WIKIPEDIA
The Free Encyclopedia

Birch and Swinnerton-Dyer conjecture

In mathematics, the **Birch and Swinnerton-Dyer conjecture** (often called the **Birch–Swinnerton-Dyer conjecture**) describes the set of rational solutions to equations defining an elliptic curve. It is an open problem in the field of number theory and is widely recognized as one of the most challenging mathematical problems. It is named after mathematicians Bryan John Birch and Peter Swinnerton-Dyer, who developed the conjecture during the first half of the 1960s with the help of machine computation. Only special cases of the conjecture have been proven.

The modern formulation of the conjecture relates to arithmetic data associated with an elliptic curve E over a number field K to the behaviour of the Hasse–Weil L-function $L(E, s)$ of E at $s = 1$. More specifically, it is conjectured that the rank of the abelian group $E(K)$ of points of E is the order of the zero of $L(E, s)$ at $s = 1$. The first non-zero coefficient in the Taylor expansion of $L(E, s)$ at $s = 1$ is given by more refined arithmetic data attached to E over K (Wiles 2006).

The conjecture was chosen as one of the seven Millennium Prize Problems listed by the Clay Mathematics Institute, which has offered a $1,000,000 prize for the first correct proof.[1]

Background

Mordell (1922) proved Mordell's theorem: the group of rational points on an elliptic curve has a finite basis. This means that for any elliptic curve there is a finite subset of the rational points on the curve, from which all further rational points may be generated.

If the number of rational points on a curve is infinite then some point in a finite basis must have infinite order. The number of *independent* basis points with infinite order is called the rank of the curve, and is an important invariant property of an elliptic curve.

If the rank of an elliptic curve is 0, then the curve has only a finite number of rational points. On the other hand, if the rank of the curve is greater than 0, then the curve has an infinite number of rational points.

Although Mordell's theorem shows that the rank of an elliptic curve is always finite, it does not give an effective method for calculating the rank of every curve. The rank of certain elliptic curves can be calculated using numerical methods but (in the current state of knowledge) it is unknown if these methods handle all curves.

An L-function $\boldsymbol{L(E, s)}$ can be defined for an elliptic curve E by constructing an Euler product from the number of points on the curve modulo each prime p. This L-function is analogous to the Riemann zeta function and the Dirichlet L-series that is defined for a binary quadratic form. It is a special case of a Hasse–Weil L-function.

The natural definition of $L(E, s)$ only converges for values of s in the complex plane with $\mathrm{Re}(s) > 3/2$. Helmut Hasse conjectured that $L(E, s)$ could be extended by analytic continuation to the whole complex plane. This conjecture was first proved by Deuring (1941) for elliptic curves with complex multiplication. It was subsequently shown to be true for all elliptic curves over $\mathbb{Q}$, as a consequence of the modularity theorem in 2001.

Finding rational points on a general elliptic curve is a difficult problem. Finding the points on an elliptic curve modulo a given prime *p* is conceptually straightforward, as there are only a finite number of possibilities to check. However, for large primes it is computationally intensive.

History

In the early 1960s Peter Swinnerton-Dyer used the EDSAC-2 computer at the University of Cambridge Computer Laboratory to calculate the number of points modulo *p* (denoted by N_p) for a large number of primes *p* on elliptic curves whose rank was known. From these numerical results Birch & Swinnerton-Dyer (1965) conjectured that N_p for a curve *E* with rank *r* obeys an asymptotic law

$$\prod_{p\leq x} \frac{N_p}{p} \approx C \log(x)^r \text{ as } x \to \infty$$

where *C* is a constant.

Initially, this was based on somewhat tenuous trends in graphical plots; this induced a measure of skepticism in J. W. S. Cassels (Birch's Ph.D. advisor).[2] Over time the numerical evidence stacked up.

This in turn led them to make a general conjecture about the behavior of a curve's L-function *L*(*E*, *s*) at *s* = 1, namely that it would have a zero of order *r* at this point. This was a far-sighted conjecture for the time, given that the analytic continuation of *L*(*E*, *s*) was only established for curves with complex multiplication, which were also the main source of numerical examples. (NB that the reciprocal of the L-function is from some points of view a more natural object of study; on occasion, this means that one should consider poles rather than zeroes.)

