References

[1] M. Abdalla, M. Bellare, and P. Rogaway. The oracle Diffie-Hellman assumptions and an analysis of DHIES. In *Topics in cryptology—CT-RSA 2001 (San Francisco, CA)*, volume 2020 of *Lecture Notes in Comput. Sci.*, pages 143–158. Springer, Berlin, 2001.

[2] D. Abramovich. Formal finiteness and the torsion conjecture on elliptic curves. A footnote to a paper: "Rational torsion of prime order in elliptic curves over number fields" [Astérisque No. 228 (1995), 3, 81–100] by S. Kamienny and B. Mazur. *Astérisque*, (228):3, 5–17, 1995. Columbia University Number Theory Seminar (New York, 1992).

[3] 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.

[4] T. M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York, 1976. Undergraduate Texts in Mathematics.

[5] T. M. Apostol. *Modular functions and Dirichlet series in number theory*, volume 41 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[6] N. Arthaud. On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication. I. *Compositio Math.*, 37(2):209–232, 1978.

[7] E. Artin. *Galois theory*. Dover Publications Inc., Mineola, NY, second edition, 1998. Edited and with a supplemental chapter by Arthur N. Milgram.

[8] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.–London–Don Mills, Ont., 1969.

[9] 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.

[10] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.

[11] A. Baker. *Transcendental number theory*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, second edition, 1990.

[12] A. Baker and J. Coates. Integer points on curves of genus 1. *Proc. Cambridge Philos. Soc.*, 67:595–602, 1970.

[13] 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.

[14] A. F. Beardon. *Iteration of Rational Functions*, volume 132 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. Complex analytic dynamical systems.

[15] E. Bekyel. The density of elliptic curves having a global minimal Weierstrass equation. *J. Number Theory*, 109(1):41–58, 2004.

[16] D. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In *Advances in cryptology—ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Comput. Sci.*, pages 29–50. Springer, Berlin, 2007.

[17] B. J. Birch. Cyclotomic fields and Kummer extensions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 85–93. Thompson, Washington, D.C., 1967.

[18] B. J. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 43:57–60, 1968.

[19] B. J. Birch and W. Kuyk, editors. *Modular functions of one variable. IV*. Springer-Verlag, Berlin, 1975. Lecture Notes in Mathematics, Vol. 476.

[20] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[21] B. J. Birch and H. P. F. Swinnerton-Dyer. Elliptic curves and modular functions. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 2–32. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

[22] 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.

[23] 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, Berlin, 2001.

[24] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 514–532. Springer, Berlin, 2001.

[25] A. I. Borevich and I. R. Shafarevich. *Number theory*. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York, 1966.

[26] A. Bremner. On the equation $Y^2 = X(X^2 + p)$. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 3–22. Kluwer Acad. Publ., Dordrecht, 1989.

[27] A. Bremner and J. W. S. Cassels. On the equation $Y^2 = X(X^2 + p)$. *Math. Comp.*, 42(165):257–264, 1984.

[28] 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 (electronic), 2001.

[29] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptogr.*, 37(1):133–141, 2005.

[30] M. L. Brown. Note on supersingular primes of elliptic curves over $\mathbf{Q}$. *Bull. London Math. Soc.*, 20(4):293–296, 1988.

[31] W. D. Brownawell and D. W. Masser. Vanishing sums in function fields. *Math. Proc. Cambridge Philos. Soc.*, 100(3):427–434, 1986.

[32] Y. Bugeaud. Bounds for the solutions of superelliptic equations. *Compositio Math.*, 107(2):187–219, 1997.

[33] J. P. Buhler, B. H. Gross, and D. B. Zagier. On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3. *Math. Comp.*, 44(170):473–481, 1985.

[34] E. R. Canfield, P. Erdős, and C. Pomerance. On a problem of Oppenheim concerning "factorisatio numerorum." *J. Number Theory*, 17(1):1–28, 1983.

[35] H. Carayol. Sur les représentations galoisiennes modulo l attachées aux formes modulaires. *Duke Math. J.*, 59(3):785–801, 1989.

[36] J. W. S. Cassels. A note on the division values of $\wp(u)$. *Proc. Cambridge Philos. Soc.*, 45:167–172, 1949.

[37] J. W. S. Cassels. Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups. *Proc. London Math. Soc. (3)*, 12:259–296, 1962.

[38] J. W. S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *J. Reine Angew. Math.*, 211:95–112, 1962.

