum to a paper of K. Harada and M.-L. Lang: “Some elliptic curves arising from the Leech lattice” [*J. Algebra* 125 (1989), no. 2, 298–310]; *J. Algebra*, 145(2): 463–467, 1992.
- [29] G. Cornell, J. H. Silverman, and G. Stevens, editors. *Modular forms and Fermat’s last theorem*. Springer-Verlag, New York, 1997. Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995.
- [30] D. A. Cox. The arithmetic-geometric mean of Gauss. *Enseign. Math.* (2), 30(3-4):275–330, 1984.
- [31] J. Cremona. *Algorithms for modular elliptic curves, (2nd ed.)*. Cambridge University Press, 1997.
- [32] H. Darmon, F. Diamond, and R. Taylor. Fermat’s last theorem. In *Current developments in mathematics, 1995 (Cambridge, MA)*, pages 1–154. Internat. Press, Cambridge, MA, 1994.
- [33] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg*, 14:197–272, 1941.
- [34] L. E. Dickson. *History of the theory of numbers. Vol. II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.
- [35] D. Doud. A procedure to calculate torsion of elliptic curves over $\mathbf{Q}$. *Manuscripta Math.*, 95(4):463–469, 1998.
- [36] H. M. Edwards. A normal form for elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 44(3): 393–422, 2007.
- [37] N. D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math.*, 89(3):561–567, 1987.
- [38] A. Enge. *Elliptic curves and their applications to cryptography: An introduction*. Kluwer Academic Publishers, Dordrecht, 1999.
- [39] E. Fouvry and M. Ram Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1): 81–104, 1996.
- [40] G. Frey, M. Müller, and H.-G. Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Trans. Inform. Theory*, 45(5):1717–1719, 1999.

- [41] G. Frey and H.-G. Rück. A remark concerning m -divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62(206):865–874, 1994.
- [42] W. Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of R. Weiss, Reprint of 1969 original.
- [43] W. Fulton. *Intersection theory*. Springer-Verlag, Berlin, 1984.
- [44] S. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate pairing. In *Algorithmic number theory (Sydney, Australia, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 324–337. Springer-Verlag, Berlin, 2002.
- [45] S. D. Galbraith and N. P. Smart. A cryptographic application of Weil descent. In *Cryptography and coding (Cirencester, 1999)*, volume 1746 of *Lecture Notes in Comput. Sci.*, pages 191–200. Springer-Verlag, Berlin, 1999.
- [46] P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, 15(1):19–46, 2002.
- [47] S. Goldwasser and J. Kilian. Primality testing using elliptic curves. *J. ACM*, 46(4):450–472, 1999.
- [48] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to elliptic curve cryptography*. Springer-Verlag, New York, 2004.
- [49] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.
- [50] O. Herrmann. Über die Berechnung der Fourierkoeffizienten der Funktion $j(\tau)$. *J. reine angew. Math.*, 274/275:187–195, 1975. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III.
- [51] E. W. Howe. The Weil pairing and the Hilbert symbol. *Math. Ann.*, 305(2):387–392, 1996.
- [52] D. Husemoller. *Elliptic curves, (2nd ed.)*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2004. With appendices by O. Forster, R. Lawrence, and S. Theisen.
- [53] H. Ito. Computation of the modular equation. *Proc. Japan Acad. Ser. A Math. Sci.*, 71(3):48–50, 1995.
- [54] H. Ito. Computation of modular equation. II. *Mem. College Ed. Akita Univ. Natur. Sci.*, (52):1–10, 1997.