The conjecture was subsequently extended to include the prediction of the precise leading Taylor coefficient of the *L*-function at *s* = 1. It is conjecturally given by[3]

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\#\mathrm{Sha}(E)\Omega_E R_E \prod_{p|N} c_p}{(\#E_{\mathrm{tor}})^2}$$

where the quantities on the right-hand side are invariants of the curve, studied by Cassels, Tate, Shafarevich and others (Wiles 2006):

$\#E_{\mathrm{tor}}$ is the order of the torsion group,

$\#\mathrm{Sha}(E)$ =#Ш(E) is the order of the Tate–Shafarevich group,

Ω_E is the real period of *E* multiplied by the number of connected components of *E*,

R_E is the regulator of *E* which is defined via the canonical heights of a basis of rational points,

c_p is the Tamagawa number of E at a prime p dividing the conductor N of E. It can be found by Tate's algorithm.

At the time of the inception of the conjecture little was known, not even the well-definedness of the left side (referred to as analytic) or the right side (referred to as algebraic) of this equation. John Tate expressed this in 1974 in a famous quote.[4]:198

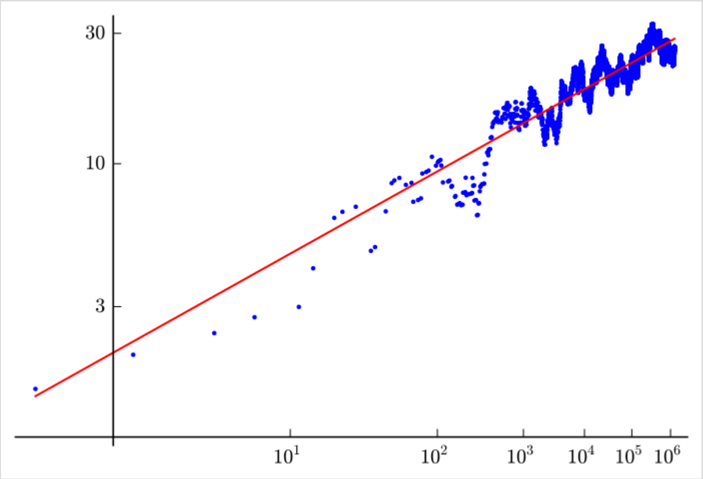
> This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group Ш which is not known to be finite!

By the modularity theorem proved in 2001 for elliptic curves over $\mathbb{Q}$ the left side is now known to be well-defined and the finiteness of Ш(E) is known when additionally the analytic rank is at most 1, i.e., if $L(E,s)$ vanishes at most to order 1 at $s=1$. Both parts remain open.

Current status

The Birch and Swinnerton-Dyer conjecture has been proved only in special cases:

1. Coates & Wiles (1977) proved that if *E* is a curve over a number field *F* with complex multiplication by an imaginary quadratic field *K* of class number 1, *F* = *K* or $\mathbb{Q}$, and *L*(*E*, 1) is not 0 then *E*(*F*) is a finite group. This was extended to the case where *F* is any finite abelian extension of *K* by Arthaud (1978).
2. Gross & Zagier (1986) showed that if a modular elliptic curve has a first-order zero at *s* = 1 then it has a rational point of infinite order; see Gross–Zagier theorem.
3. Kolyvagin (1989) showed that a modular elliptic curve *E* for which *L*(*E*, 1) is not zero has rank 0, and a modular elliptic curve *E* for which *L*(*E*, 1) has a first-order zero at *s* = 1 has rank 1.
4. Rubin (1991) showed that for elliptic curves defined over an imaginary quadratic field *K* with complex multiplication by *K*, if the *L*-series of the elliptic curve was not zero at *s* = 1, then the *p*-part of the Tate–Shafarevich group had the order predicted by the Birch and Swinnerton-Dyer conjecture, for all primes *p* > 7.
5. Breuil et al. (2001), extending work of Wiles (1995), proved that all elliptic curves defined over the rational numbers are modular, which extends results #2 and #3 to all elliptic curves over the rationals, and shows that the *L*-functions of all elliptic curves over $\mathbb{Q}$ are defined at *s* = 1.



