Д.Ф. Базылев, В.И. Янчевский

ЦЕЛОЧИСЛЕННЫЕ ТОЧКИ СПЕЦИАЛЬНЫХ АЛГЕБРАИЧЕСКИХ КРИВЫХ

In this paper we consider integer points on special algebraic curves in order to estimate bounds for coordinates of such points.

Согласно результату Зигеля, число целочисленных точек на алгебраической кривой ненулевого рода конечно. [1]

В данной работе предлагается метод оценки для координат целочисленных точек на алгебраических кривых E вида

$y^2 = a_{2m}^2 x^{2m} + \sum_{k=0}^{2m-1} a_k x^k$, где $a_{2m} \in \mathbf{N},\ a_k \in \mathbf{Z}$.

Пусть $c(x) = \sum_{k=0}^{m} c_k x^k$, где $c_m = a_{2m}, \sum_{i+j=k} c_i c_j = a_k, m \le k \le 2m-1,$ (1)

тогда $y^2 = c^2(x) + r(x), r(x) = \sum_{k=0}^{n} r_k x^k, n \le m-1.$

Известно, что $x^n + \sum_{k=0}^{n-1} b_k x^k$ >0 для любого $x \ge \max|b_k| + 1.$

Рассмотрим точку P(x,y)$\in$E(**Z**), для которой x>0. Будем считать, для определенности, y>0. Последовательно определив значения $c_{m-1},..., c_0$ из рекурентных соотношений (1), найдем натуральное число B такое, что Bc(x)$\in$**Z**[x]. Если r_n >0, то r(x)>0 для любого

$x \ge A_1 = \max_{k<n}\left|\frac{r_k}{r_n}\right| + 1,$ тогда $y^2 > c^2(x)$ для любого $x \ge A_1$. Так как

$c_m = a_{2m} > 0,$ то c(x)>0 для любого $x \ge B_1 = \max_{k<m}\left|\frac{c_k}{c_m}\right| + 1,$

следовательно, y>c(x)>0 для любого $x \ge \max(A_1, B_1)$. Так как By, Bc(x) – целые числа, By>Bc(x)>0, то

$(By)^2 \ge (Bc(x)+1)^2,\ c(x) - 0{,}5B(y^2 - c^2(x)) + (2B)^{-1} \le 0,$ т.е.

$H(x) \stackrel{def}{=} c(x) - 0{,}5Br(x) + (2B)^{-1} \le 0.$ Пусть $H(x) = \sum_{k=0}^{m} h_k x^k$, тогда

$h_m = c_m, h_k = c_k - 0{,}5Br_k, h_0 = c_0 - 0{,}5Br_0 + (2B)^{-1},$ где 0<k<m

(при n<m–1 обозначим $r_{n+1} = 0,..., r_{m-1} = 0$). Так как $H(x) \le 0,$ то $x \le \max_{k<m}\left|\frac{h_k}{h_m}\right| + 1 = H_1.$ Таким образом, если $r_n > 0,$ то $x \le \max(A_1, B_1, H_1).$

Если $r_n < 0,$ то r(x)<0 для любого $x \ge A_1,$ значит $y^2 < c^2(x)$ для любого $x \ge A_1$, следовательно, y<c(x) для любого $x \ge \max(A_1, B_1).$ Так как By, Bc(x) - целые числа, 0<By<Bc(x), то $(By)^2 \le (Bc(x)-1)^2,$ $c(x) + 0{,}5B(y^2 - c^2(x)) - (2B)^{-1} \le 0,$ т.е.

$L(x) \overset{def}{=} c(x) + 0{,}5Br(x) - (2B)^{-1} \le 0.$ Пусть $L(x) = \sum_{k=0}^{m} l_k x^k,$ тогда $l_m = c_m, l_k = c_k + 0{,}5Br_k, l_0 = c_0 + 0{,}5Br_0 - (2B)^{-1},$ где 0<k<m. Так как $L(x) \le 0,$ то $x \le \max_{k<m} \left|\frac{l_k}{l_m}\right| + 1 = L_1.$ Таким образом, если $r_n < 0,$ то $x \le \max(A_1, B_1, L_1).$

Итак, если P(x,y)$\in$E(**Z**), x>0, то $x \le \max(A_1, B_1, L_1, H_1).$

Если x<0, то $y^2 = a_{2m}^2 u^{2m} + \sum_{k=0}^{2m-1} a_k (-1)^k u^k,$ где $u = -x > 0.$ Аналогично находим константы A_2, B_2, L_2, H_2 такие, что $u \le \max(A_2, B_2, L_2, H_2),$ т.е. $x \ge -\max(A_2, B_2, L_2, H_2).$

Итак, в вышеприведенных обозначениях справедлива следующая теорема.

Теорема 1. Пусть задана алгебраическая кривая E: $y^2 = a_{2m}^2 x^{2m} + \sum_{k=0}^{2m-1} a_k x^k$ ($a_{2m} \in \mathbf{N}, a_k \in \mathbf{Z}$), P(x,y)$\in$E(**Z**), тогда $-\max(A_2, B_2, L_2, H_2) \le x \le \max(A_1, B_1, L_1, H_1).$

В качестве примера рассмотрим кривую, заданную уравнением

$$y^2 = \sum_{k=0}^{2m} a^{2m-k} x^k \quad (a \in \mathbf{N}). \tag{2}$$

Справедлива следующая теорема.