[39] J. W. S. Cassels. Arithmetic on curves of genus 1. V. Two counterexamples. *J. London Math. Soc.*, 38:244–248, 1963.

[40] J. W. S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965.

[41] J. W. S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 41:193–291, 1966.

[42] J. W. S. Cassels. Global fields. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 42–84. Thompson, Washington, D.C., 1967.

[43] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[44] T. Chinburg. An introduction to Arakelov intersection theory. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 289–307. Springer, New York, 1986.

[45] D. V. Chudnovsky and G. V. Chudnovsky. Padé approximations and Diophantine geometry. *Proc. Nat. Acad. Sci. U.S.A.*, 82(8):2212–2216, 1985.

[46] C. H. Clemens. *A scrapbook of complex curve theory*, volume 55 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 2003.

[47] L. Clozel, M. Harris, and R. Taylor. Automorphy for some l-adic lifts of automorphic mod l representations. 2007. IHES Publ. Math., submitted.

[48] J. Coates. Construction of rational functions on a curve. *Proc. Cambridge Philos. Soc.*, 68:105–123, 1970.

[49] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[50] H. Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[51] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete Mathematics and Its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[52] D. A. Cox. The arithmetic-geometric mean of Gauss. *Enseign. Math. (2)*, 30(3-4):275–330, 1984.

[53] J. Cremona. *Elliptic Curve Data*. `http://sage.math.washington.edu/cremona/index.html`, `http://www.math.utexas.edu/users/tornaria/cnt/cremona.html`.

[54] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997. available free online at `www.warwick.ac.uk/staff/J.E.Cremona/book/fulltext/index.html`.

[55] J. E. Cremona, M. Prickett, and S. Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, 116(1):42–68, 2006.

[56] L. V. Danilov. The Diophantine equation $x^3 - y^2 = k$ and a conjecture of M. Hall. *Mat. Zametki*, 32(3):273–275, 425, 1982. English translation: *Math. Notes Acad. Sci. USSR* **32** (1982), no. 3–4, 617–618 (1983).

[57] H. Davenport. On $f^3(t) - g^2(t)$. *Norske Vid. Selsk. Forh. (Trondheim)*, 38:86–87, 1965.

[58] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.)*, (62):iv+143, 1995.

[59] B. M. M. de Weger. *Algorithms for Diophantine equations*, volume 65 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[60] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[61] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. Math.-Phys.-Chem. Abt.*, 1953:85–94, 1953.

[62] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. II. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1955:13–42, 1955.

[63] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. III. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1956:37–76, 1956.

[64] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. IV. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1957:55–80, 1957.

[65] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6):644–654, 1976.

[66] L. Dirichlet. Über den biquadratischen Charakter der Zahl "Zwei." *J. Reine Angew. Math.*, 57:187–188, 1860.

[67] Z. Djabri, E. F. Schaefer, and N. P. Smart. Computing the p-Selmer group of an elliptic curve. *Trans. Amer. Math. Soc.*, 352(12):5583–5597, 2000.

[68] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[69] R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. *J. Cryptology*, 18(2):79–89, 2005.

[70] B. Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math.*, 82:631–648, 1960.

[71] H. M. Edwards. A normal form for elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 44(3):393–422 (electronic), 2007.

[72] M. Eichler. Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Arch. Math.*, 5:355–366, 1954.

[73] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[74] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, 31(4):469–472, 1985.

[75] N. Elkies. List of integers x, y with $x < 10^{18}$, $0 < |x^3 - y^2| < x^{1/2}$. `www.math.harvard.edu/~elkies/hall.html`.

[76] N. Elkies. $\mathbb{Z}^{28}$ in $E(\mathbb{Q})$. Number Theory Listserver, May 2006.

[77] N. D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. *Invent. Math.*, 89(3):561–567, 1987.

[78] N. D. Elkies. Distribution of supersingular primes. *Astérisque*, (198-200):127–132 (1992), 1991. Journées Arithmétiques, 1989 (Luminy, 1989).

[79] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

[80] J.-H. Evertse. On equations in S-units and the Thue-Mahler equation. *Invent. Math.*, 75(3):561–584, 1984.

[81] J.-H. Evertse and J. H. Silverman. Uniform bounds for the number of solutions to $Y^n = f(X)$. *Math. Proc. Cambridge Philos. Soc.*, 100(2):237–248, 1986.

[82] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[83] G. Faltings. Calculus on arithmetic surfaces. *Ann. of Math. (2)*, 119(2):387–424, 1984.