- [55] M. J. Jacobson, N. Koblitz, J. H. Silverman, A. Stein, and E. Teske. Analysis of the xedni calculus attack. *Des. Codes Cryptogr.*, 20(1):41–64, 2000.
- [56] A. Joux. A one round protocol for tripartite Diffie-Hellman. In *Algorithmic Number Theory (Leiden, The Netherlands, herefore maps2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 385–394. Springer-Verlag, Berlin, 2000.
- [57] A. Joux. The Weil and Tate pairings as building blocks for public key cryptosystems. In *Algorithmic number theory (Sydney, Australia, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 20–32. Springer-Verlag, Berlin, 2002.
- [58] A. Joux and R. Lercier. Improvements to the general number field sieve for discrete logarithms in prime fields. A comparison with the Gaussian integer method. *Math. Comp.*, 72(242):953–967, 2003.
- [59] E. Kani. Weil heights, Néron pairings and V -metrics on curves. *Rocky Mountain J. Math.*, 15(2):417–449, 1985. Number theory (Winnipeg, Man., 1983).
- [60] K. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4): 323–338, 2001; 18(4): 417–418, 2003.
- [61] A. W. Knap. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.
- [62] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3): 139–150, 1989.
- [63] N. Koblitz. CM-curves with good cryptographic properties. In *Advances in cryptology—CRYPTO '91 (Santa Barbara, CA, 1991)*, volume 576 of *Lecture Notes in Comput. Sci.*, pages 279–287. Springer-Verlag, Berlin, 1992.
- [64] N. Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.
- [65] N. Koblitz. *A course in number theory and cryptography*, volume 114 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.
- [66] N. Koblitz. *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998. With an appendix by A. J. Menezes, Y.-H. Wu, and R. J. Zuccherato.
- [67] D. S. Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

- [68] S. Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1978.
- [69] S. Lang. *Abelian varieties*. Springer-Verlag, New York, 1983. Reprint of the 1959 original.
- [70] S. Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.
- [71] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [72] H. Lange and W. Ruppert. Addition laws on elliptic curves in arbitrary characteristics. *J. Algebra*, 107(1):106–116, 1987.
- [73] G.-J. Lay and H. G. Zimmer. Constructing elliptic curves with given group order over large finite fields. In *Algorithmic number theory (Ithaca, NY, 1994)*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 250–263. Springer-Verlag, Berlin, 1994.
- [74] H. W. Lenstra, Jr. Elliptic curves and number-theoretic algorithms. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986)*, pages 99–120, Providence, RI, 1987. Amer. Math. Soc.
- [75] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math.* (2), 126(3):649–673, 1987.
- [76] E. Liverance. *Heights of Heegner points in a family of elliptic curves*. PhD thesis, Univ. of Maryland, 1993.
- [77] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.
- [78] H. McKean and V. Moll. *Elliptic curves. Function theory, geometry, arithmetic*. Cambridge University Press, Cambridge, 1997.
- [79] A. Menezes and M. Qu. Analysis of the Weil descent attack of Gaudry, Hess and Smart. In *Topics in cryptology—CT-RSA 2001 (San Francisco, CA)*, volume 2020 of *Lecture Notes in Comput. Sci.*, pages 308–318. Springer-Verlag, Berlin, 2001.
- [80] A. J. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.
- [81] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by R. L. Rivest.

- [82] A. Menezes. *Elliptic curve public key cryptosystems*, volume 234 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, MA, 1993. With a foreword by N. Koblitz.
- [83] V. Miller. The Weil pairing and its efficient calculation. *J. Cryptology*, 17(4):235–161, 2004.
- [84] T. Nagell. Sur les propriétés arithmétiques des cubiques planes du premier genre. *Acta Math.*, 52:93–126, 1929.
- [85] J. Oesterlé. Nouvelles approches du “théorème” de Fermat. *Astérisque*, (161-162):Exp. No. 694, 4, 165–186 (1989). Séminaire Bourbaki, Vol. 1987/88.
- [86] IEEE P1363-2000. *Standard specifications for public key cryptography*.
- [87] J. M. Pollard. Monte Carlo methods for index computation (mod p). *Math. Comp.*, 32(143):918–924, 1978.
- [88] V. Prasolov and Y. Solovyev. *Elliptic functions and elliptic integrals*, volume 170 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1997. Translated from the Russian manuscript by D. Leites.
- [89] K. A. Ribet. From the Taniyama-Shimura conjecture to Fermat’s last theorem. *Ann. Fac. Sci. Toulouse Math. (5)*, 11(1):116–139, 1990.
- [90] K. A. Ribet. On modular representations of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.
- [91] A. Robert. *Elliptic curves*. Springer-Verlag, Berlin, 1973. Lecture Notes in Mathematics, Vol. 326.
- [92] A. Rosing. *Implementing elliptic curve cryptography*. Manning Publications Company, 1999.
- [93] H.-G. Rück. A note on elliptic curves over finite fields. *Math. Comp.*, 49(179):301–304, 1987.
- [94] T. Satoh. On p -adic point counting algorithms for elliptic curves over finite fields. In *Algorithmic number theory (Sydney, Australia, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 43–66. Springer-Verlag, Berlin, 2002.
- [95] T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Comment. Math. Univ. St. Paul.*, 47(1):81–92, 1998. Errata: 48 (1999), 211–213.
- [96] E. Schaefer. A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field. *Computational aspects*

