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 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 **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 **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. Knapp. *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 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 $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *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. Vélu 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 Rodrigáñez and C. Andradas)*, 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