[84] G. Faltings. Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 9–27. Springer, New York, 1986. Translated from the German original [Invent. Math. **73** (1983), no. 3, 349–366; ibid. **75** (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz.

[85] S. Fermigier. Une courbe elliptique définie sur $\mathbf{Q}$ de rang ≥ 22. *Acta Arith.*, 82(4):359–363, 1997.

[86] E. V. Flynn and C. Grattoni. Descent via isogeny on elliptic curves with large rational torsion subgroups. *J. Symbolic Comput.*, 43(4):293–303, 2008.

[87] D. Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 452–465. Springer, Berlin, 2006.

[88] G. Frey. Links between stable elliptic curves and certain Diophantine equations. *Ann. Univ. Sarav. Ser. Math.*, 1(1):iv+40, 1986.

[89] G. Frey. Elliptic curves and solutions of $A - B = C$. In *Séminaire de Théorie des Nombres, Paris 1985–86*, volume 71 of *Progr. Math.*, pages 39–51. Birkhäuser Boston, Boston, MA, 1987.

[90] G. Frey. Links between solutions of $A - B = C$ and elliptic curves. In *Number theory (Ulm, 1987)*, volume 1380 of *Lecture Notes in Math.*, pages 31–62. Springer, New York, 1989.

[91] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.

[92] A. Fröhlich. Local fields. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 1–41. Thompson, Washington, D.C., 1967.

[93] A. Fröhlich. *Formal groups*. Lecture Notes in Mathematics, No. 74. Springer-Verlag, Berlin, 1968.

[94] R. Fueter. Ueber kubische diophantische Gleichungen. *Comment. Math. Helv.*, 2(1):69–89, 1930.

[95] 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 Richard Weiss, Reprint of 1969 original.

[96] J. Gebel, A. Pethő, and H. G. Zimmer. Computing integral points on elliptic curves. *Acta Arith.*, 68(2):171–192, 1994.

[97] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. In *STOC '86: Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 316–329, New York, 1986. ACM.

[98] R. Greenberg. On the Birch and Swinnerton-Dyer conjecture. *Invent. Math.*, 72(2):241–265, 1983.

[99] P. Griffiths and J. Harris. *Principles of algebraic geometry*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1994. Reprint of the 1978 original.

[100] B. Gross, W. Kohnen, and D. Zagier. Heegner points and derivatives of L-series. II. *Math. Ann.*, 278(1-4):497–562, 1987.

[101] B. Gross and D. Zagier. Points de Heegner et dérivées de fonctions L. *C. R. Acad. Sci. Paris Sér. I Math.*, 297(2):85–87, 1983.

[102] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[103] R. Gross. A note on Roth's theorem. *J. Number Theory*, 36:127–132, 1990.

[104] R. Gross and J. Silverman. S-integer points on elliptic curves. *Pacific J. Math.*, 167(2):263–288, 1995.

[105] K. Gruenberg. Profinite groups. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 116–127. Thompson, Washington, D.C., 1967.

[106] M. Hall, Jr. The Diophantine equation $x^3 - y^2 = k$. In *Computers in number theory (Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969)*, pages 173–198. Academic Press, London, 1971.

[107] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to elliptic curve cryptography*. Springer Professional Computing. Springer-Verlag, New York, 2004.

[108] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[109] J. Harris. *Algebraic geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. A first course.

[110] M. Harris, N. Shepherd-Barron, and R. Taylor. A family of Calabi-Yau varieties and potential automorphy. *Ann. of Math. (2)*. to appear.

[111] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[112] M. Hazewinkel. *Formal groups and applications*, volume 78 of *Pure and Applied Mathematics*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1978.

[113] M. Hindry and J. H. Silverman. The canonical height and integral points on elliptic curves. *Invent. Math.*, 93(2):419–450, 1988.

[114] M. Hindry and J. H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[115] G. Hochschild and J.-P. Serre. Cohomology of group extensions. *Trans. Amer. Math. Soc.*, 74:110–134, 1953.

[116] J. Hoffstein, J. Pipher, and J. H. Silverman. *An introduction to mathematical cryptography*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2008.

[117] A. Hurwitz. Über ternäre diophantische Gleichungen dritten Grades. *Vierteljahrschrift d. Naturf. Ges. Zürich*, 62:207–229, 1917.

[118] D. Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[119] J.-I. Igusa. Class number of a definite quaternion with prime discriminant. *Proc. Nat. Acad. Sci. U.S.A.*, 44:312–314, 1958.