Теорема 2. Пусть алгебраическая кривая E задана уравнением (2), P(x,y)$\in$E(**Z**), тогда $|x| < 2^{2m-2} a^{m+1}(1-(4m)^{-1}) + 1{,}375a.$

Доказательство:

Рассмотрим x>0, m>1. Будем считать, для определенности, y>0. Согласно (2), имеем $z^2 = \sum_{k=0}^{2m} t^k,$ где $z = ya^{-m}, t = xa^{-1}.$

Пусть $c(t) = \sum_{k=0}^{m} c_{m-k} t^k,$ где $c_0 = 1, c_k = \frac{(2k-1)!!}{(2k)!!} = \frac{C_{2k-1}^k}{2^{2k-1}},$ тогда $c^2(t) = \sum_{k=m}^{2m} t^k + r(t),$ где $r(t) = \sum_{k=0}^{m-1} r_k t^k,$

$$1 > r_{m-1} > \dots > r_0 > 0, 1 = c_0 > \dots > c_m > 0, \ \frac{1}{2\sqrt{k}} \le c_k < \frac{1}{\sqrt{\pi k}}, \tag{3}$$

$r_{m-1} = c_1 c_m + c_2 c_{m-1} + ... + c_m c_1 = 1 - 2c_{m+1}$, $r_{m-2} = c_2 c_m + ... + c_m c_2 =$
$= 1 - 2(c_{m+2} + c_1 c_{m+1}), \ldots, r_1 = c_{m-1}c_m + c_m c_{m-1}, r_0 = c_m^2$ (см. [2]). (4)

Имеем $z^2 = \sum_{k=0}^{2m} t^k > \sum_{k=m}^{2m} t^k + r(t) = c^2(t)$, значит $z > c(t)$.

Так как $2^{2k-1} c_k \in \mathbf{N}$, то $2^{2m-1} c(t) \in \mathbf{Z}[t]$, значит $2^{2m-1} a^m c(t) =$
$= 2^{2m-1} \sum_{k=0}^{m} c_{m-k} a^{m-k} x^k \in \mathbf{Z}[x]$, учитывая, что $a^m z = y \in \mathbf{N}$, $z > c(t)$,
имеем $2^{2m-1} a^m z \geq 2^{2m-1} a^m c(t) + 1$, $z \geq c(t) + q$, где $q = 2^{1-2m} a^{-m}$,
следовательно, $z^2 \geq (c(t)+q)^2$, $c(t) - (2q)^{-1}(z^2 - c^2(t)) + 0{,}5q \leq 0$, т.е.
$H(t) \stackrel{def}{=} c(t) - 2^{2m-2} a^m \sum_{k=0}^{m-1} (1 - r_k) t^k + (4a)^{-m} \leq 0$. Пусть $H(t) = \sum_{k=0}^{m} h_k t^k$,
тогда $h_m = c_0 = 1$, $h_k = c_{m-k} - 2^{2m-2} a^m (1 - r_k)$, где 0<k<m;
$h_0 = c_m - 2^{2m-2} a^m (1 - r_0) + (4a)^{-m}$. (5)

Согласно (3) и (4), имеем $h_1 < ... < h_{m-1} = c_1 - 2^{2m-2} a^m (1 - r_{m-1}) =$
$= 0{,}5 - 2^{2m-1} a^m c_{m+1} \leq 0{,}5 - \frac{2^{2m-2} a^m}{\sqrt{m+1}} < 0$, причем $h_1 - h_0 =$
$= (c_{m-1} - 2^{2m-2} a^m (1 - 2c_{m-1}c_m)) - (c_m - 2^{2m-2} a^m (1 - c_m^2) + (4a)^{-m}) =$
$= 2^{2m-2} a^m c_m (2c_{m-1} - c_m) + (c_{m-1} - c_m) - (4a)^{-m} >$
$2^{2m-2} a^m \frac{1}{2\sqrt{m}} \left(\frac{1}{\sqrt{m-1}} - \frac{1}{\sqrt{\pi m}} \right) - (4a)^{-m} > 0$, т.е. $0 > h_{m-1} > ... > h_0$,
значит $\max_{k<m} |h_k| = |h_0|$. Далее, $|h_0| = 2^{2m-2} a^m (1 - c_m^2) - c_m - (4a)^{-m} <$
$< 2^{2m-2} a^m (1 - (4m)^{-1}) + 0{,}375$, следовательно, $xa^{-1} = t \leq \max_{k<m} |h_k| + 1 =$
$= |h_0| + 1 < 2^{2m-2} a^m (1 - (4m)^{-1}) + 1{,}375$,
т.е. $x < 2^{2m-2} a^{m+1} (1 - (4m)^{-1}) + 1{,}375a = B$.

Рассмотрим x<0, m>1. Будем считать, для определенности, y>0. Заменой переменных x, y на $t = -xa^{-1}, z = ya^{-m}$, получаем
$z^2 = \sum_{k=0}^{2m} (-t)^k$.

