Elliptic curves - continued

March 20, 2010

Corollary

(a) For every prime p, the subgroup $C(p)$ contains no points of finite order (other than $\mathcal{O}$).

(b) Let $P = (x, y) \neq \mathcal{O}$ be a rational point of finite order. Then x and y are integers.

Nagell-Lutz theorem

Let

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients a, b, c; and let D be the discriminant of the cubic polynomial $f(x)$:

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Let $P = (x, y)$ be a rational point of finite order.
Then x and y are integers and either $y = 0$, in which case P has order two, or else y divides D.

Nagell-Lutz - finishing the proof

Nagell-Lutz - finishing the proof

- Recall: Let $P = (x, y)$ be a point on the cubic curve such that P and $2P$ are not $\mathcal{O}$ and both have integer coordinates. Then $y \mid D$.

Applications of Nagell-Lutz

- A necessary condition for a point to have finite order
- Proving that a point is of infinite order

Applications of Nagell-Lutz

- A necessary condition for a point to have finite order
- Proving that a point is of infinite order
  Recall (for $P = (x, y)$):

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

Mazur's theorem

Let C be a non-singular rational cubic curve and suppose that $C(\mathbb{Q})$ contains a point of finite order m. Then either

$$1 \leq m \leq 10 \quad \text{or} \quad m = 12$$

More precisely, the set of all points of finite order in $C(\mathbb{Q})$ forms a subgroup which is isomorphic to the one of the following:

1. $\mathbb{Z}_N$ with $1 \leq N \leq 10$ or $N = 12$.
2. $\mathbb{Z}_2 \times \mathbb{Z}_{2N}$ with $1 \leq N \leq 4$