THE LEAST COMMON MULTIPLE AND LATTICE POINTS ON HYPERBOLAS

Andrew Granville and Jorge Jiménez-Urroz

Abstract. We bound, from below, the least common multiple of k integers from a short interval. This is used to bound the length of an arc Γ of the hyperbola, $xy = N$, containing k integer lattice points.

1. Introduction

The problem of finding lattice points on curves has been studied by many authors, most famously Gauss's investigation on lattice points inside the circle. If we restrict our attention to lattice points on short arcs, then there are several bounds known; for example, for conics see [1, 2, 3, 4]. We consider the hyperbola $xy = N$ so that each lattice point is a divisor of N. Therefore counting lattice points on a small arc of the hyperbola, is the same as counting divisors of N in a short interval. We prove the following result:

Theorem 1. *Given k integers $X \le a_1 < \cdots < a_k \le X + L$, we have*

$$LCM[a_1, \cdots, a_k] \ \ge \ C_k \frac{X^k}{L^{\binom{k}{2}}}, \tag{1}$$

where C_k is positive and

$$C_k^2 = \frac{\left(\frac{2k}{k-1}\right)^k \binom{2k-2}{k}^{2k-1} \prod_{m=1}^{k-2} m!^2}{2(k!)\prod_{m=1}^{k-1}\binom{2m}{m}^2}. \tag{2}$$

Using Stirling's formula (see section 5) one can show that

$$C_k = \left(4e^{-3/2}k\right)^{k^2/2-3k/2} \left(16\pi e^{-5/2}\right)^{k/2} k^{7/24} e^{\alpha+O(1/k)} \tag{3}$$

where

$$\alpha = \frac{\log 4}{3} + \frac{\log \pi}{8} - \frac{53}{24} + \frac{5\gamma}{12} + \frac{5}{4}\sum_{j\ge 2}\frac{\zeta(j)-1}{j+2},$$

γ is the Euler constant, and $\zeta(j) := \sum_{n\ge 1} 1/n^j$ is the Riemann zeta function.

The first author is a Presidential Faculty Fellow and is supported, in part, by the National Science Foundation.

We give the first few values of C_k in the following table.

k	C_k
2	1
3	2^2
4	$2\cdot 5^2\sqrt{5}$
5	$\dfrac{2^6\cdot 7^3\sqrt{3\cdot 7}}{3}$
6	$2^7\cdot 3^6\cdot 7^3\sqrt{3\cdot 7}$
7	$\dfrac{2^{16}\cdot 3^7\cdot 11^5\cdot\sqrt{3\cdot 5\cdot 11}}{5^2}$
8	$\dfrac{2^{12}\cdot 3^6\cdot 11^5\cdot 13^6\cdot\sqrt{3\cdot 5\cdot 11\cdot 13}}{5}$
9	$\dfrac{2^{24}\cdot 3^7\cdot 5^8\cdot 11^5\cdot 13^6\cdot\sqrt{7\cdot 11\cdot 13}}{7^3}$
10	$\dfrac{2^{23}\cdot 3^9\cdot 5^4\cdot 11^5\cdot 13^6\cdot 17^8\cdot\sqrt{7\cdot 11\cdot 13\cdot 17}}{7^2}$

If p is a prime in the interval $(k, 2k-1)$ then p divides C_k^2 but p^2 does not, as may be seen by examining (2). Thus, by Bertrand's postulate, C_k is irrational for all $k\ge 4$.

Write $N := \mathrm{LCM}[a_1,\cdots,a_k]$ and $A_i = N/a_i$ for each i. Then Theorem 1 gives, since $N/(X+L)\le A_1<\cdots<A_k\le N/X$ that $N^{\binom{k-1}{2}}\ge C_kX^{k(k-2)}/L^{\binom{k}{2}}$. Thus

Corollary 1. *Given $k\ge 3$ integers $X\le a_1<\cdots<a_k\le X+L$, we have*

$$\mathrm{LCM}[a_1,\cdots,a_k]\ge C_k^{1/\binom{k-1}{2}}X^{2k/(k-1)}/L^{k/(k-2)}. \tag{4}$$

Notice that the bound in (1) is sharper than that of (4) exactly when $C_kX^{k-2}\ge L^{\binom{k}{2}}$ for $k\ge 4$ (the bounds are identical for $k=3$).

