MASTER'S THESIS

On the problem of the rank of the Mordell-Weil group

Author:
Rocío Sepúlveda-Manzo

Supervisor:
Héctor Pastén

A thesis submitted in fulfillment of the requirements for the degree of Master of Mathematics in the Faculty of Mathematics of Pontificia Universidad Católica de Chile.

Committee:
Daniel Barrera (Universidad de Santiago de Chile)
Ricardo Menares (Pontificia Universidad Católica de Chile)

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

April 24, 2025

Dedicado a mis abuelos Ciliano Manzo Fuentes y Noemí Maldonado Saavedra. También a mi madre Noemí del Carmen Manzo Maldonado.

CONTENTS

CHAPTER I
MAIN QUESTION

§1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ with minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and conductor N. By the Mordell–Weil theorem, the group of rational points $E(\mathbb{Q})$ is finitely generated and decomposes as

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r,$$

where $r := \operatorname{rank} E(\mathbb{Q}) < \infty$ is the ***rank*** of the elliptic curve E, and $E(\mathbb{Q})_{\mathrm{tors}}$ denotes its torsion subgroup. Furthermore, by the modularity theorem [**35**], there exists a non-constant morphism

$$\phi_E \colon X_0(N) \to E$$

defined over $\mathbb{Q}$, where $X_0(N)$ is the modular curve associated with the congruence subgroup $\Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$. This morphism is called a ***modular parametrization***. If it has minimal degree, we say that ϕ_E is minimal, and we denote its degree by $\deg \phi_E$.

The present thesis is concerned with the following question:

Question 1.1: Is the $\operatorname{rank} E(\mathbb{Q})$ bounded as E varies over all elliptic curves over $\mathbb{Q}$?

Question 1.1 was implicitly posed by Poincaré in 1901 [**23**, p. 173], even before it was known that $E(\mathbb{Q})$ is finitely generated. Several heuristics have been proposed to support the existence of such a bound [**3**, **22**, **24**, **25**, **26**, **33**]. Notice that if the rank is bounded, then $E(\mathbb{Q})$ has finitely many possibilities (up to isomorphism). A promising approach to addressing the main question is to consider the following conjecture by Watkins.

Conjeture 1 (Watkins, [32]): For every elliptic curve E over $\mathbb{Q}$ we have $\operatorname{rank} E(\mathbb{Q}) \leq v_2(\deg \phi_E)$.

However, our main result in this thesis is that the 2-adic valuation of modular degree is unbounded and, in fact, we show it can grow like the logarithm of the conductor.

Main Theorem: *Given an arbitrary elliptic curve E over $\mathbb{Q}$ with conductor N. Then there is a sequence of quadratic twists $E^{(D_n)}$ of E by fundamental (quadratic) discriminant D_n such that*

$$\log N_{E^{(D_n)}} \ll v_2(\deg \phi_{E^{(D_n)}}).$$

This result allows us to conclude that Watkins' conjecture *does not* imply the existence of a uniform bound to the rank. To prove the main theorem, we set up a family of twists of a fixed elliptic curve through the fundamental discriminants involved and use the arithmetic properties related to its invariants. Finally, we apply a tool from analytic number theory to establish an inequality between the 2-adic valuation of the modular degree and the logarithm of the conductor.

§2. Acknowledgements

The author would like to thank Héctor Pastén for his guidance throughout this thesis, and José Cuevas for providing valuable information references related to height theory.

Special thanks are also extended to the CIMPA School "Serre's Big Image Theorem for Galois Representations Associated to Elliptic Curves," the program Arithmetic and p-adic Geometry in Chile, and SaNTAS (Santiago Algebra & Number Theory Seminar) for offering the opportunity to present these results prior to publication and for the insightful discussions with participants and instructors, whose feedback contributed numerous ideas.

