Integral Points on Families of Elliptic Curves

Szabolcs Tengely

29/01/2009

Algebraic Curves

Let $f \in \mathbb{Q}[X,Y], C(R) = \{(x,y) \in R^2 : f(x,y) = 0\}$.

- genus at least 1: Siegel (1929) proved that $C(\mathbb{Z})$ is finite.
- genus at least 2: Faltings (1983) proved that $C(\mathbb{Q})$ is finite.

curves of genus 1:

$$Y^2 = X^3 + AX + B.$$

curves of genus 2:

$$Y^2 = b_6X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0.$$

Elliptic Curves

General Weierstrass equation:

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

Weierstrass equation:

$$E : \quad y^2 = x^3 + Ax + B.$$

Discriminant of E : $\quad \Delta = -16(4A^3 + 27B^2)$,
j-invariant of E : $\quad j = -\frac{1728(4A)^3}{\Delta}$.
Mordell-Weil group: $(E(\mathbb{Q}), +)$

$$P \in E(\mathbb{Q}) = T + n_1P_1 + n_2P_2 + \ldots + n_rP_r,$$

Rank of E : $\mathrm{rank}(E) = r$.

There are only finitely many integral points: Mordell (1922).

Bounds for the solutions: Baker (1968)

$$\max(|x|,|y|) < \exp((10^6 H)^{10^6}).$$

Algorithms to determine integral points:
Gebel, Pethő, Zimmer (1994) and independently
Stroeker, Tzanakis (1994).

Improved explicit bounds for the heights of (S-)integer solutions of elliptic equations:
Hajdu and Herendi (1998):

$$\max\{|x|, |y|\} \leq \exp\{5 \cdot 10^{64} c_1 \log(c_1)(c_1 + log(c_2))\}.$$

Improved bounds for special curves.

Draziotis (2006):
Let

$$E : \quad Y^2 = (X - k)f(X)$$

elliptic curve over $\mathbb{Q}$, where $k \in \mathbb{Z}$ and $f(k) = \pm 1$.

Improved explicit bounds for the heights of (S-)integer solutions of elliptic equations:
Hajdu and Herendi (1998):

$$\max\{|x|,|y|\} \leq \exp\{5 \cdot 10^{64} c_1 \log(c_1)(c_1 + log(c_2))\}.$$

Improved bounds for special curves.

Draziotis (2006):
Let

$$E: \quad Y^2 = (X-k)f(X)$$

elliptic curve over $\mathbb{Q}$, where $k \in \mathbb{Z}$ and $f(k) = \pm 1$. If $(x, y) \in E(\mathbb{Z})$ is an integral point, then we have

$$|x| < 11H^2 + 5,$$

where H is the height of the polynomial $(X-k)f(X)$.

A congruent number is an integer that is equal to the area of a rational right triangle.

n is congruent $\Rightarrow E_n: \quad y^2 = x^3 - n^2x, \quad \text{rank}(E_n) > 0.$

Sometimes it is difficult to find generators of the MW group:

$$Y^2 = X(X - 157)(X + 157).$$

A congruent number is an integer that is equal to the area of a rational right triangle.

n is congruent $\Rightarrow E_n: \quad y^2 = x^3 - n^2x, \quad \mathrm{rank}(E_n) > 0.$

Sometimes it is difficult to find generators of the MW group:

$$Y^2 = X(X - 157)(X + 157).$$

A point of infinite order $P = (x, y)$, where:

$$x = \frac{-166136231668185267540804}{2825630694251145858025},$$
$$y = \frac{-167661624456834335404812111469782006}{150201095200135518108761470235125}.$$

Hasse Principle (Local-to-Global Principle)

$\exists$ points over $\mathbb{Q}_v \Rightarrow$

$\exists$ points over $\mathbb{Q}$.

Hasse Principle (Local-to-Global Principle)
$\exists$ points over $\mathbb{Q}_v \Rightarrow$
$\exists$ points over $\mathbb{Q}$.