Пусть $c(t) = \sum_{k=0}^{m} c_{m-k} (-t)^k$, где $c_0 = 1, c_k = \frac{C_{2k-1}^k}{2^{2k-1}}$, тогда
$c^2(t) = \sum_{k=m}^{2m} (-t)^k + r(t)$, где $r(t) = \sum_{k=0}^{m-1} r_k (-t)^k$, $1 > r_{m-1} > ... > r_0 > 0$,
$1 = c_0 > ... > c_m > 0$, следовательно, $z^2 - c^2(t) = \sum_{k=0}^{m-1} (1 - r_k)(-t)^k$.

Если m$\equiv$1(mod 2), то $z^2 - c^2(t) > 0$ для любого $t \geq A =$
$= \max\limits_{k<m-1}\left|\frac{1-r_k}{1-r_{m-1}}\right| + 1.$ Заметим, что $\left|\frac{1-r_k}{1-r_{m-1}}\right| = \frac{1-r_k}{2c_{m+1}} < \frac{1}{2c_{m+1}} \leq \sqrt{m+1},$
значит $z^2 > c^2(t)$ для любого $t \geq \sqrt{m+1}+1,$ причем c(t)<0 для любого

$t \geq \max\limits_{0<k\leq m}|c_k| + 1 = c_1 + 1 = 1{,}5,$ следовательно, $z > -c(t)$ для любого $t \geq \sqrt{m+1}+1.$ Аналогично получаем, $z \geq -c(t)+q,$ где $q = 2^{1-2m}a^{-m};$
$z^2 \geq (-c(t)+q)^2,\ -c(t)-(2q)^{-1}(z^2-c^2(t))+0{,}5q \leq 0,$ т.е.
$N(t) \overset{def}{=} -c(t) - 2^{2m-2}a^m\sum\limits_{k=0}^{m-1}(1-r_k)(-t)^k + (4a)^{-m} \leq 0.$ Пусть

$N(t) = \sum\limits_{k=0}^{m} n_k(-1)^{k+1}t^k,$ тогда $n_m = c_0 = 1,$ $n_k = c_{m-k} + 2^{2m-2}a^m(1-r_k),$
где 0<k<m; $n_0 = c_m + 2^{2m-2}a^m(1-r_0) - (4a)^{-m}.$ Так как $N(t) \leq 0,$
то $t \leq \max\limits_{k<m}|n_k| + 1.$ Если $k = 1,2,\ldots,m-2,$ то $n_k - n_{k+1} =$
$= 2^{2m-2}a^m(r_{k+1}-r_k) + c_{m-k} - c_{m-k-1} \geq 2^{2m-2}a^m c_{m-k-1}c_m + c_{m-k} - c_{m-k-1} >$
$> (2^{2m-2}a^m c_m - 1)c_{m-k-1} > 0,$ т.е. $n_1 > \ldots > n_{m-1} > 0.$ Действительно,
$r_{k+1} = c_{m-k-1}c_m + \ldots + c_m c_{m-k-1},\ r_k = c_{m-k}c_m + \ldots + c_m c_{m-k},\ r_{k+1} - r_k =$
$= c_{m-k-1}c_m + c_{m-k}(c_{m-1} - c_m) + \ldots + c_m(c_{m-k-1} - c_{m-k}) \geq c_{m-k-1}c_m.$
Далее,
$n_0 - n_1 = 2^{2m-2}a^m c_m(2c_{m-1} - c_m) + c_m - c_{m-1} - (4a)^{-m} =$
$= (2^{2m-2}a^m c_m - 1)(2c_{m-1} - c_m) + (c_{m-1} - (4a)^{-m}) > 0.$ Таким образом,
$\max\limits_{k<m}|n_k| = n_0.$ Так как $c_m \leq c_3,$ m$\equiv$1(mod 2), то
$n_0 < 2^{2m-2}a^m(1-(4m)^{-1}) + 0{,}375,$ следовательно,
$-xa^{-1} = t \leq \max\limits_{k<m}|n_k| + 1 = |n_0| + 1 < 2^{2m-2}a^m(1-(4m)^{-1}) + 1{,}375,$
т.е. $-x < B, x > -B.$

Если m$\equiv$0(mod 2), то аналогичным образом получаем, что c(t)>0 для любого $t \geq 1{,}5;$ $z < c(t)$ для любого $t \geq \sqrt{m+1}+1,$ значит $z \leq c(t) - q,$ где $q = 2^{1-2m}a^{-m};$ $z^2 \leq (c(t)-q)^2,$
$c(t) + (2q)^{-1}(z^2 - c^2(t)) - 0{,}5q \leq 0.$ Аналогично получаем, что $-x < B.$

Несложно проверить, что для m=1 неравенство выполнено.
Теорема доказана.

1. Lang S. *Elements of Diophantine Geometry*. Springer – Verlag: New – York, 1983.
2. Kanold Hans - Joachim *Űber eine spezielle Klasse von Diophantischen Gleichungen*, J.reine und angew. Math., 1970, **245**, 165-171.