- of algebraic curves, volume 13 in *Lecture Notes Ser. Comput.*, pages 1–12, World Sci. Publ., Hackensack, NJ, 2005.
- [97] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p . *Math. Comp.*, 44(170):483–494, 1985.
 - [98] R. Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.
 - [99] R. Schoof. Counting points on elliptic curves over finite fields *J. Théorie des Nombres de Bordeaux*, 7: 219–254, 1995.
 - [100] R. Schoof and L. Washington. Untitled. In *Dopo le parole (aangeboden aan Dr. A. K. Lenstra. verzameld door H. W. Lenstra, Jr., J. K. Lenstra en P. van Emde Boas*, Amsterdam, 16 mei, 1984. 1 page.
 - [101] A. Selberg and S. Chowla. On Epstein’s zeta-function. *J. reine angew. Math.*, 227:86–110, 1967.
 - [102] I. A. Semaev. Evaluation of discrete logarithms in a group of p -torsion points of an elliptic curve in characteristic p . *Math. Comp.*, 67(221):353–356, 1998.
 - [103] J.-P. Serre. Complex multiplication. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 292–296. Thompson, Washington, D.C., 1967.
 - [104] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.
 - [105] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.
 - [106] I. Shafarevich *Basic algebraic geometry*. Translated from the Russian by K. A. Hirsch. Die Grundlehren der mathematischen Wissenschaften, Band 213. Springer-Verlag, New York-Heidelberg, 1974.
 - [107] D. Shanks. Class number, a theory of factorization, and genera. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, NY, 1969)*, pages 415–440. Amer. Math. Soc., Providence, RI, 1971.
 - [108] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.
 - [109] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
 - [110] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.

- [111] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.
- [112] J. H. Silverman. The xedni calculus and the elliptic curve discrete logarithm problem. *Des. Codes Cryptogr.*, 20(1):5–40, 2000.
- [113] J. H. Silverman and J. Suzuki. Elliptic curve discrete logarithms and the index calculus. In *Advances in cryptology—ASIACRYPT '98 (Beijing, China)*, volume 1514 of *Lecture Notes in Comput. Sci.*, pages 110–125. Springer-Verlag, Berlin, 1998.
- [114] J. H. Silverman and J. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.
- [115] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12(3):193–196, 1999.
- [116] J. Tate. The arithmetic of elliptic curves. *Invent. Math.*, 23:179–206, 1974.
- [117] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476. Springer-Verlag, Berlin, 1975.
- [118] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.
- [119] E. Teske. Speeding up Pollard's rho method for computing discrete logarithms. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 541–554. Springer-Verlag, Berlin, 1998.
- [120] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. *Advances in cryptology —ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Comput. Sci.*, pages 75–92. Springer-Verlag, Berlin, 2003.
- [121] W. Trappe and L. Washington. *Introduction to cryptography with coding theory, (2nd ed.)*. Prentice Hall, Upper Saddle River, NJ, 2006.
- [122] J. B. Tunnell. A classical Diophantine problem and modular forms of weight $3/2$. *Invent. Math.*, 72(2):323–334, 1983.
- [123] J. Vélú Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.
- [124] E. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *Eurocrypt 2001*, volume 2045 in *Lecture Notes in Computer Science*, pages 195–210. Springer-Verlag, Berlin 2001.