Hasse Principle fails:

Probably the most famous example (due to Selmer):

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

Hasse Principle (Local-to-Global Principle)
$\exists$ points over $\mathbb{Q}_v \Rightarrow$
$\exists$ points over $\mathbb{Q}$.

Hasse Principle fails:

Probably the most famous example (due to Selmer):

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

Example by Lind and Reichart:

$$X^4 - 17Y^4 = 2Z^2.$$

Lang's conjecture: There is an absolute constant C such that if E is given by a minimal (affine) Weierstrass equation, then the number of integral points is at most

$$C^{1+\mathrm{rank}(E)}.$$

Lang's conjecture: There is an absolute constant C such that if E is given by a minimal (affine) Weierstrass equation, then the number of integral points is at most

$$C^{1+\mathrm{rank}(E)}.$$

Silverman: Lang's conjecture is true if $j(E) \in \mathbb{Z}$.

Given rank, small conductor $\Rightarrow$ many integral points?

$$Y^2 + Y = X^3 + X^2 - 2X,$$

here the rank is 2, the conductor is 389 and there are 20 integral points on the curve.

Given rank, small conductor $\Rightarrow$ many integral points?

$$Y^2 + Y = X^3 + X^2 - 2X,$$

here the rank is 2, the conductor is 389 and there are 20 integral points on the curve.

$$Y^2 + Y = X^3 - 7X + 6,$$

here the rank is 3, the conductor is 5077 and there are 36 integral points on the curve.

Rank 0 curves

Iskra (1998): Let $p_1, p_2, \dots, p_l$ distinct primes : $p_i \equiv 3 \mod 8$ and $(p_j/p_i) = -1$ if $j < i$. Then $n = p_1 p_2 \cdots p_l$ is a non-congruent number.

Example 1. $E: \quad y^2 = x^3 - (3 \cdot 19)^2 x$, the rank of E is 0.

Example 2. (Genocchi 1855) $E_p: \quad y^2 = x^3 - p^2 x$, where $p \equiv 3 \mod 8$, the rank of E_p is 0.

$E_p: \quad y^2 = x^3 - p^2 x$, where $p \equiv 3 \bmod 8$, the rank of E_p is 0.

$$\begin{aligned} x &= au^2, \\ x - p &= bv^2, \\ x + p &= cw^2, \\ abc &= \square. \end{aligned}$$

$E_p : \quad y^2 = x^3 - p^2 x$, where $p \equiv 3 \bmod 8$, the rank of E_p is 0.

$$\begin{aligned} x &= au^2, \\ x - p &= bv^2, \\ x + p &= cw^2, \\ abc &= \square. \end{aligned}$$

One obtains that $a, b, c \in \{\pm 1, \pm 2, \pm p, \pm 2p\}$. There are 64 systems of equations.
32 systems have no solution in $\mathbb{R}$,
28 systems have no solution modulo some prime (power),
$(1,1,1); (-1,-p,p); (p,2,2p); (-p,-2p,2) \leftrightarrow$ torsion points.
Therefore the rank is 0.

Rank 1 curves

Let

$$E_m : \quad Y^2 = X^3 + mX^2 - (m+3)X + 1.$$

Duquesne (2001): if $\text{rank}(E_m) = 1$, then the integral points of E_m :

$(0,1)$ if m is even,

$(0,1)$ and $2(0,1)$ if m odd.

Rank 1 curves

Let

$$E_m : \quad Y^2 = X^3 + mX^2 - (m+3)X + 1.$$

Duquesne (2001): if $\operatorname{rank}(E_m) = 1$, then the integral points of E_m :

$$(0,1) \text{ if } m \text{ is even,}$$

$$(0,1) \text{ and } 2(0,1) \text{ if } m \text{ odd.}$$

Let

$$Q_m : \quad Y^2 = X^4 - mX^3 - 6X^2 + mX + 1,$$

where $m^2 + 16$ is not divisible by and odd square. Duquesne (2007): if $\operatorname{rank}(Q_m) = 1$, then $Q_m(\mathbb{Z}) = \{(0, \pm 1)\}$.