[120] A. Joux. A one round protocol for tripartite Diffie-Hellman. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 385–393. Springer, Berlin, 2000.

[121] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

[122] S. Kamienny and B. Mazur. Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, (228):3, 81–100, 1995. With an appendix by A. Granville, Columbia University Number Theory Seminar (New York, 1992).

[123] N. M. Katz. An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields. In *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974)*, pages 275–305. Amer. Math. Soc., Providence, R.I., 1976.

[124] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[125] M. A. Kenku. On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class. *J. Number Theory*, 15(2):199–202, 1982.

[126] J.-H. Kim, R. Montenegro, Y. Peres, and P. Tetali. A birthday paradox for Markov chains, with an optimal bound for collision in Pollard rho for discrete logarithm. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 402–415. Springer, Berlin, 2008.

[127] A. W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[128] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[129] N. Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[130] V. A. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[131] S. V. Kotov and L. A. Trelina. S-ganze Punkte auf elliptischen Kurven. *J. Reine Angew. Math.*, 306:28–41, 1979.

[132] D. S. Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[133] E. Kunz. *Introduction to plane algebraic curves*. Birkhäuser Boston Inc., Boston, MA, 2005. Translated from the 1991 German edition by Richard G. Belshoff.

[134] M. Lal, M. F. Jones, and W. J. Blundon. Numerical solutions of the Diophantine equation $y^3 - x^2 = k$. *Math. Comp.*, 20:322–325, 1966.

[135] S. Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1978.

[136] S. Lang. *Introduction to algebraic and abelian functions*, volume 89 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1982.

[137] S. Lang. *Complex multiplication*, volume 255 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983.

[138] S. Lang. Conjectured Diophantine estimates on elliptic curves. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 155–171. Birkhäuser Boston, Boston, MA, 1983.

[139] S. Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[140] S. Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[141] S. Lang. *Number theory III*, volume 60 of *Encyclopedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1991.

[142] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[143] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[144] S. Lang and J. Tate. Principal homogeneous spaces over abelian varieties. *Amer. J. Math.*, 80:659–684, 1958.

[145] S. Lang and H. Trotter. *Frobenius distributions in* GL_2*-extensions*. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers, Lecture Notes in Mathematics, Vol. 504.

[146] M. Laska. An algorithm for finding a minimal Weierstrass equation for an elliptic curve. *Math. Comp.*, 38(157):257–260, 1982.

[147] M. Laska. *Elliptic curves over number fields with prescribed reduction type*. Aspects of Mathematics, E4. Friedr. Vieweg & Sohn, Braunschweig, 1983.

[148] D. J. Lewis and K. Mahler. On the representation of integers by binary forms. *Acta Arith.*, 6:333–363, 1960/1961.

[149] S. Lichtenbaum. The period-index problem for elliptic curves. *Amer. J. Math.*, 90:1209–1223, 1968.

[150] C.-E. Lind. Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins. *Thesis, University of Uppsala,*, 1940:97, 1940.

[151] J. Liouville. Sur des classes très-étendues de quantités dont la irrationalles algébriques. *C. R. Acad. Paris*, 18:883–885 and 910–911, 1844.

[152] E. Lutz. Sur l'equation $y^2 = x^3 - ax - b$ dans les corps p-adic. *J. Reine Angew. Math.*, 177:237–247, 1937.

[153] K. Mahler. On the lattice points on curves of genus 1. *Proc. London Math. Soc. (3)*, 39:431–466, 1935.

[154] J. I. Manin. The Hasse-Witt matrix of an algebraic curve. *Izv. Akad. Nauk SSSR Ser. Mat.*, 25:153–172, 1961.

[155] J. I. Manin. The p-torsion of elliptic curves is uniformly bounded. *Izv. Akad. Nauk SSSR Ser. Mat.*, 33:459–465, 1969.

[156] J. I. Manin. Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, 26(6(162)):7–71, 1971. English translation: Russian Math. Surveys 26 (1971), no. 6, 7–78.

[157] R. C. Mason. The hyperelliptic equation over function fields. *Math. Proc. Cambridge Philos. Soc.*, 93(2):219–230, 1983.

[158] R. C. Mason. Norm form equations. I. *J. Number Theory*, 22(2):190–207, 1986.

[159] D. Masser. *Elliptic functions and transcendence*. Springer-Verlag, Berlin, 1975. Lecture Notes in Mathematics, Vol. 437.

[160] D. Masser and G. Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993.

[161] D. W. Masser. Specializations of finitely generated subgroups of abelian varieties. *Trans. Amer. Math. Soc.*, 311(1):413–424, 1989.