CHAPTER II
PRELIMINARIES

§1. Notations

Let us record the basic notation used throughout this thesis. If f and g are functions on $\mathbb{N}$, with f complex-valued and g positive real-valued, Landau's notation $f = O(g)$ means that there exists a constant $c > 0$ and an integer n_0 such that $|f(n)| \leq c \cdot g(n)$ for all $n \geq n_0$. This is equivalent to Vinogradov's notation $f \ll g$. The constant c in the previous definition is referred to as the ***implicit constant***.

We will denote by $(a, b) = 1$ to indicate that a and b are coprime. The p-adic valuation is denoted by v_p.

Further notation will be introduced as needed.

§2. Modular Curves

Let E be an elliptic curve over $\mathbb{Q}$ with conductor N, and let $\phi_E \colon X_0(N) \to E$ be the corresponding modular parametrization. Take a minimal Weierstrass equation for $E/\mathbb{Q}$ as in the introduction, and let

$$\omega_E = \frac{\mathrm{d}x}{2y + a_1 x + a_3}$$

be the ***Néron differential*** (It is unique up to sign). We have that the pull-back

$$\phi_E^* \omega_E = 2\pi i c_E f_E(z)\,\mathrm{d}z, \tag{2.1}$$

is a regular differential on $X_0(N)$, where f_E is a newform of weight 2 for $\Gamma_0(N)$, and $c_E \in \mathbb{Q}^*$ is the *Manin constant*. We assume that the signs of ϕ_E and ω_E are chosen such that $c_E > 0$.

Let us recall the following result due to B. Edixhoven about c_E:

Lemma 2: The Manin constant c_E is an integer.

Proof. See [11]. $\square$

For more results about the constant see Apendix 1.

The ***Faltings' height*** of E over $\mathbb{Q}$ is defined as a certain Arakelov degree, c.f. [6], §5, which in our case takes the simpler form, c.f. [27], §3.

$$h(E) = -\frac{1}{2}\log\left(\frac{i}{2}\int_{E(\mathbb{C})}\omega_E \wedge \overline{\omega}_E\right). \tag{2.2}$$

Let us recall the Ramanujan Δ-function

$$\Delta(\tau) = q\prod_{n=1}^{\infty}(1-q)^{24},$$

where $q = \exp(2\pi i\tau)$ is defined on the upper half-plane $\mathfrak{h} = \{\tau \in \mathbb{C} : \Im(\tau) > 0\}$.

For $E/\mathbb{Q}$ with discriminant Δ_E, we let $\tau_E \in \mathfrak{h}$ be the point in the fundamental domain of $SL_2(\mathbb{Z})$ acting on $\mathfrak{h}$ (see [10] for basic definitions) such that $j(\tau_E) = j_E$, the j-invariant of E.

Therefore, a more explicit formula to the height is the following:

Lemma 3: With the notation as above,

$$h(E) = \frac{1}{12}\left(\log|\Delta_E| - \log|\Delta(\tau_E)\Im(\tau_E)^6|\right) - \log(2\pi).$$

Proof. See [27], prop. 1.1. $\square$

The ***Petersson's norm*** of f relative to $\Gamma_0(N)$ is defined by

$$\|f\|_N := \left(\int_{X_0(N)}|f(z)|^2\,\mathrm{d}x\wedge\mathrm{d}y\right)^{1/2}, \qquad z = x+iy \in \mathfrak{h}. \tag{2.3}$$

Therefore, by integrating both sides of equation (2.1) using (2.2) and (2.3), we obtain

$$4\pi^2 c_E^2\,\|f\|_N^2 = \int_{X_0(N)}\phi_E^*\omega_E \wedge \overline{\phi_E^*\omega_E},$$

$$= \deg \phi_E \int_{E(\mathbb{C})} \omega_E \wedge \overline{\omega_E},$$
$$= \deg \phi_E \exp(-2h(E)).$$

This gives the following result:

Proposition 4: With the notation as above,

$$\deg \phi_E = 4\pi^2 c_E^2 \|f\|_N^2 \exp(2h(E)).$$

§3. Linnik's Theorem

A famous theorem of Dirichlet asserts that any arithmetic progression $a,\ a+b,\ a+2b,\ldots$, where $(a,b)=1$, contains infinitely many primes. However, this theorem does not provide information regarding the least prime that appears in the progression. For this, we use a theorem due to Linnik:

Theorem 5 (Linnik): Let $p_{a,b}$ be the smallest prime satisfying $p \equiv a \mod b$, where a and b are coprime integers. Then there exists an effectively computable absolute constant $L > 0$ such that

$$p_{a,b} \ll b^L.$$

To prove the theorem 5 one must study the zero-free region, the log-free zero-density estimate and the exceptional zero of the Dirichlet L-functions, the proof of which are covered in [15] without determining the constant L but this could have been computed. Here is a selected list of the Linnik constant produced by various researchers.

L	Name	Year
10000	Pan [21]	1957
777	Chen [16]	1965
80	Jutila [17]	1977
20	Graham [13]	1981
8	Wang [34]	1991
5.5	Heath-Brown [14]	1992
5.18	Xylouris [36]	2009

Table II.1: Estimates For Linnik's Constant

§4. Quadratic twists

For an elliptic curve E over $\mathbb{Q}$ with conductor N, and an integer $D \neq 1$, the ***quadratic twist*** of E by D is a non-isomorphic elliptic curve that is isomorphic to E over the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, where d is a square-free integer and $D = d$ if $d \equiv 1 \pmod 4$, and $D = 4d$ if $d \equiv 2$ or $3 \pmod 4$. We will refer to D as the ***fundamental discriminant***. The quadratic twist of E by D will be denoted by $E^{(D)}$ and its conductor by $N^{(D)}$.

Proposition 6: With the hypothesis of $(D, N) = 1$, we have $N^{(D)} = 2^a 3^b D^2 \cdot N$ where a, b are uniformed bounded integers.

Proof. By Proposition VIII.8.7 of [28], the elliptic curve E admits a Weierstrass equation of the form

$$E: \qquad y^2 = x^3 + Ax + B \tag{4.1}$$

with $A, B \in \mathbb{Z}[1/2, 1/3]$ and discriminant Δ, which is minimal at any prime $p \neq 2, 3$. Then, the quadratic twist $E^{(D)}$ is given by the following equation:

$$E^{(D)} : y^2 = x^3 + d^2Ax + d^3B$$

We claim that this equation remain minimal at p. First, notice that as (4.1) is minimal at p, we have that either $v_p(\Delta) < 12$ or $v_p(A) < 4$ (see Remark VII.1.1, [28]). The discriminant $\Delta^{(D)}$ of $E^{(D)}$ is $d^6\Delta$. And as Δ and d are prime to each other, we see that $v_p(\Delta) < 12$ implies $v_p(\Delta^{(D)}) < 12$ as well. If $v_p(\Delta) \geq 12$, then $p \mid N$ and $v_p(d) = 0$, so $v_p(d^2A) = v_p(A) < 4$.

We analyze the following cases:

- $\boxed{\text{Case } p \mid D\text{:}}$ Since $p \mid d$, the reduction of $E^{(D)}$ modulo p is the cuspidal curve $y^2 = x^3$, implying that $v_p(N^{(D)}) = 2$.

- $\boxed{\text{Case } p \mid N\text{:}}$ By definition, E has bad reduction at p, so $E^{(D)}$ does as well, since $p \mid \Delta^{(D)}$. Conversely, if $E^{(D)}$ has bad reduction at p, then E must also have bad reduction at p, given that $p \nmid d$, which implies $p \mid \Delta$.

Recall that E has additive reduction if and only if $p \mid A$ and $p \mid B$ (exercise VII.7.1 (b) (iii) of [28]). Since D is coprime to N, we have $p \nmid D$. Therefore, E has additive reduction if and only if $E^{(D)}$ does as well. Consequently, E and $E^{(D)}$ share the same type of bad reduction at p. Specifically, $v_p(N^{(D)}) = v_p(N)$.

