The BSD Conjecture

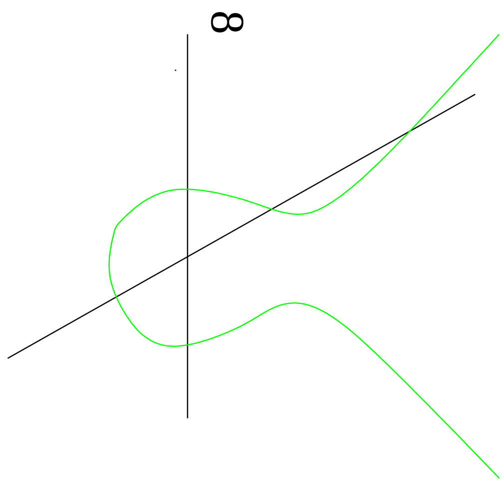
William Stein
Berkeley

January 12, 2000

An elliptic curve "$X_0(27)$":

$$y^2 + y = x^3 - 7$$

Cubic curve: Random line intersects at *3 points*, including ∞!



Points: $\infty, (3, 4), (3, -5)$
Searched with computer; all I found.

More points over finite fields:

- $\mathbf{F}_2 = \{0, 1\}$, $y^2 + y = x^3 + 1$:

$$\infty, (1, 0), (1, 1)$$

- $\mathbf{F}_3 = \{0, 1, 2\}$, $y^2 + y = x^3 + 2$:

$$\infty, (0,1), (1, 0), (1, 2)$$

  Group law: The points form an abelian group. No nontrivial map $\mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z}$!! $F = y^2 + y - x^3 - 2 = 0$, $F_x = 0 = F_y = 2y + 1 = 0$ at singular point $(0, 1)$. Tamagawa number $c_3 = 3$, measures type of reduction.

- $\mathbf{F}_5$, $y^2 + y = x^3 + 3$

$$\{\infty, (2, 2), (3, 0), (3, 4), (4, 1), (4, 3)\}$$

  Cryptography: Schaefer's course, Koblitz, SEA, discrete log problem, Lenstra's ECM.