[162] D. W. Masser and G. Wüstholz. Fields of large transcendence degree generated by values of elliptic functions. *Invent. Math.*, 72(3):407–464, 1983.

[163] D. W. Masser and G. Wüstholz. Estimating isogenies on elliptic curves. *Invent. Math.*, 100(1):1–24, 1990.

[164] H. Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[165] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[166] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[167] H. McKean and V. Moll. *Elliptic curves*. Cambridge University Press, Cambridge, 1997. Function theory, geometry, arithmetic.

[168] 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.

[169] 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.

[170] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[171] J.-F. Mestre. Construction d'une courbe elliptique de rang ≥ 12. *C. R. Acad. Sci. Paris Sér. I Math.*, 295(12):643–644, 1982.

[172] J.-F. Mestre. Courbes elliptiques et formules explicites. In *Seminar on number theory, Paris 1981–82 (Paris, 1981/1982)*, volume 38 of *Progr. Math.*, pages 179–187. Birkhäuser Boston, Boston, MA, 1983.

[173] M. Mignotte. Quelques remarques sur l'approximation rationnelle des nombres algébriques. *J. Reine Angew. Math.*, 268/269:341–347, 1974. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II.

[174] S. D. Miller and R. Venkatesan. Spectral analysis of Pollard rho collisions. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 573–581. Springer, Berlin, 2006.

[175] S. D. Miller and R. Venkatesan. Non-degeneracy of Pollard rho collisions, 2008. `arXiv:0808.0469`.

[176] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer, Berlin, 1986.

[177] J. S. Milne. *Arithmetic duality theorems*, volume 1 of *Perspectives in Mathematics*. Academic Press Inc., Boston, MA, 1986.

[178] J. S. Milne. *Elliptic curves*. BookSurge Publishers, Charleston, SC, 2006.

[179] J. Milnor. On Lattès maps. `ArXiv:math.DS/0402147`, Stony Brook IMS Preprint #2004/01.

[180] R. Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1995.

[181] A. Miyaji, M. Nakabayashi, and S. Takano. Characterization of elliptic curve traces under FR-reduction. In *Information security and cryptology—ICISC 2000 (Seoul)*, volume 2015 of *Lecture Notes in Comput. Sci.*, pages 90–108. Springer, Berlin, 2001.

[182] P. Monsky. Three constructions of rational points on $Y^2 = X^3 \pm NX$. *Math. Z.*, 209(3):445–462, 1992.

[183] F. Morain. Building cyclic elliptic curves modulo large primes. In *Advances in cryptology—EUROCRYPT '91 (Brighton, 1991)*, volume 547 of *Lecture Notes in Comput. Sci.*, pages 328–336. Springer, Berlin, 1991.

[184] L. J. Mordell. The diophantine equation $x^4 + my^4 = z^2$.. *Quart. J. Math. Oxford Ser. (2)*, 18:1–6, 1967.

[185] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.

[186] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[187] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)]*. Springer-Verlag, Berlin, third edition, 1994.

[188] K.-I. Nagao. Construction of high-rank elliptic curves. *Kobe J. Math.*, 11(2):211–219, 1994.

[189] K.-I. Nagao. $\mathbb{Q}(T)$-rank of elliptic curves and certain limit coming from the local points. *Manuscripta Math.*, 92(1):13–32, 1997. With an appendix by Nobuhiko Ishida, Tsuneo Ishikawa and the author.

[190] T. Nagell. Solution de quelque problèmes dans la théorie arithmétique des cubiques planes du premier genre. *Wid. Akad. Skrifter Oslo I*, 1935. Nr. 1.

[191] NBS–DSS. Digital Signature Standard (DSS). FIPS Publication 186-2, National Bureau of Standards, 2000. `http://csrc.nist.gov/publications/PubsFIPS.html`.

[192] A. Néron. Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps. *Bull. Soc. Math. France*, 80:101–166, 1952.

[193] A. Néron. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Inst. Hautes Études Sci. Publ.Math. No.*, 21:128, 1964.

[194] A. Néron. Quasi-fonctions et hauteurs sur les variétés abéliennes. *Ann. of Math. (2)*, 82:249–331, 1965.

[195] O. Neumann. Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. I. *Math. Nachr.*, 49:107–123, 1971.

[196] J. Oesterlé. Nouvelles approches du "théorème" de Fermat. *Astérisque*, (161-162):Exp. No. 694, 4, 165–186 (1989), 1988. Séminaire Bourbaki, Vol. 1987/88.