- [125] S. Wagstaff. *Cryptanalysis of number theoretic ciphers*. Computational Mathematics Series. Chapman and Hall/CRC, Boca Raton, 2003.
- [126] D. Q. Wan. On the Lang-Trotter conjecture. *J. Number Theory*, 35(3):247–268, 1990.
- [127] X. Wang, Y. Yin, Yiqun, and H. Yu. Finding collisions in the full SHA-1. *Advances in cryptology—CRYPTO 2005*, volume 3621 of *Lecture Notes in Comput. Sci.*, pages 17–36, Springer, Berlin, 2005.
- [128] L. Washington. Wiles’ strategy. In *Cuatrocientos años de matemáticas en torno al Último Teorema de Fermat* (ed. by C. Corrales Rodríguez and C. Andradás), pages 117–136. Editorial Complutense, Madrid, 1999. Section 13.4 of the present book is a reworking of much of this article.
- [129] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*, (2nd ed.). Springer-Verlag, New York, 1997.
- [130] W. C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.
- [131] A. Weil *Courbes algébriques et variétés abéliennes*. 2e éd.. Hermann & Cie., Paris, 1971.
- [132] E. Weiss. *Cohomology of groups*. Pure and Applied Mathematics, Vol. 34. Academic Press, New York, 1969.
- [133] A. Wiles. Modular elliptic curves and Fermat’s last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.
- [134] H. C. Williams. A $p+1$ method of factoring. *Math. Comp.*, 39(159):225–234, 1982.

Index

- Abel-Jacobi theorem, 266
- abelian variety, 215, 336
- additive reduction, 64, 434
- Adleman, 424
- affine plane, 19
- algebraic, 481
- algebraic closure, 481
- algebraic curve, 364
- algebraic integer, 314, 322
- algebraically independent, 485
- Alice, 169
- analytic continuation, 438
- anomalous curves, 159, 165
- arithmetic-geometric mean, 290
- Artin, E., 430, 431
- Artin, M., 432
- associativity, 20
- Atkin, 123, 396, 399
- Atkin prime, 401
- automorphism, 47, 74

- baby step, giant step, 112, 146, 151, 166, 197
- bad reduction, 436
- basis, 79, 87
- Bellare, 180
- Bernoulli numbers, 445
- beta function, 310
- Birch-Swinnerton-Dyer conjecture, 440
- Bob, 169
- Boneh-Franklin, 184
- Breuil, 436, 437
- Brumer, 447
- Buhler, 446

- cannonballs, 1

- canonical divisor, 366
- canonical height, 217
- Cantor's algorithm, 417
- characteristic, 481
- characteristic polynomial, 102, 333, 430
- characteristic three, 74
- characteristic two, 47, 52
- Chinese remainder theorem, 69, 152, 182, 193, 427, 472
- Chowla-Selberg formula, 293
- ciphertext, 169
- class number formula, 441
- Clay Mathematics Institute, 441
- Coates, 440
- coboundary, 245
- cocycle, 244
- cohomology, 244, 245
- complex multiplication, 197, 322, 336
- conductor, 314, 436, 451
- congruent number problem, 5
- conic section, 33
- conjecture of Taniyama-Shimura-Weil, 447, 455
- Conrad, 436, 437
- Crandall, 446
- Cremona, 111
- cryptography, 169
- cubic equations, 36
- cuspidal, 456
- cuspidal form, 450
- cyclic group, 478