In the cases $p = 2$ and $p = 3$ we can find a simple p-adic bound to $N^{(D)}$. By definition of conductor (cite silverman) we have $v_2(N^{(D)}) \leq 5$ and $v_3(N^{(D)}) \leq 3$. If we set $a := v_2(N^{(D)}/D^2N) = v_2(N^{(D)}) - 2v_2(D) - v_2(N)$ then we have $|a| \leq 5$. Similarly, for $p = 3$, we have $|b| \leq 3$. □

Proposition 7: *If two elliptic curves are quadratic twists of each other then they have the same j-invariant.*

Proof. See [28] prop. 1.4(b). □

CHAPTER III
ARITHMETIC RESULTS FOR QUADRATIC TWISTS

§1. Arithmetic of the twist under 2-adic valuation

The following results are based on Esparza-Lozano & Pasten [12], and this section is largely derived from that article.

Let E be an elliptic curve over $\mathbb{Q}$, let D be a fundamental discriminant, and let $E^{(D)}$ be the quadratic twist of E by D. Given elliptic curves E_1 and E_2 over $\mathbb{Q}$, we define

$$\delta(E_1, E_2) := \exp\left(2h(E_1) - 2h(E_2)\right).$$

Lemma 8 (Variation of $h(E)$ under quadratic twist): *The value $\delta(E^{(D)}, E)$ is a rational number satisfying: $|v_p(\delta(E^{(D)}, E))| = 1$ for every odd prime p dividing D, and $|v_2(\delta(E^{(D)}, E))| \leq 3$.*

Proof. We apply Lemma 3 to both E and $E^{(D)}$. Since E and $E^{(D)}$ have the same j-invariant, it follows that $\tau_E = \tau_{E^{(D)}}$. Therefore, $\delta(E, E^{(D)}) = |\Delta_E/\Delta_{E^{(D)}}|^{1/6}$.

By Proposition 2.4 of [20], we have the following:

1. For an odd prime p dividing the square-free d of the implicit quadratic extension:
   (a) If $\min\{3v_p(c_4(E)), 2v_p(c_6(E)), v_p(\Delta_E)\} < 6$, or if $p = 3$ and $v_p(c_6(E)) = 5$, then $v_p(\Delta_{E^{(D)}}/\Delta_E) = 6$.
   (b) Otherwise, $v_p(\Delta_{E^{(D)}}/\Delta_E) = -6$.
2. For $p = 2$:
   (a) If $d \equiv 1 \pmod 4$, then $v_2(\Delta_{E^{(D)}}/\Delta_E) = 0$.

(b) If $d \equiv 3 \pmod 4$, then $v_2(\Delta_{E^{(D)}}/\Delta_E) \in \{-12, 0, 12\}$.

(c) If $d \equiv 2 \pmod 4$, then $v_2(\Delta_{E^{(D)}}/\Delta_E) \in \{-18, -6, 6, 18\}$.

From these results, it follows that $(\Delta_{E^{(D)}}/\Delta_E)^{1/6}$ is a rational number, completing the proof. □

Let us introduce some notation for the following result by Delaunay [9] (allowing D and N to have common prime factors): We have

$$N^{(D)} = MD_1^2D_2^2 2^k \quad \text{and} \quad N = MD_2 2^\lambda,$$

where D_1 (resp. D_2) is the product of the odd primes p such that $p \mid D$ and $p \nmid N$ (resp. $p \mid D$ and $p \parallel N$), $\lambda = v_2(N)$, $k = v_2(N^{(D)})$ so that $\lambda \leq k$ and M, D_1, D_2 are odd. Then:

Lemma 9 (Variation of the Petersson norm under quadratic twist): *We have* $\|f_{E^{(D)}}\|^2_{N^{(D)}} / \|f_E\|^2_N \in \mathbb{Q}^\times$ *and*

$$v_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) + 1 \geq \sum_{p \mid D_1} v_2((p-1)(p+1-a_p(E))(p+1+a_p(E))).$$

