JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

JAVIER CILLERUELO

JORGE JIMÉNEZ-URROZ

The hyperbola $xy = N$

Journal de Théorie des Nombres de Bordeaux, tome 12, n^{o} 1 (2000), p. 87-92.

<http://www.numdam.org/item?id=JTNB_2000__12_1_87_0>

Journal de Théorie des Nombres
de Bordeaux **12** (2000), 87–92

The hyperbola $xy = N$

par Javier CILLERUELO et Jorge JIMÉNEZ-URROZ

RÉSUMÉ. On montre plusieurs résultats à propos de la longueur minimale d'un arc de l'hyperbole $xy = N$ contenant k points entiers.

ABSTRACT We include several results providing bounds for an interval on the hyperbola $xy = N$ containing k lattice points.

1. Introduction

Consider the hyperbola $xy = N$, for $N \in \mathbb{Z}$. We are interested in finding bounds for the length of an arc of the hyperbola having certain number of lattice points. Clearly, any lattice point on $xy = N$ gives a divisor of N. We will use this arithmetic interpretation to get the results.

In [2] the authors proved a lower bound, depending on the curvature. Namely

Theorem. *On the hyperbola $xy = N$ there are at most k lattice points $(x_1, y_1), \cdots, (x_k, y_k)$ such that $N^\gamma \leq x_1 < \cdots < x_k$ and $x_k - x_1 \leq N^{E_k(\gamma)}$. where*

$$E_k(\gamma) = \frac{[k\gamma](2k\gamma - [k\gamma] - 1)}{k(k-1)}.$$

In [3] the authors proved that this lower bound is best possible whenever $1/k < \gamma \leq 1/(k-1)$. However, it does not seems to be the case for other γ. Here we include some results which tell us that in general $E_k(\gamma)$ is far from the real bound.

For $k = 2, 3$ and any γ we found in [3] examples as good as possible with polynomial growth, in arcs of length $N^{E_k(\gamma)}$. For $k = 4$ we already proved there that it is not possible to find such kind of examples. However in this case we still can get four points in an arc of lenght $E_4(1/2)$. In other words, let us fix an integer k and $0 < \gamma < 1$. We define

$$\varepsilon_k(\gamma) = \liminf \{\varepsilon \mid N^\gamma \ll a_1 < \cdots < a_k = a_1 + N^\varepsilon\},$$

where $a_i | N$ for all $1 \leq i \leq k$, i.e. the minimum ε such that for infinitely many N there exist k lattice points (a_i, b_i), $a_i \asymp N^\gamma$, on an arc of length N^ε of the hyperbola $xy = N$. We can prove

Theorem 1. $\varepsilon_4(1/2) = E_4(1/2)$.

We give an example which grows exponentially.

For other γ we can give partial results by a convexity theorem

Theorem 2. *There exists $g_{k,\gamma} \in (1/k, \gamma)$ such that, for any $1/k < g < g_{k,\gamma}$ we have*

$$\varepsilon_k(g)/(kg-1) \leq \varepsilon_k(\gamma)/(k\gamma - 1)$$

This result, and the symmetry restricts our interest to $\gamma = 1/2$. By generalizing Theorem 1 we get

Theorem 3. *There exist a constant c such that*

$$\varepsilon_k(1/2) < 1/2 - c/\log k.$$

This theorem should be compared with the trivial $\varepsilon_k(1/2) < 1/2 - c/k^{1/2}$.

Even in $\gamma = 1/2$, the exact center of the hyperbola $(\sqrt{N}, \sqrt{N})$, turns out to be of special interest. In this particular case, it is more convenient to reformulate the problem as follows:

Question. Given $\alpha < 1/2$, how many lattice points (x, y) of the hyperbola $xy = N$ verify $N^{1/2} \leq x \leq N^{1/2} + N^{\alpha}$?