- decision Diffie-Hellman problem, 171, 172
- deformations, 468

- degree, 51, 83, 87, 89, 100, 258, 339, 382, 387, 423
- Deligne, 432, 452
- Δ , 269, 275
- DeMarrais, 424
- descent, 209
- deterministic, 151
- Deuring's lifting theorem, 320
- Diamond, 436, 437
- Diffie-Hellman key exchange, 170
- Diffie-Hellman problem, 171, 174
- digital signature algorithm, 179
- digital signatures, 175
- Diophantus, 1, 8
- direct sum, 478
- Dirichlet unit theorem, 442
- discrete logarithm, 18, 143, 144, 157, 407, 420, 424
- discriminant, 314
- division polynomials, 80, 81, 83, 124, 294, 297, 300, 397
- divisor, 258, 339, 364, 409
- divisor of a function, 259, 342, 364
- doubly periodic function, 258
- Doud, 302
- dual isogeny, 382, 391, 396, 402, 405
- Dwork, 430
- ECIES, 180
- Edwards coordinates, 44
- Eichler, 437, 451
- Eisenstein series, 267, 273
- ElGamal digital signatures, 175, 187
- ElGamal public key encryption, 174
- Elkies, 123, 136, 396
- Elkies prime, 401
- elliptic curve, 9, 67, 310
- elliptic curve factorization, 192
- elliptic integral, 287, 310
- elliptic regulator, 440
- endomorphism, 50, 313, 319
- Ernvall, 446
- Euler product, 432, 433, 435
- Eve, 169
- exact sequence, 244, 246
- factor base, 144
- factoring, 181, 183, 189, 192
- Faltings, 402, 451
- Fermat, 231
- Fermat's Last Theorem, 7, 36, 38, 445, 455
- field, 481
- finite field, 482
- finite representation, 453
- flex, 93
- Floyd, 148
- Fouvry, 136
- Frey, 157
- Frey curve, 446, 454
- Frey-Rück attack, 157
- Frobenius automorphism, 482
- Frobenius endomorphism, 52, 58, 87, 98, 124, 142, 156, 318, 333, 351, 391, 430, 449
- function, 339
- functional equation, 430, 431, 438
- fundamental domain, 278, 456
- fundamental parallelogram, 257
- G -module, 244
- g_2 , 268, 274
- g_3 , 268, 274
- Galois representation, 80, 448
- gamma function, 293, 310, 437
- Gaudry, 424
- Gauss, 115, 288, 417
- generalized Weierstrass equation, 10, 15, 48, 254, 434
- genus, 366
- Goldwasser-Kilian test, 196
- good reduction, 64, 433
- Gross, 440
- Grothendieck, 432
- group, 477
- group law, 14, 71, 272
- Harley, 111, 424
- hash function, 177, 187, 188

- Hasse's theorem, 97, 100, 423, 431
Hasse-Minkowski theorem, 238
Hecke algebra, 450, 452, 459
Hecke operator, 450, 459
Heegner points, 440
height, 216
height pairing, 230
Hellegouarch, 446
Hensel's lemma, 241, 474
Hessian, 93
homomorphism, 480
homothetic, 273, 316
Huang, 424
hyperelliptic curve, 407, 408
hyperelliptic involution, 408

imaginary quadratic field, 314
index, 478, 509
index calculus, 144, 423
infinite descent, 231
isogenous, 381
isogeny, 142, 236, 381, 386, 397, 451
isomorphic, 389

 j -function, 275, 276
 j -invariant, 46–48, 73, 74, 139, 322, 331, 337
Jacobi sum, 118
Jacobian, 407, 415, 458
Jacobian coordinates, 43
Jugendtraum, 336

kangaroos, 150
kernel, 480
key, 169
Koblitz, 174, 407, 423
Kolyvagin, 252, 441
Kramer, 447
Kronecker-Weber theorem, 336
Kummer, 445

 L -function, 433, 435
 L -series, 447
Lagrange's theorem, 477

Lang-Trotter method, 106
Langlands, 462
lattice, 257, 479
Legendre equation, 35, 73, 132
Legendre symbol, 104, 140
Lenstra, 189
level, 450, 453
lines, 72, 73
local rings, 66
local-global principle, 238
Lutz-Nagell, 205

Magma, 492
Massey-Omura encryption, 173
maximal order, 319
Mazur, 208, 447
Mestre, 108
Metsänkylä, 446
minimal Weierstrass equation, 434
modular curve, 456
modular elliptic curve, 447, 458
modular form, 447, 450
modular polynomial, 329, 383, 398, 399
modular representation, 453
Mordell, 215
Mordell-Weil theorem, 16, 216
MOV attack, 154, 158
multiplication by n , 83
multiplicative reduction, 64, 434
Mumford representation, 415
Murty, 136

newform, 450
Newton's method, 413
nonsingular curve, 23, 24
nonsplit multiplicative reduction, 64, 434
normalized, 451
Nyberg-Rueppel signature, 188

