Integer points on an elliptic curve

Bogdan Grechuk • 27 Jul 2026

This is the third post in a series begun here and continued here. The series presents one striking and comparatively accessible theorem associated with each of the 2026 Fields Medalists and the 2026 Abacus Medalist. This post concerns Fields Medalist Jacob Tsimerman and a basic quantitative question about elliptic curves: how many integer points can such a curve have?

Elliptic curves have appeared several times on this blog, for example here and here. In this post, an elliptic curve E is given by an integral short Weierstrass equation

$$y^2 = x^3 + ax + b, \tag{1}$$

where $a, b \in \mathbb{Z}$ and

$$\Delta_E = -16\big(4a^3 + 27b^2\big) \neq 0.$$

The condition $\Delta_E \neq 0$ ensures that the curve is nonsingular. We also assume that the model is minimal in the following elementary sense: there is no prime p for which both $p^4 \mid a$ and $p^6 \mid b$. Its naive height is

$$H(E) = \max\{4|a|^3,\, 27b^2\}.$$

We are interested in the number

$$N_E = \#\big\{(x, y) \in \mathbb{Z}^2 : y^2 = x^3 + ax + b\big\}$$

of integer points on E. A fundamental theorem of Siegel (Siegel 1929) states that N_E is finite. Siegel's theorem, however, does not by itself provide a uniform bound for N_E in terms of a simple invariant such as the discriminant.

In 1992, Schmidt (Schmidt 1992) proved that, for every $\epsilon > 0$,

$$N_E \leq C_\epsilon |\Delta_E|^{1/2+\epsilon},$$

where C_ϵ depends only on ϵ. Helfgott and Venkatesh (Helfgott and Venkatesh 2006) substantially improved this result in 2006, showing that

$$N_E \leq C_\epsilon |\Delta_E|^{\beta+\epsilon},$$

where

$$\beta = \frac{4\sqrt{3}\log(2+\sqrt{3}) - 6\log 2 - 3\log 3}{12\log 2} = 0.2007\ldots.$$

Thus the number of integer points grows much more slowly than the square root of the discriminant.

This estimate remained the strongest known general bound for more than a decade. In 2020, Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, and Zhao (Bhargava et al. 2020) nearly halved the exponent.

Theorem 1 *For every $\epsilon > 0$, there exists a constant $C_\epsilon < \infty$ such that every elliptic curve E as above satisfies*

$$N_E \leq C_\epsilon |\Delta_E|^{\alpha+\epsilon},$$

where $\alpha = 0.1117\ldots$ is an explicit constant.

In other words, although an elliptic curve may have many integer points, their number is severely constrained by the arithmetic complexity of the curve. The theorem gives a uniform bound valid for every elliptic curve and improves the previously best exponent from approximately 0.2007 to approximately 0.1117.

References

Bhargava, Manjul, Arul Shankar, Takashi Taniguchi, Frank Thorne, Jacob Tsimerman, and Yongqiang Zhao. 2020. “Bounds on 2-Torsion in Class Groups of Number Fields and Integral Points on Elliptic Curves.” *J. Amer. Math. Soc.* 33 (4): 1087–99.

Helfgott, Harald, and Akshay Venkatesh. 2006. “Integral Points on Elliptic Curves and 3-Torsion in Class Groups.” *J. Amer. Math. Soc.* 19 (3): 527–50.

Schmidt, Wolfgang M. 1992. “Integer Points on Curves of Genus 1.” *Compos. Math.* 81 (1): 33–59.

Siegel, Carl Ludwig. 1929. *Über einige Anwendungen diophantischer Approximationen*. Akad. de Gruyter in Komm.