To prove Theorem 1 we write $a_i = X+\delta_iL$ for each i, so that $0\le\delta_1<\delta_2<\cdots<\delta_k\le 1$. Note that

$$\begin{aligned}\Lambda :&= \mathrm{LCM}[a_1,\cdots,a_k] = (a_1a_2\cdots a_k/L^{\binom{k}{2}})\cdot(\Lambda_2/\Lambda_1)\\ &\ge (X^k/L^{\binom{k}{2}})\cdot(\Lambda_2/\Lambda_1) \qquad (4a)\end{aligned}$$

where

$$\Lambda_1=\Lambda_1(a_1,\cdots,a_k;L) := \prod_{1\le i<j\le k}\frac{(a_j-a_i)}{L} = \prod_{1\le i<j\le k}(\delta_j-\delta_i),$$

$$\text{and}\quad \Lambda_2=\Lambda_2(a_1,\cdots,a_k) := \frac{\mathrm{LCM}[a_1,\cdots,a_k]}{\prod_{i=1}^k a_i}\prod_{1\le i<j\le k}(a_j-a_i),$$

In Proposition 1 we give a sharp upper bound on Λ_1 by analytic methods, and in Proposition 2 we give a sharp lower bound on Λ_2 by elementary methods. Combining these two results implies Theorem 1, using (4a).

Hilbert [10], Stieltjes [16], and others [14,15], have all shown how to maximize $(\Lambda_1 =) \prod_{1\le i<j\le k}(\delta_j - \delta_i)$ when $0 \le \delta_1 < \delta_2 < \cdots < \delta_k \le 1$. We present our own proof in section 2, though like most previous proofs, it involves computing discriminants of certain classical polynomials from the theory of orthogonal polynomials.

Proposition 1. *We have*

$$\max_{0\le\delta_1<\delta_2<\cdots<\delta_k\le 1}\left(\prod_{1\le i<j\le k}(\delta_j-\delta_i)\right)^2 = \frac{2(k-1)^k k!\prod_{m=1}^{k-1}\binom{2m}{m}^2}{(2k)^k\binom{2k-2}{k}^{2k-1}}.$$

We bound Λ_2 from below, by more elementary methods, in section 3.

Proposition 2. *Given integers $a_1 < a_2 < \cdots < a_k$, the number $\Lambda_2(a_1,\cdots,a_k)$, defined above, is an integer and is divisible by $\prod_{m=1}^{k-2} m!$.*

Remark. In section 4a we exhibit many examples with $\Lambda_2(a_1,\cdots,a_k) = \prod_{m=1}^{k-2} m!$, so Proposition 2 cannot be improved.

The lower bounds (1) and (4) are trivial for sufficiently large L, so we want to find the largest L for which these inequalities are sharp.

Theorem 2. *Given integer $k \ge 2$ and sufficiently large L, there exists $X \ll L^{\binom{k}{2}}$, such that*

$$M_k := \min_{X\le a_1<a_2<\cdots<a_k\le X+L} LCM[a_1,\cdots,a_k] = \left(1+O\left(\frac{1}{\sqrt{L}}\right)\right)C_k\frac{X^k}{L^{\binom{k}{2}}}.$$

Remark 1. Our proof gives many such k-tuples of integers with $X \gg L^{\binom{k}{2}}$. With a better understanding of the distribution of congruence classes we could give such a result in a wider range.