Rank 2 curves

Let

$$Q_m : \quad Y^2 = X^4 - mX^3 - 6X^2 + mX + 1,$$

where $m^2 + 16$ is not divisible by and odd square. Duquesne (2007): if $m = 6k^2 + 2k - 1$ and $\mathrm{rank}(Q_m) = 2$, then $Q_m(\mathbb{Z}) = \{(0, \pm 1), (-3, \pm(2 + 12k))\}$.

Generators of the MW group:

$$\begin{aligned} G_1 &= (-4, 2(6k^2 + 2k - 1)), \\ G_2 &= (-2k^2 + 2k - 1, 4(k+1)(2k^2 - 2k + 1)). \end{aligned}$$

Figurate numbers

g-gonal numbers:

$$\mathcal{G}_{m,g} = \frac{m\{(g-2)m-(g-4)\}}{2}.$$

In cases of $g \in \{3, 4, 5, 7\}$ all g-gonal numbers were determined in certain recurrence sequences by Cohn, Katayama, Ljunggren, Luo, Prasad, Rao.

Figurate numbers

g-gonal numbers:

$$\mathcal{G}_{m,g} = \frac{m\{(g-2)m-(g-4)\}}{2}.$$

In cases of $g \in \{3,4,5,7\}$ all g-gonal numbers were determined in certain recurrence sequences by Cohn, Katayama, Ljunggren, Luo, Prasad, Rao.

Tengely (2008): if $g \in \{6,8,9,10,\ldots,20\}$, then all solutions were computed in the following cases

$$F_n = \mathcal{G}_{m,g}, \quad L_n = \mathcal{G}_{m,g},$$
$$P_n = \mathcal{G}_{m,g}, \quad Q_n = \mathcal{G}_{m,g}$$

Useful identities:

$$L_n^2 - 5F_n^2 = 4(-1)^n,$$
$$Q_n^2 - 2P_n^2 = (-1)^n.$$

One has to compute integral points on the families of genus 1 curves:

$$\begin{aligned}
C_{F_n}^{even} &: \quad Y^2 = 5((g-2)X^2-(g-4)X)^2+16,\\
C_{F_n}^{odd} &: \quad Y^2 = 5((g-2)X^2-(g-4)X)^2-16,\\
C_{L_n}^{even} &: \quad Y^2 = 5((g-2)X^2-(g-4)X)^2-80,\\
C_{L_n}^{odd} &: \quad Y^2 = 5((g-2)X^2-(g-4)X)^2+80,\\
C_{P_n}^{even} &: \quad Y^2 = 2((g-2)X^2-(g-4)X)^2+4,\\
C_{P_n}^{odd} &: \quad Y^2 = 2((g-2)X^2-(g-4)X)^2-4,\\
C_{Q_n}^{even} &: \quad Y^2 = 2((g-2)X^2-(g-4)X)^2-8,\\
C_{Q_n}^{odd} &: \quad Y^2 = 2((g-2)X^2-(g-4)X)^2+8.
\end{aligned}$$

Experiments

The equation $F_n = \mathcal{G}_{m,g} \Rightarrow$

$$\begin{aligned} C_{F_n}^{even} &: \quad Y^2 = 5((g-2)X^2 - (g-4)X)^2 + 16, \\ P_e &= (0,4) \\ C_{F_n}^{odd} &: \quad Y^2 = 5((g-2)X^2 - (g-4)X)^2 - 16, \\ P_o &= (1,2). \end{aligned}$$

If $\operatorname{rank}(E_{F_n}^{even,odd}) \in \{1,2\}$ and $16 < g < 100$, then

$$X \in \{0, \pm 1\}.$$