Proof. The quadratic Dirichlet character attached to D has conductor $|D|$. By Theorem 1 in [9], and following its notation, we have

$$\begin{aligned} \|f_{E^{(D)}}\|^2_{N^{(D)}} = & \|f\|^2_N \cdot \frac{1}{D_1} \prod_{p \mid D_1} (p-1)(p+1-a_p(E))(p+1+a_p(E)) \\ & \times \frac{1}{D_2} \prod_{p \mid D_2} (p-1)(p+1) \\ & \times \begin{cases} 2^{k-3}(3-a_2(E))(3+a_2(E)) & \text{if } \lambda = 0,\ k \geq 4, \\ 2^{k-3} \times 3 & \text{if } \lambda = 1,\ k \neq \lambda, \\ 2^{k-\lambda} & \text{if } 2 \leq \lambda \leq k \text{ or if } \lambda = k = 1. \end{cases} \end{aligned}$$

Since D_1 and D_2 are odd, we analyze the integer factors: The first term directly contributes to the ratio. The second term has a positive contribution to the 2-adic valuation. And in the third term, the 2-adic valuation is at least -1.

This concludes the proof. □

CHAPTER IV
PROOF OF MAIN THEOREM

Let us fix an integer $\alpha \geq \max\{2, \log_2 N\}$. By Dirichlet's theorem on arithmetic progressions, there exists a prime of the form $q = 2^\alpha m + 1$ with m a positive integer such that $N < q$ so that $(q, N) = 1$ and $q \neq 2, 3$. Let now E be an elliptic curve over $\mathbb{Q}$ and let $D = q$ be a fundamental discriminant. By Lemma 9, we have

$$v_2\left(\frac{\|f_{E^{(q)}}\|^2_{N^{(q)}}}{\|f_E\|^2_N}\right) + 1 \geq v_2((q-1)(q+1-a_q(E))(q+1+a_q(E))).$$

Since $v_2(q-1) \geq \alpha$ and $\alpha - 1 \geq \frac{1}{2}\alpha$, we have

$$v_2(\|f_{E^{(q)}}\|^2_{N^{(q)}} \,/\, \|f_E\|^2_N) \gg \alpha. \tag{0.1}$$

Now, recall the formula for computing the modular degree in Proposition 4. Thus,

$$\frac{\deg \phi_{E^{(q)}}}{\deg \phi_E} = \frac{c^2_{E^{(q)}} \|f_{E^{(q)}}\|^2_{N^{(q)}}}{c^2_E \|f_E\|^2_N} \cdot \delta(E^{(q)}, E).$$

Therefore, using equation (0.1) above, by Lemma 2, and by Lemma 8, we conclude $v_2(\deg \phi_{E_D} / \deg \phi_E) \gg \alpha$.

On the other hand, by Proposition 6, $N^{(q)}$ is bounded by $2^a 3^b q^2 N$, so $\log N^{(q)} \ll \log q$ (recall that a and b are bounded). By Linnik's theorem, $q \ll 2^{\alpha L}$. Thus $\log N^{(q)} \ll \alpha$. Finally,

$$\log N^{(q)} \ll \alpha \ll v_2(\deg \phi_{E^{(q)}}).$$

APPENDIX

§1. Manin Constant (based on the introduction in [2])

Let E be an elliptic curve defined over the rational numbers $\mathbb{Q}$, and let N denote its conductor. As discussed in §2, the *Manin constant* c_E is the constant appearing in the relation

$$\phi_E^*\omega_E = 2\pi i c_E f(z)\,\mathrm{d}z.$$

It is known that c_E is an integer (lemma 2), and significant work has been done to restrict the primes that may divide c_E.

The Manin constant plays a crucial role in the Birch and Swinnerton-Dyer conjecture (see, e.g., [37], p. 130) and in the study of modular parametrizations (see [30, 29, 31]).

By the results of [4], E can be realized as a quotient of the modular Jacobian $J_0(N)$. After possibly replacing E by an isogenous curve, we may assume that the kernel of the map $J_0(N) \to E$ is connected. In this case, E is referred to as an ***optimal quotient*** of $J_0(N)$ (or a *strong Weil curve* in older terminology).