A plot, in blue, of $\prod_{p\leq X}\frac{N_p}{p}$ for the curve $y^2 = x^3 - 5x$ as *X* varies over the first 100000 primes. The *X*-axis is in log(log) scale -*X* is drawn at distance proportional to $\log(\log(X))$ from 0- and the *Y*-axis is in a logarithmic scale, so the conjecture predicts that the data should tend to a line of slope equal to the rank of the curve, which is 1 in this case -that is, the quotient $\frac{\log\left(\prod_{p\leq X}\frac{N_p}{p}\right)}{\log C + r\log(\log X))} \to 1$ as $X\to\infty$, with *C*, *r* as in the text. For comparison, a line of slope 1 in (log(log),log)-scale -that is, with equation $\log y = a + \log(\log x)$- is drawn in red in the plot.

6. Bhargava & Shankar (2015) proved that the average rank of the Mordell–Weil group of an elliptic curve over $\mathbb{Q}$ is bounded above by 7/6. Combining this with the p-parity theorem of Nekovář (2009) and Dokchitser & Dokchitser (2010) and with the proof of the main conjecture of Iwasawa theory for GL(2) by Skinner & Urban (2014), they conclude that a positive proportion of elliptic curves over $\mathbb{Q}$ have analytic rank zero, and hence, by Kolyvagin (1989), satisfy the Birch and Swinnerton-Dyer conjecture.

There are currently no proofs involving curves with a rank greater than 1.

There is extensive numerical evidence for the truth of the conjecture.[5]

Consequences

Much like the Riemann hypothesis, this conjecture has multiple consequences, including the following two:

- Let n be an odd square-free integer. Assuming the Birch and Swinnerton-Dyer conjecture, n is the area of a right triangle with rational side lengths (a congruent number) if and only if the number of triplets of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is twice the number of triplets satisfying $2x^2 + y^2 + 32z^2 = n$. This statement, due to Tunnell's theorem (Tunnell 1983), is related to the fact that *n* is a congruent number if and only if the elliptic curve $y^2 = x^3 - n^2x$ has a rational point of infinite order (thus, under the Birch and Swinnerton-Dyer conjecture, its L-function has a zero at 1). The interest in this statement is that the condition is easily verified.[6]
- In a different direction, certain analytic methods allow for an estimation of the order of zero in the center of the critical strip of families of *L*-functions. Admitting the BSD conjecture, these estimations correspond to information about the rank of families of elliptic curves in question. For example: suppose the generalized Riemann hypothesis and the BSD conjecture, the average rank of curves given by $y^2 = x^3 + ax + b$ is smaller than 2.[7]
- Because of the existence of the functional equation of the *L*-function of an elliptic curve, BSD allows us to calculate the parity of the rank of an elliptic curve. This is a conjecture in its own right called the parity conjecture, and it relates the parity of the rank of an elliptic curve to its global root number. This leads to many explicit arithmetic phenomena which are yet to be proved unconditionally. For instance:
    - Every positive integer $n \equiv 5, 6 \text{ or } 7 \pmod 8$ is a congruent number.
    - The elliptic curve given by $y^2 = x^3 + ax + b$ where $a \equiv b \pmod 2$ has infinitely many solutions over $\mathbb{Q}(\zeta_8)$.
    - Every positive rational number d can be written in the form $d = s^2(t^3 - 91t - 182)$ for s and t in $\mathbb{Q}$.
    - For every rational number t, the elliptic curve given by $y^2 = x(x^2 - 49(1 + t^4)^2)$ has rank at least 1.
    - There are many more examples for elliptic curves over number fields.

Generalizations

There is a version of this conjecture for general abelian varieties over number fields. A version for abelian varieties over $\mathbb{Q}$ is the following:[8]:462

$$\lim_{s\to 1}\frac{L(A/\mathbb{Q},s)}{(s-1)^r}=\frac{\#\mathrm{Sha}(A)\Omega_A R_A\prod_{p|N}c_p}{\#A(\mathbb{Q})_{\mathrm{tors}}\cdot\#\hat{A}(\mathbb{Q})_{\mathrm{tors}}}.$$

All of the terms have the same meaning as for elliptic curves, except that the square of the order of the torsion needs to be replaced by the product $\#A(\mathbb{Q})_{\mathrm{tors}}\cdot\#\hat{A}(\mathbb{Q})_{\mathrm{tors}}$ involving the dual abelian variety $\hat{A}$. Elliptic curves as 1-dimensional abelian varieties are their own duals, i.e. $\hat{E}=E$, which simplifies the statement of the BSD conjecture. The regulator R_A needs to be understood for the pairing between a basis for the free parts of $A(\mathbb{Q})$ and $\hat{A}(\mathbb{Q})$ relative to the Poincare bundle on the product $A\times\hat{A}$.