By a geometric argument we see that for two lattice points we already need $\alpha \geq 1/4$. This is notably bigger than our best exponent $E_4(1/2) = 1/6$.

There is a conjecture apparently of I. Ruzsa which goes even further:

Conjecture. For all $\varepsilon > 0$ there exists an integer k such that only for a finite number of values of N there can be more than k lattice points on $xy = N$ verifying

$$N^{1/2} \leq x \leq N^{1/2} + N^{1/2-\varepsilon}.$$

We prove that the conjecture is true on average, in the following sense; Let us define

$$d_\alpha(n) = \#\{(a,b) \mid a, b \in I,\ ab = n\},$$

for $I = (N, N + N^{\alpha}]$.

Theorem 4. *Let $0 < \alpha < 1$ fixed. Then*

$$\sum d_\alpha^2(n) = 2N^{2\alpha} + O\left(N^{3\alpha-1}\log N\right) + O\left(N^{\alpha}\right).$$

Theorem 4 was suggested by a similar result about points on circles studied in [1].

We will use $f(x) = O(g(x))$ in the standard way, and $f(x) \asymp g(x)$ will mean both $f(x) = O(g(x))$ and $g(x) = O(f(x))$, $[a_1, \cdots, a_k]$ and $(a_1, \cdots, a_k)$ will be the least common multiple and greatest common divisor of $a_1, \cdots, a_k$ respectively.

2. Proof of Theorems

Let us consider $k = 2$ for a moment. The least common multiple, M, of two integers a_1, a_2 with greatest common divisor $(a_1, a_2) = d$ verify

$$M = a_1 a_2 / d \geq a_1 a_2 / (a_1 - a_2),$$

and equality happens only when $d = a_1 - a_2$. In order to find good bounds for the length, in terms of the least common multiple, we need to find integers so that their differences will be comparable with their greatest common divisors.

Proof of Theorems 1 and 3. For $k = 4$, consider p_n/q_n the convergents of $\sqrt{5}$ in its continuos fraction. Let

$$\begin{aligned} a_1 &= \quad p_m p_{m+2} q_{m+1} \\ a_2 &= \quad p_{m+1} p_{m+2} q_m \\ a_3 &= \quad p_m p_{m+1} q_{m+2} \\ a_4 &= \quad 5 q_m q_{m+1} q_{m+2}. \end{aligned}$$

It is well known that for i fixed we have

$$\left| \frac{p_{m+i}}{q_{m+i}} - \sqrt{5} \right| = O\left(\frac{1}{q_m^2} \right).$$

Hence, for any fixed i, j, $p_{m+i} \asymp q_{m+i} \asymp p_m$ and

$$\begin{aligned} p_{m+i} q_{m+j} - p_{m+j} q_{m+i} &\leq C, \\ p_{m+i} p_{m+j} - 5 q_{m+i} q_{m+j} &\leq C. \end{aligned}$$

We deduce then that numerators and denominators of close convergents are almost coprimes and so, for $1 \leq i < j \leq 4$ $(a_i, a_j) \asymp |a_1 - a_j|$. Moreover $M \asymp \prod_i p_{m+i} q_{m+i} \asymp p_m^6$, and $a_i \asymp p_m^3$, which give us the result since $E_4(1/2) = 1/6$ and $\varepsilon_k(\gamma) \geq E_k(\gamma)$ by definition.