[197] A. Ogg. *Modular forms and Dirichlet series*. W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[198] A. P. Ogg. Abelian curves of 2-power conductor. *Proc. Cambridge Philos. Soc.*, 62:143–148, 1966.

[199] A. P. Ogg. Abelian curves of small conductor. *J. Reine Angew. Math.*, 226:204–215, 1967.

[200] A. P. Ogg. Elliptic curves and wild ramification. *Amer. J. Math.*, 89:1–21, 1967.

[201] L. D. Olson. Torsion points on elliptic curves with given j-invariant. *Manuscripta Math.*, 16(2):145–150, 1975.

[202] *PARI/GP*, 2005. `http://pari.math.u-bordeaux.fr/`.

[203] A. N. Paršin. Algebraic curves over function fields. I. *Izv. Akad. Nauk SSSR Ser. Mat.*, 32:1191–1219, 1968.

[204] R. G. E. Pinch. Elliptic curves with good reduction away from 2. *Math. Proc. Cambridge Philos. Soc.*, 96(1):25–38, 1984.

[205] S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over $\mathrm{GF}(p)$ and its cryptographic significance. *IEEE Trans. Information Theory*, IT-24(1):106–110, 1978.

[206] J. M. Pollard. Monte Carlo methods for index computation $(\mathrm{mod}\ p)$. *Math. Comp.*, 32(143):918–924, 1978.

[207] H. Reichardt. Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen. *J. Reine Angew. Math.*, 184:12–18, 1942.

[208] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[209] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[210] A. Robert. *Elliptic curves*. Springer-Verlag, Berlin, 1973. Notes from postgraduate lectures given in Lausanne 1971/72, Lecture Notes in Mathematics, Vol. 326.

[211] D. E. Rohrlich. On L-functions of elliptic curves and anticyclotomic towers. *Invent. Math.*, 75(3):383–408, 1984.

[212] P. Roquette. *Analytic theory of elliptic functions over local fields*. Hamburger Mathematische Einzelschriften (N.F.), Heft 1. Vandenhoeck & Ruprecht, Göttingen, 1970.

[213] M. Rosen and J. H. Silverman. On the rank of an elliptic surface. *Invent. Math.*, 133(1):43–67, 1998.

[214] K. Rubin. Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 64(3):455–470, 1981.

[215] K. Rubin. Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. *Invent. Math.*, 89(3):527–559, 1987.

[216] K. Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.

[217] T. Saito. Conductor, discriminant, and the Noether formula of arithmetic surfaces. *Duke Math. J.*, 57(1):151–173, 1988.

[218] 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.

[219] E. F. Schaefer and M. Stoll. How to do a p-descent on an elliptic curve. *Trans. Amer. Math. Soc.*, 356(3):1209–1231 (electronic), 2004.

[220] S. H. Schanuel. Heights in number fields. *Bull. Soc. Math. France*, 107(4):433–449, 1979.

[221] W. M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[222] S. Schmitt and H. G. Zimmer. *Elliptic curves*, volume 31 of *de Gruyter Studies in Mathematics*. Walter de Gruyter & Co., Berlin, 2003. A computational approach, With an appendix by Attila Pethő.

[223] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

[224] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[225] E. S. Selmer. The Diophantine equation $ax^3+by^3+cz^3 = 0$. *Acta Math.*, 85:203–362 (1 plate), 1951.

[226] E. S. Selmer. A conjecture concerning rational points on cubic curves. *Math. Scand.*, 2:49–54, 1954.

[227] E. S. Selmer. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. Completion of the tables. *Acta Math.*, 92:191–197, 1954.

[228] 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.

[229] J.-P. Serre. Géométrie algébrique et géométrie analytique. *Ann. Inst. Fourier, Grenoble*, 6:1–42, 1955–1956.

[230] J.-P. Serre. Complex multiplication. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 292–296. Thompson, Washington, D.C., 1967.

[231] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[232] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[233] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[234] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[235] 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.

[236] J.-P. Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[237] J.-P. Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[238] J.-P. Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[239] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[240] B. Setzer. Elliptic curves of prime conductor. *J. London Math. Soc. (2)*, 10:367–378, 1975.

[241] B. Setzer. Elliptic curves over complex quadratic fields. *Pacific J. Math.*, 74(1):235–250, 1978.

[242] I. R. Shafarevich. Algebraic number fields. In *Proc. Int. Cong. (Stockholm 1962)*, pages 25–39. American Mathematical Society, Providence, R.I., 1963. Amer. Math. Soc. Transl., Series 2, Vol. 31.