Manin made the following influential conjecture:

Conjeture 1 (Manin, cf. [18]): For any optimal elliptic curve E over $\mathbb{Q}$, the Manin constant c_E is equal to 1.

The conjecture is proven in the case when E has semi-stable reduction (i.e., N is square-free). First, we mention previous results which cover many special cases:

Theorem 2 (Mazur, cf. [19]): *For an odd prime p. We have if $p \mid c_E$, then $p^2 \mid 4N$.*

The following results refine the above result at $p = 2$.

Theorem 3 (Abbes-Ullmo, cf. [1]): *If $p \mid c_E$, then $p \mid N$.*

Theorem 4 (Agashe-Ribet-Stein, cf. [2]): *If $p \mid c_E$, then $p^2 \mid N$ or $p \mid m_E$.*

The following result contains all cases of semistable curves

> ***Theorem 5 (Česnavičius, cf. [5]):*** *The conjecture 1 holds in the case when E is semistable.*

The following theorem verifies Manin's conjecture in a wide range of cases:

Theorem 6 (Cremona, cf. [8]): *If E is an optimal elliptic curve over $\mathbb{Q}$ with conductor at most 130000, then the Manin constant c_E satisfies $c_E = 1$.*

BIBLIOGRAPHY

1. Abbes, A. & Ullmo, E. À propos de la conjecture de Manin pour les courbes elliptiques modulaires. *Compositio Mathematica* **103,** 269–286 (1996).
2. Agashe, A., Ribet, K. A. & Stein, W. A. The Manin Constant. *Pure and Applied Mathematics Quarterly* **2,** 617–636. https://wstein.org/papers/ars-manin/ (2006).
3. Bhargava, M., Kane, D., Lenstra, H., Poonen, B. & Rains, E. Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. *Cambridge Journal of Mathematics* **3,** 275–321. doi:10.4310/CJM.2015.v3.n3.a1 (2013).
4. Breuil, C., Conrad, B., Diamond, F. & Taylor, R. On the Modularity of Elliptic Curves Over Q: Wild 3-Adic Exercises. *Journal of the American Mathematical Society* **14.** doi:10.1090/S0894-0347-01-00370-8 (Oct. 2001).
5. Česnavičius, K. The Manin constant in the semistable case. *Compositio Mathematica* **154,** 1889–1920. doi:10.1112/S0010437X18007273 (2018).
6. Chai, C.-L. *Siegel Moduli Schemes and Their Compactifications over* $\mathbb{C}$ in *Arithmetic Geometry* (eds Cornell, G. & Silverman, J. H.) (Springer-Verlag, 1986), 231–252.
7. (eds Cornell, G. & Silverman, J. H.) *Arithmetic Geometry* (Springer-Verlag, 1986).
8. Cremona, J. E. *Algorithms for Modular Elliptic Curves* Second. http://www.maths.nott.ac.uk/personal/jec/book/ (Cambridge University Press, 1997).
9. Delaunay, C. Computing modular degrees using L-functions. *Journal de Théorie des Nombres de Bordeaux* **15,** 673–682 (2003).
10. Diamond, F. & Shurman, J. *A First Course in Modular Forms* ISBN: 9780387272269 (Springer New York, 2006).
11. Edixhoven, B. in *Arithmetic Algebraic Geometry* (eds van der Geer, G., Oort, F. & Steenbrink, J.) 25–39 (Birkhäuser Boston, 1991). doi:10.1007/978-1-4612-0457-2_3.