The rank-one Birch-Swinnerton-Dyer conjecture for modular elliptic curves and modular abelian varieties of GL(2)-type over totally real number fields was proved by Shou-Wu Zhang in 2001.[9][10]

Another generalization is given by the Bloch-Kato conjecture.[11]

Notes

1. Birch and Swinnerton-Dyer Conjecture (http://www.claymath.org/millennium-problems/birch-and-swinnerton-dyer-conjecture) at Clay Mathematics Institute
2. Stewart, Ian (2013), *Visions of Infinity: The Great Mathematical Problems* (https://books.google.com/books?id=dzdSy3diraUC&pg=PA253), Basic Books, p. 253, ISBN 9780465022403, "Cassels was highly skeptical at first".
3. Cremona, John (2011). "Numerical evidence for the Birch and Swinnerton-Dyer Conjecture" (https://people.maths.bris.ac.uk/~matyd/BSD2011/bsd2011-Cremona.pdf) (PDF). *Talk at the BSD 50th Anniversary Conference, May 2011.*, page 50
4. Tate, John T. (1974). "The arithmetic of elliptic curves" (https://eudml.org/doc/142261). *Invent Math*. **23** (3–4): 179–206. Bibcode:1974InMat..23..179T (https://ui.adsabs.harvard.edu/abs/1974InMat..23..179T). doi:10.1007/BF01389745 (https://doi.org/10.1007%2FBF01389745)., page 198
5. Cremona, John (2011). "Numerical evidence for the Birch and Swinnerton-Dyer Conjecture" (https://people.maths.bris.ac.uk/~matyd/BSD2011/bsd2011-Cremona.pdf) (PDF). *Talk at the BSD 50th Anniversary Conference, May 2011*.
6. Koblitz, Neal (1993). *Introduction to Elliptic Curves and Modular Forms*. Graduate Texts in Mathematics. Vol. 97 (2nd ed.). Springer-Verlag. ISBN 0-387-97966-2.
7. Heath-Brown, D. R. (2004). "The Average Analytic Rank of Elliptic Curves". *Duke Mathematical Journal*. **122** (3): 591–623. arXiv:math/0305114 (https://arxiv.org/abs/math/0305114). doi:10.1215/S0012-7094-04-12235-3 (https://doi.org/10.1215%2FS0012-7094-04-12235-3). MR 2057019 (https://mathscinet.ams.org/mathscinet-getitem?mr=2057019). S2CID 15216987 (https://api.semanticscholar.org/CorpusID:15216987).
8. Hindry, Marc; Silverman, Joseph H. (2000). *Diophantine Geometry: An Introduction* (https://link.springer.com/book/10.1007/978-1-4612-1210-2). Graduate Texts in Mathematics. Vol. 201. New York, NY: Springer. p. 462. doi:10.1007/978-1-4612-1210-2 (https://doi.org/10.1007%2F978-1-4612-1210-2). ISBN 978-0-387-98975-4.
9. Zhang, Wei (2013). "The Birch–Swinnerton-Dyer conjecture and Heegner points: a survey" (https://doi.org/10.4310%2FCDM.2013.v2013.n1.a3). *Current Developments in Mathematics*. **2013**: 169–203. doi:10.4310/CDM.2013.v2013.n1.a3 (https://doi.org/10.4310%2FCDM.2013.v2013.n1.a3)..

10. Leong, Y. K. (July–December 2018). "Shou-Wu Zhang: Number Theory and Arithmetic Algebraic Geometry" (https://ims.nus.edu.sg/wp-content/uploads/2020/05/imprints-32-2018.pdf) (PDF). *Imprints*. No. 32. The Institute for Mathematical Sciences, National University of Singapore. pp. 32–36. Retrieved 5 May 2019.
11. Kings, Guido (2003). "The Bloch–Kato conjecture on special values of *L*-functions. A survey of known results" (http://jtnb.cedram.org/item?id=JTNB_2003__15_1_179_0). *Journal de théorie des nombres de Bordeaux*. **15** (1): 179–198. doi:10.5802/jtnb.396 (https://doi.org/10.5802%2Fjtnb.396). ISSN 1246-7405 (https://search.worldcat.org/issn/1246-7405). MR 2019010 (https://mathscinet.ams.org/mathscinet-getitem?mr=2019010).