[243] I. R. Shafarevich. *Basic algebraic geometry*. Springer-Verlag, Berlin, study edition, 1977. Translated from the Russian by K. A. Hirsch, Revised printing of Grundlehren der mathematischen Wissenschaften, Vol. 213, 1974.

[244] I. R. Shafarevich and J. Tate. The rank of elliptic curves. In *Amer. Math. Soc. Transl.*, volume 8, pages 917–920. Amer. Math. Soc., 1967.

[245] A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology (Santa Barbara, Calif., 1984)*, volume 196 of *Lecture Notes in Comput. Sci.*, pages 47–53. Springer, Berlin, 1985.

[246] G. Shimura. Correspondances modulaires et les fonctions ζ de courbes algébriques. *J. Math. Soc. Japan*, 10:1–28, 1958.

[247] G. Shimura. On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. *Nagoya Math. J.*, 43:199–208, 1971.

[248] G. Shimura. On the zeta-function of an abelian variety with complex multiplication. *Ann. of Math. (2)*, 94:504–533, 1971.

[249] 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, Kano Memorial Lectures, 1.

[250] G. Shimura and Y. Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.

[251] T. Shioda. An explicit algorithm for computing the Picard number of certain algebraic surfaces. *Amer. J. Math.*, 108(2):415–432, 1986.

[252] R. Shipsey. *Elliptic divisibility sequences*. PhD thesis, Goldsmith's College (University of London), 2000.

[253] V. Shoup. Lower bounds for discrete logarithms and related problems. In *Advances in cryptology—EUROCRYPT '97 (Konstanz)*, volume 1233 of *Lecture Notes in Comput. Sci.*, pages 256–266. Springer, Berlin, 1997. updated version at `www.shoup.net/papers/dlbounds1.pdf`.

[254] J. H. Silverman. Lower bound for the canonical height on elliptic curves. *Duke Math. J.*, 48(3):633–648, 1981.

[255] J. H. Silverman. *The Néron–Tate height on elliptic curves*. PhD thesis, Harvard University, 1981.

[256] J. H. Silverman. Heights and the specialization map for families of abelian varieties. *J. Reine Angew. Math.*, 342:197–211, 1983.

[257] J. H. Silverman. Integer points on curves of genus 1. *J. London Math. Soc. (2)*, 28(1):1–7, 1983.

[258] J. H. Silverman. The S-unit equation over function fields. *Math. Proc. Cambridge Philos. Soc.*, 95(1):3–4, 1984.

[259] J. H. Silverman. Weierstrass equations and the minimal discriminant of an elliptic curve. *Mathematika*, 31(2):245–251 (1985), 1984.

[260] J. H. Silverman. Divisibility of the specialization map for families of elliptic curves. *Amer. J. Math.*, 107(3):555–565, 1985.

[261] J. H. Silverman. Arithmetic distance functions and height functions in Diophantine geometry. *Math. Ann.*, 279(2):193–216, 1987.

[262] J. H. Silverman. A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves. *J. Reine Angew. Math.*, 378:60–100, 1987.

[263] J. H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988.

[264] J. H. Silverman. Wieferich's criterion and the abc-conjecture. *J. Number Theory*, 30(2):226–237, 1988.

[265] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.

[266] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[267] J. H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[268] N. P. Smart. S-integral points on elliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 116(3):391–399, 1994.

[269] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12(3):193–196, 1999.

[270] K. Stange. The Tate pairing via elliptic nets. In *Pairing Based Cryptography*, Lecture Notes in Comput. Sci. Springer, 2007.

[271] K. Stange. *Elliptic Nets and Elliptic Curves*. PhD thesis, Brown University, 2008.

[272] K. Stange. Elliptic nets and elliptic curves, 2008. `arXiv:0710.1316v2`.

[273] H. M. Stark. Effective estimates of solutions of some Diophantine equations. *Acta Arith.*, 24:251–259, 1973.

[274] W. Stein. *The Modular Forms Database*. `http://modular.fas.harvard.edu/Tables`.

[275] W. Stein. *Sage Mathematics Software*, 2007. `http://www.sagemath.org`.

[276] N. M. Stephens. The Diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 231:121–162, 1968.

[277] D. R. Stinson. *Cryptography: Theory and Practice*. CRC Press Series on Discrete Mathematics and Its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2002.