12. Esparza-Lozano, J. A. & Pasten, H. A conjecture of Watkins for quadratics twist. *Proceedings of the American Mathematical Society* **152,** 2381–2385 (2021).
13. Graham, S. On Linnik's constant. *Acta Arithmetica* **39,** 163–179 (1981).
14. Heath-Brown, D. R. Zero-Free Regions for Dirichlet L-Functions, and the Least Prime in an Arithmetic Progression. *Proceedings of the London Mathematical Society* **s3-64,** 265–338. doi:10.1112/plms/s3-64.2.265 (1992).
15. Iwaniec, H. & Kowalski, E. *Analytic Number Theory* (American Mathematical Society, 2004).
16. Jing-run, C. On the least prime in an arithmetical progression. *Scientia Sinica* **14,** 1868–1871 (1965).
17. Jutila, M. On Linnik's constant. *Mathematica Scandinavica* **41,** 45–62 (1977).
18. Manin, Y. I. Parabolic points and zeta-functions of modular curves. *Mathematics of the USSR* **1,** 19–64. doi:10.1070/IM1972v006n01ABEH001867 (1972).
19. Mazur, B. & Goldfeld, D. Rational isogenies of prime degree. *Inventiones Mathematicae* **44,** 129–162. doi:10.1007/BF01390348 (1978).
20. Pal, V. & Agashe, A. Periods of quadratic twist of elliptic curves. *Proceedings of the American Mathematical Society* **140,** 1513–1525. doi:10.1090/S0002-9939-2011-11014-1 (2012).
21. Pan, C. D. On the least prime in an arithmetical progression. *Science Record. New Series* **1,** 311–313 (1957).
22. Park, J., Poonen, B., Voight, J. & Wood, M. M. A heuristic for boundedness of ranks of elliptic curves. *Journal of the European Mathematical Society.* doi:10.4171/JEMS/893 (2019).
23. Poincaré, H. Sur les propriétés arithmétiques des courbes algébriques. *Journal de Mathématiques Pures et Appliquées* **7,** 161–234 (1901).
24. Poonen, B. Heuristics for the arithmetic of elliptic curves, 399–414. doi:10.1142/9789813272880_0060 (2018).
25. Poonen, B. & Rains, E. Random maximal isotropic subspaces and Selmer groups. *Journal of the American Mathematical Society* **25,** 245–269. doi:10.1090/s0894-0347-2011-00710-8 (2012).
26. Rubin, K. & Silverberg, A. Ranks of elliptic curves in families of quadratic twists. *Experimental Mathematics* **9,** 583–590. doi:10.1080/10586458.2000.10504661 (2000).
27. Silverman, J. H. *Heights and Elliptic Curves* in *Arithmetic Geometry* (eds Cornell, G. & Silverman, J. H.) (Springer-Verlag, 1986), 253–265.
28. Silverman, J. H. *The Arithmetic of Elliptic Curves* (Springer Science Business Media, 2009).

29. Stein, W. & Watkins, M. Modular parametrizations of Neumann-Setzer elliptic curves. *International Mathematics Research Notices* **2004,** 1395–1405. doi:10.1155/S1073792804133916 (2004).

30. Stevens, G. Stickelberger elements and modular parametrizations of elliptic curves. *Inventiones mathematicae* **98,** 75–106. doi:10.1007/BF01388845 (1989).

31. Vatsal, V. Multiplicative subgroups of J0(N) and applications to elliptic curves. *Journal of the Institute of Mathematics of Jussieu* **4,** 281–316. doi:10.1017/S147474800500006X (Apr. 2005).

32. Watkins, M. Computing the modular degree of an elliptic curve. *Experimental Mathematics* **11,** 487–502. doi:10.1080/10586458.2002.10504701 (2002).

33. Watkins, M. *et al.* Ranks of quadratic twists of elliptic curves. *Publications mathématiques de Besançon,* 63–98. doi:10.5802/pmb.9 (2014).

34. Wei, W. On the least prime in an arithmetic progression. *Acta Mathematica Sinica* **7,** 279–288. doi:10.1007/BF02583005 (1991).

35. Wiles, A. Modular Elliptic Curves and Fermat's Last Theorem. *Annals of Mathematics* **141,** 443–551 (1995).

36. Xylouris, T. On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions. *Acta Arithmetica* **150,** 65–91 (2011).

37. Zagier, B. H. G. D. B. Heegner points and derivatives of L-series. *Inventiones Mathematicae* **84,** 225–320. doi:10.1007/BF01388809 (1986).