oldform, 450
order, 106, 258, 279, 314, 340, 471, 477
ordinary, 79, 319, 320

- p -adic absolute value, 472
- p -adic numbers, 318, 472
- p -adic valuation, 160, 199, 472
- $p - 1$ factorization method, 191
- pairings, 154
- PalmPilot, 169
- Pappus's theorem, 34
- parallelogram law, 217
- Pari, 489
- Pascal's theorem, 33
- periods, 258, 284, 286
- Picard-Fuchs differential equation, 137
- plaintext, 169
- Pocklington-Lehmer test, 194
- Pohlig-Hellman method, 151, 167
- point at infinity, 11, 20, 408
- points at infinity, 18
- pole, 340
- Pollard's λ method, 150
- Pollard's ρ method, 147, 425
- primality testing, 189, 194, 196
- prime, 423
- prime number theorem, 141
- primitive, 65
- primitive root, 471
- principal divisor, 342
- probabilistic, 151
- projective coordinates, 42
- projective space, 18, 65, 72
- public key encryption, 170
- Pythagorean triples, 231

- quadratic field, 314
- quadratic surface, 39
- quaternions, 318, 319, 321, 338

- ramified, 318, 319
- rank, 16, 223, 479
- reduced divisor, 411
- reduction, 63, 70, 207, 416
- residue, 258
- Ribet, 448, 454
- Riemann hypothesis, 430, 431
- Riemann-Hurwitz, 395
- Riemann-Roch theorem, 366, 413, 414
- rings, 65
- Rogaway, 180
- root of unity, 87, 483
- RSA, 181
- Rubin, 252, 441
- Rück, 157

- Sage, 494
- Schmidt, 430, 431
- Schoof's algorithm, 123, 396
- Selmer group, 237, 252
- semi-reduced, 411
- semistable, 76, 437, 446, 447
- separable, 387
- separable endomorphism, 51, 58, 87, 351
- Serre, 452
- Shafarevich-Tate group, 237, 239, 252, 440
- Shanks, 146
- Shimura, 336, 436, 437, 451
- Shimura curve, 460
- $SL_2(\mathbf{Z})$, 276
- smooth, 191, 423, 424
- split, 318, 319
- split multiplicative reduction, 64, 434
- structure theorems, 478
- subexponential algorithm, 145
- subfield curves, 102
- successive doubling, 17, 18, 361
- successive squaring, 140
- sum, 339
- supersingular, 79, 130, 133, 142, 156, 168, 183, 185, 319, 321
- symmetric encryption, 169
- symmetric square, 470

- tangent line, 24
- tangent space, 465
- Taniyama, 436, 437
- Tate, 401

- Tate-Lichtenbaum pairing, 90, 157,
167, 168, 354, 360, 364,
374, 375
- Tate-Shafarevich group, 238
- Taylor, 436, 437
- Thériault, 424
- torsion, 88, 302, 479
- torsion points, 77, 79
- torsion subgroup, 206, 208, 223
- torus, 257, 267, 283, 285
- transcendence degree, 485
- tripartite Diffie-Hellman, 172
- Tunnell, 462
- twist, 47, 75, 108, 141, 334
- twisted homomorphisms, 245
- uniformizer, 340
- universal deformation, 468
- unramified representation, 453
- upper half plane, 273, 276, 436
- Vélu, 392
- van Duin, 178
- Vandiver, 446
- Wan, 136
- Wang, 178
- Waterhouse, 98
- weak Mordell-Weil theorem, 214
- Weierstrass $\wp$ -function, 262, 303,
341, 386
- Weierstrass equation, 9
- Weierstrass equation, generalized,
10, 15, 48
- Weil, 215, 423, 431, 436, 437
- Weil conjectures, 431
- Weil pairing, 86, 87, 154, 171, 172,
184, 185, 350, 359, 360
- Weil reciprocity, 357
- Wiles, 437, 440, 448, 461
- xedni calculus, 165
- Yin, 178
- Yu, 178
- Zagier, 440
- zero, 340
- zeta function, 273, 430, 432, 441