References

- Arthaud, Nicole (1978). "On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication". *Compositio Mathematica*. **37** (2): 209–232. MR 0504632 (https://mathscinet.ams.org/mathscinet-getitem?mr=0504632).
- Bhargava, Manjul; Shankar, Arul (2015). "Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0". *Annals of Mathematics*. **181** (2): 587–621. arXiv:1007.0052 (https://arxiv.org/abs/1007.0052). doi:10.4007/annals.2015.181.2.4 (https://doi.org/10.4007%2Fannals.2015.181.2.4). S2CID 1456959 (https://api.semanticscholar.org/CorpusID:1456959).
- Birch, Bryan; Swinnerton-Dyer, Peter (1965). "Notes on Elliptic Curves (II)". *J. Reine Angew. Math.* **165** (218): 79–108. doi:10.1515/crll.1965.218.79 (https://doi.org/10.1515%2Fcrll.1965.218.79). S2CID 122531425 (https://api.semanticscholar.org/CorpusID:122531425).
- Breuil, Christophe; Conrad, Brian; Diamond, Fred; Taylor, Richard (2001). "On the Modularity of Elliptic Curves over Q: Wild 3-Adic Exercises" (https://doi.org/10.1090%2FS0894-0347-01-00370-8). *Journal of the American Mathematical Society*. **14** (4): 843–939. doi:10.1090/S0894-0347-01-00370-8 (https://doi.org/10.1090%2FS0894-0347-01-00370-8).
- Coates, J.H.; Greenberg, R.; Ribet, K.A.; Rubin, K. (1999). *Arithmetic Theory of Elliptic Curves*. Lecture Notes in Mathematics. Vol. 1716. Springer-Verlag. ISBN 3-540-66546-3.
- Coates, J.; Wiles, A. (1977). "On the conjecture of Birch and Swinnerton-Dyer". *Inventiones Mathematicae*. **39** (3): 223–251. Bibcode:1977InMat..39..223C (https://ui.adsabs.harvard.edu/abs/1977InMat..39..223C). doi:10.1007/BF01402975 (https://doi.org/10.1007%2FBF01402975). S2CID 189832636 (https://api.semanticscholar.org/CorpusID:189832636). Zbl 0359.14009 (https://zbmath.org/?format=complete&q=an:0359.14009).
- Deuring, Max (1941). "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper". *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*. **14** (1): 197–272. doi:10.1007/BF02940746 (https://doi.org/10.1007%2FBF02940746). S2CID 124821516 (https://api.semanticscholar.org/CorpusID:124821516).
- Dokchitser, Tim; Dokchitser, Vladimir (2010). "On the Birch–Swinnerton-Dyer quotients modulo squares". *Annals of Mathematics*. **172** (1): 567–596. arXiv:math/0610290 (https://arxiv.org/abs/math/0610290). doi:10.4007/annals.2010.172.567 (https://doi.org/10.4007%2Fannals.2010.172.567). MR 2680426 (https://mathscinet.ams.org/mathscinet-getitem?mr=2680426). S2CID 9479748 (https://api.semanticscholar.org/CorpusID:9479748).
- Gross, Benedict H.; Zagier, Don B. (1986). "Heegner points and derivatives of L-series". *Inventiones Mathematicae*. **84** (2): 225–320. Bibcode:1986InMat..84..225G (https://ui.adsabs.harvard.edu/abs/1986InMat..84..225G). doi:10.1007/BF01388809 (https://doi.org/10.1007%2FBF01388809). MR 0833192 (https://mathscinet.ams.org/mathscinet-getitem?mr=0833192). S2CID 125716869 (https://api.semanticscholar.org/CorpusID:125716869).
- Kolyvagin, Victor (1989). "Finiteness of $E(Q)$ and $X(E, Q)$ for a class of Weil curves". *Math. USSR Izv*. **32** (3): 523–541. Bibcode:1989IzMat..32..523K (https://ui.adsabs.harvard.edu/abs/1989IzMat..32..523K). doi:10.1070/im1989v032n03abeh000779 (https://doi.org/10.1070%2Fim1989v032n03abeh000779).