[278] W. W. Stothers. Polynomial identities and Hauptmoduln. *Quart. J. Math. Oxford Ser. (2)*, 32(127):349–370, 1981.

[279] R. J. Stroeker and N. Tzanakis. Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arith.*, 67(2):177–196, 1994.

[280] J. Tate. Letter to J.-P. Serre, 1968.

[281] J. Tate. Duality theorems in Galois cohomology over number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 288–295. Inst. Mittag-Leffler, Djursholm, 1963.

[282] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[283] 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, Berlin, 1975.

[284] J. Tate. Variation of the canonical height of a point depending on a parameter. *Amer. J. Math.*, 105(1):287–294, 1983.

[285] J. Tate. A review of non-Archimedean elliptic functions. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 162–184. Int. Press, Cambridge, MA, 1995.

[286] J. Tate. WC-groups over $\mathfrak{p}$-adic fields. In *Séminaire Bourbaki, Vol. 4 (1957/58)*, pages Exp. No. 156, 265–277. Soc. Math. France, Paris, 1995.

[287] J. T. Tate. Algebraic cycles and poles of zeta functions. In *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 93–110. Harper & Row, New York, 1965.

[288] J. T. Tate. Global class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 162–203. Thompson, Washington, D.C., 1967.

[289] J. T. Tate. The arithmetic of elliptic curves. *Invent. Math.*, 23:179–206, 1974.

[290] R. Taylor. Automorphy for some l-adic lifts of automorphic mod l representations. II. *Inst. Hautes Études Sci. Publ. Math.* submitted.

[291] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[292] E. Teske. A space efficient algorithm for group structure computation. *Math. Comp.*, 67(224):1637–1663, 1998.

[293] 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, Berlin, 1998.

[294] E. Teske. Square-root algorithms for the discrete logarithm problem (a survey). In *Public-Key Cryptography and Computational Number Theory (Warsaw, 2000)*, pages 283–301. de Gruyter, Berlin, 2001.

[295] D. Ulmer. Elliptic curves with large rank over function fields. *Ann. of Math. (2)*, 155(1):295–315, 2002.

[296] B. L. van der Waerden. *Algebra. Vols. I and II*. Springer-Verlag, New York, 1991. Based in part on lectures by E. Artin and E. Noether, Translated from the seventh German edition by Fred Blum and John R. Schulenberger.

[297] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[298] P. Vojta. A higher-dimensional Mordell conjecture. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 341–353. Springer, New York, 1986.

[299] P. Vojta. Siegel's theorem in the compact case. *Ann. of Math. (2)*, 133(3):509–548, 1991.

[300] J. F. Voloch. Diagonal equations over function fields. *Bol. Soc. Brasil. Mat.*, 16(2):29–39, 1985.

[301] P. M. Voutier. An upper bound for the size of integral solutions to $Y^m = f(X)$. *J. Number Theory*, 53(2):247–271, 1995.

[302] R. J. Walker. *Algebraic curves*. Springer-Verlag, New York, 1978. Reprint of the 1950 edition.
[303] M. Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.
[304] L. C. Washington. *Elliptic curves*. Discrete Mathematics and Its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.
[305] A. Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.
[306] A. Weil. Jacobi sums as "Grössencharaktere." *Trans. Amer. Math. Soc.*, 73:487–495, 1952.
[307] A. Weil. On algebraic groups and homogeneous spaces. *Amer. J. Math.*, 77:493–512, 1955.
[308] A. Weil. Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Ann.*, 168:149–156, 1967.
[309] A. Weil. *Dirichlet Series and Automorphic Forms*, volume 189 of *Lecture Notes in Mathematics*. Springer-Verlag, 1971.
[310] E. T. Whittaker and G. N. Watson. *A course of modern analysis*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1996. Reprint of the fourth (1927) edition.
[311] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.
[312] A. Wiles. The Birch and Swinnerton-Dyer conjecture. In *The millennium prize problems*, pages 31–41. Clay Math. Inst., Cambridge, MA, 2006.
[313] G. Wüstholz. Recent progress in transcendence theory. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 280–296. Springer, Berlin, 1984.
[314] G. Wüstholz. Multiplicity estimates on group varieties. *Ann. of Math. (2)*, 129(3):471–500, 1989.
[315] D. Zagier. Large integral points on elliptic curves. *Math. Comp.*, 48(177):425–436, 1987.
[316] H. G. Zimmer. On the difference of the Weil height and the Néron-Tate height. *Math. Z.*, 147(1):35–51, 1976.
[317] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math.*, 3:265–284, 1892.