In general, to prove Theorem 3 we construct our integers as follows; Let I, J a disjoint partition of $\{1, 2, \cdots, 2l\}$ such that $|I| = 2n$, we call

$$a_0 = \prod_{i=1}^{2l} p_{m+i},$$

and

$$a_I = 5^n \prod_{j \in J} p_{m+j} \prod_{i \in I} q_{m+i}.$$

We have $k = \sum_{n=0}^{l} \binom{2l}{2n} = 4^l/2$ integers. Moreover, if $I' \subset I$ and $|I \setminus I'| = 2$ then

$$\frac{a_I - a_{I'}}{a_{I'}} = \frac{a_I}{a_{I'}} - 1 = \frac{5q_{m+i}q_{m+j}}{p_{m+i}p_{m+j}} - 1 = O\left(\frac{1}{p_m^2}\right).$$

Hence $|a_I - a_{I'}| \ll p_m^{2l-2}$, and by the triangle inequality we get $|a_I - a_0| \ll lp_m^{2l-2}$, and so $|a_{I_1} - a_{I_2}| \ll lp_m^{2l-2}$ for any I_1, I_2 as above.

Furthermore, the least common multiple M of these k integers verifies

$$M \asymp \prod_{i=1}^{2l} p_{m+i}q_{m+i} \asymp p_m^{4l},$$

hence, $L \leq CM^{1/2-1/2l}$ for some constant depending on l which proves the thoeorem, since $l \leq c \log k$.

Proof of Theorem 2. By hypothesis, we know that there exist infinitely many integers M and $a_1 < a_2 < \cdots < a_k$ such that $[a_1, \cdots, a_k] = M$, $M^\gamma \ll a_1 < a_2 < \cdots < a_k$ and $a_k - a_1 \ll M^{\varepsilon_k(\gamma)+o(1)}$.

Consider the integers $A_i = a_i + TMD$ where $D = \prod_{1 \leq i < j \leq k} (a_j - a_i)/(a_j, a_i)$, and T is an integer $T \asymp M^{\beta-1}/D$ for $\beta = g(k\gamma - 1)/(kg - 1)$.

This selection is possible whenever $M^{\beta-1}/D \geq 1$. However since $D \leq M^\delta$ for some fix δ independent of M, we can find such T whenever $\beta - 1 - \delta \geq 0$, in other words $1/k < g \leq (1+\delta)/(k(1+\delta) - k\gamma + 1) = g_{k,\gamma} < \gamma$ since $1/k < \gamma < 1$.

Clearly $(A_i, A_j) = (a_i, a_j)$ and so

$$\frac{\prod A_i}{[A_1, \cdots, A_k]} = \frac{\prod a_i}{[a_1, \cdots, a_k]} \asymp M^{k\gamma-1}.$$

Moreover $A_i \asymp TMD \asymp M^\beta$. Hence,

$$N = [A_1, \cdots, A_k] \asymp \frac{\prod A_i}{M^{k\gamma-1}} \asymp \frac{A_1^k}{A_1^{(k\gamma-1)/\beta}} = A_1^{1/g},$$

and on the other hand $A_k - A_1 = a_k - a_1 \ll M^{\varepsilon_k(\gamma)+o(1)} \asymp N^{g\varepsilon_k(\gamma)/\beta+o(1)}$, which give us the result.

Remark 1. In order to get a better value of $g_{k,\gamma}$ we have to minimize D, being the best possible $g_{k,\gamma} = 1/(k - k\gamma + 1)$ when the differences are comparable with the greatest common divisors or, in other words when $D \leq C$ for some constant C. In Theorem 1 we have $(a_i, a_j) \asymp |a_i - a_j|$, hence $D \leq C$ for some constant C and so

$$\varepsilon_4(g) \leq \varepsilon_4(1/2)(4g - 1) = (4g - 1)/6,$$

in the range $1/4 < g < 1/3$, and this is the best result since $E_4(g) = (4g - 1/6)$ in this range. As we mentioned this fact is already proved in [3].

Proof of Theorem 4. First of all we note that

$$\sum d_\alpha(n) = N^{2\alpha} + O(N^\alpha), \tag{2.1}$$

since this sum counts exactly the lattice points in the square $Q = I \times I$.