- Mordell, L. J. (1922). "On the rational solutions of the indeterminate equations of the third and fourth degrees" (https://archive.org/details/proceedingscambr21camb/page/178/mode/2up). *Mathematical Proceedings of the Cambridge Philosophical Society*. **21**: 179–192.
- Nekovář, Jan (2009). "On the parity of ranks of Selmer groups IV" (https://doi.org/10.1112%2FS0010437X09003959). *Compositio Mathematica*. **145** (6): 1351–1359. doi:10.1112/S0010437X09003959 (https://doi.org/10.1112%2FS0010437X09003959).
- Rubin, Karl (1991). "The 'main conjectures' of Iwasawa theory for imaginary quadratic fields". *Inventiones Mathematicae*. **103** (1): 25–68. Bibcode:1991InMat.103...25R (https://ui.adsabs.harvard.edu/abs/1991InMat.103...25R). doi:10.1007/BF01239508 (https://doi.org/10.1007%2FBF01239508). S2CID 120179735 (https://api.semanticscholar.org/CorpusID:120179735). Zbl 0737.11030 (https://zbmath.org/?format=complete&q=an:0737.11030).
- Skinner, Christopher; Urban, Éric (2014). "The Iwasawa main conjectures for GL_2". *Inventiones Mathematicae*. **195** (1): 1–277. Bibcode:2014InMat.195....1S (https://ui.adsabs.harvard.edu/abs/2014InMat.195....1S). CiteSeerX 10.1.1.363.2008 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.363.2008). doi:10.1007/s00222-013-0448-1 (https://doi.org/10.1007%2Fs00222-013-0448-1). S2CID 120848645 (https://api.semanticscholar.org/CorpusID:120848645).
- Tunnell, Jerrold B. (1983). "A classical Diophantine problem and modular forms of weight 3/2" (http://dml.cz/bitstream/handle/10338.dmlcz/137483/ActaOstrav_14-2006-1_8.pdf) (PDF). *Inventiones Mathematicae*. **72** (2): 323–334. Bibcode:1983InMat..72..323T (https://ui.adsabs.harvard.edu/abs/1983InMat..72..323T). doi:10.1007/BF01389327 (https://doi.org/10.1007%2FBF01389327). hdl:10338.dmlcz/137483 (https://hdl.handle.net/10338.dmlcz%2F137483). S2CID 121099824 (https://api.semanticscholar.org/CorpusID:121099824). Zbl 0515.10013 (https://zbmath.org/?format=complete&q=an:0515.10013).
- Wiles, Andrew (1995). "Modular elliptic curves and Fermat's last theorem". *Annals of Mathematics*. Second Series. **141** (3): 443–551. doi:10.2307/2118559 (https://doi.org/10.2307%2F2118559). ISSN 0003-486X (https://search.worldcat.org/issn/0003-486X). JSTOR 2118559 (https://www.jstor.org/stable/2118559). MR 1333035 (https://mathscinet.ams.org/mathscinet-getitem?mr=1333035).
- Wiles, Andrew (2006). "The Birch and Swinnerton-Dyer conjecture" (https://web.archive.org/web/20180329033023/http://www.claymath.org/sites/default/files/birchswin.pdf) (PDF). In Carlson, James; Jaffe, Arthur; Wiles, Andrew (eds.). *The Millennium prize problems*. American Mathematical Society. pp. 31–44. ISBN 978-0-8218-3679-8. MR 2238272 (https://mathscinet.ams.org/mathscinet-getitem?mr=2238272). Archived from the original (http://www.claymath.org/sites/default/files/birchswin.pdf) (PDF) on 29 March 2018. Retrieved 16 December 2013.

External links

- Weisstein, Eric W. "Swinnerton-Dyer Conjecture" (https://mathworld.wolfram.com/Swinnerton-DyerConjecture.html). *MathWorld*.
- "Birch and Swinnerton-Dyer Conjecture" (https://planetmath.org/BirchAndSwinnertonDyerConjecture). *PlanetMath*.
- The Birch and Swinnerton-Dyer Conjecture (https://issuu.com/thedeltaepsilon/docs/de1): An Interview with Professor Henri Darmon by Agnes F. Beaudry
- *What is the Birch and Swinnerton-Dyer Conjecture?* (https://www.youtube.com/watch?v=2gbQWIzb6Dg&t=3s) lecture by Manjul Bhargava (September 2016) given during the Clay Research Conference held at the University of Oxford