We will say that the lattice points (a,b), (b,a) are symmetric, and we will call two lattice points on $xy = n$ onto Q non-symmetric representations of n if they are not symmetric. Define

$$S(n) = \{\text{non-symmetric representations of } n\}.$$

Suppose we have $d_\alpha(n) > 2$. Then, there exist at least two elements of $S(n)$, say $ab = n = cd$ where $a,b,c,d \in I$ and $a \neq c, d$.

Let us consider $m_1 = (a,c)$ and write $a = m_1 l_1$, $c = m_1 l_2$. Then there is an integer m_2 such that $b = m_2 l_2$ and $d = m_2 l_1$. Now, $a, c \in I$ so $m_1 \leq |c-a| \leq N^\alpha$. Hence, if we call

$$R = \{(m_1, m_2, l_1, l_2) \,|\, m_i l_j \in I, \text{ for } i,j \in \{1,2\}, \ 0 \leq m_1 \leq N^\alpha\}$$

then

$$\sum |S(n)| \leq |R|.$$

We now give an upper bound for $|R|$. We define a dilation of the interval I by $DI = (DN, D(N+N^\alpha)]$. Then

$$|R| \leq \sum_{0 \leq m_1 \leq N^\alpha} \sum_{l_1 \in m_1^{-1} I} \sum_{m_2 \in l_1^{-1} I} \sum_{l_2 \in m_2^{-1} I} 1 \ll N^{3\alpha - 1} \log N,$$

since $m_1, m_2, l_1, l_2 \leq N^\alpha$ and

$$\sum_{m \in DI} m^k \ll D^{k+1} N^{\alpha + k},$$

for any $D \leq N^\alpha$ and $k \in \mathbb{Z}$.

Suppose $d_\alpha(n) = j$. Then, $|S(n)| = j(j-2)/4$ if j is even and $|S(n)| = (j-1)^2/4$ if j is odd and in any case for $j \geq 3$ we have $|S(n)| \geq cj^2 = c d_\alpha^2(n)$ for some constant c. If we define $C_j = \{n \,|\, d_\alpha(n) = j\}$, then

$$\sum d_\alpha^2(n) = \sum j^2 |C_j|, \tag{2.2}$$

and we have just seen that

$$\sum_{j \geq 3} d_\alpha^2(n) \leq \sum |S(n)| \leq |R|. \tag{2.3}$$

On the other hand $C_1 = O(N^\alpha)$ since it counts the integers with only one representation in the diagonal, and by (2.1) and (2.3) we have

$$N^{2\alpha} + O(N^\alpha) = C_1 + 2C_2 + \sum_{j \geq 3} jC_j = 2C_2 + O\left(N^{3\alpha-1} \log N\right) + O(N^\alpha).$$

Hence

$$C_2 = \frac{1}{2}N^{2\alpha} + O\left(N^{3\alpha-1}\log N\right) + O\left(N^{\alpha}\right),$$

which give us the result in Theorem 4 by 2.2.

Remark 2. Theorem 4 cannot be extended to $\alpha = 1$. This is the analogous to $\varepsilon = 0$ in the conjecture of Ruzsa, which is trivially false in this case.

References

[1] J. Cilleruelo, A. Córdoba, *Trigonometric polynomials and lattice points.* Proc. Amer. Math. Soc. **115** (1992), 899–905.

[2] J. Cilleruelo, J. Jiménez-Urroz, *Divisors in a Dedekind domain.* Acta. Arith. **85** (1998), 229–233 .

[3] A. Granville, J. Jiménez-Urroz, *The least common multiple and lattice points on hyperbolas.* To appear in Quart. J. Math.

[4] G. H. Hardy, E. M. Wright, *Introduction to the theory of numbers.* Clarendon Press. 4th ed., Oxford, 1960.

Javier Cilleruelo, Jorge Jiménez-Urroz
Departamento de Matemáticas,
Facultad de Ciencias,
Universidad Autónoma de Madrid,
28049 Madrid, ESPAÑA.
E-mail : franciscojavier.cilleruelo@uam.es
jorge.jimenez@uam.es