Remark 2. One can give examples in Theorem 2 described by polynomials. For example, if $k = 2$ let $X = a_1 = nL$ and $a_2 = (n+1)L$ for a given integer L. Since $(a_2, a_1) = L = a_2 - a_1$, we see that

$$[a_1,a_2] = \frac{a_1a_2}{(a_1,a_2)} = (n+1)X = \left(1+\frac{1}{n}\right)\frac{X^2}{L}.$$

For $k = 3$ we take, for any integers n and t, with $L = 4n$,

$$\begin{aligned} X = a_1 &= (n+1+(2n+1)t)4n(2n-1),\\ a_2 &= a_1+(2n-1) = ((2n+1)+4nt)(2n+1)(2n-1)\\ a_3 &= a_1+4n = (n+(2n-1)t)4n(2n+1)\end{aligned}$$

Again note that $(a_j, a_i) = a_j - a_i$ and that $(a_1, a_2, a_3) = 1$. Therefore

$$[a_1, a_2, a_3] = \frac{a_1 a_2 a_3}{\prod_{1 \le i < j \le 3}(a_j, a_i)} = \frac{a_1 a_2 a_3}{4n(2n+1)(2n-1)}$$
$$= 4\frac{X^3}{L^3}\left\{1 + O\left(\frac{n}{X} + \frac{1}{n^2}\right)\right\}$$

In both of these cases we have given polynomial examples which are as good as possible (in that they give examples with lcm$\sim C_k X^k / L^{\binom{k}{2}}$). This is not possible for $k \ge 4$: To see this notice that if it were then every $f_j(t) = a_j - a_1$ ($j \ge 2$) would have the same degree and would have integer coefficients. The ratios of the leading coefficients of the $f_j(t)$ would thus all be rational and so Λ_1 would be a rational number. However if lcm$\sim C_k X^k / L^{\binom{k}{2}}$ then the value of Λ_1^2 is given in Proposition 1, and this is not the square of a rational for any $k \ge 4$.

On the other hand we will show, in section 4c, how to construct such polynomials for each k which lead to examples with lcm$\ll_k X^k / L^{\binom{k}{2}}$.

We may re-interpret our results to give results about lattice points on the hyperbola $xy = N$ in as small an arc as possible. As a consequence of (1), (4) and Theorem 2 we have (taking $X = a_1$ and $L = a_k - a_1$):

Theorem 3. *If there are k distinct lattice points (a_i, b_i) on the hyperbola $ab = N$ with $a_1 < a_2 < \cdots < a_k$ then*

$$a_k - a_1 \ge c_k \max\left\{\frac{a_1^{2-\frac{2}{k-1}}}{N^{1-2/k}}, \frac{a_1^{\frac{2}{k-1}}}{N^{1/\binom{k}{2}}}\right\}. \tag{4b}$$

where $c_k := C_k^{1/\binom{k}{2}}$. On the other hand one can find integer N, together with k distinct lattice points (a_i, b_i) on the hyperbola $ab = N$ with

$$\text{either} \quad a_1 \gg_k N^{1-\frac{1}{k-1}} \quad \text{and} \quad a_k - a_1 \le \{c_k + o(1)\} a_1^{2-\frac{2}{k-1}} / N^{1-2/k},$$
$$\text{or} \quad a_1 \ll_k N^{\frac{1}{k-1}} \quad \text{and} \quad a_k - a_1 \le \{c_k + o(1)\} a_1^{\frac{2}{k-1}} / N^{1/\binom{k}{2}}.$$

Remarks. The first of the bounds in (4b) is larger if and only if $X \ge N^{1/2}$, when $k \ge 4$. When $k = 3$ they are equal. Note that if $a = a_1 \ll_k N^{1/k}$ then we can have $a_k - a_1 \ll 1$ simply by taking each $a_j = a + j$ and $N = (a+1)(a+2)\cdots(a+k)$.

Taking $k = 3$ in Theorem 3, we find that one always has $a_3 - a_1 \ge 2^{2/3} a_1 / N^{1/3}$. By making an analagous remark about the b_is, we find that the Euclidean distance between (a_1, b_1) and (a_3, b_3) is always $\gg N^{1/6}$ (however one can have two lattice points on the hyperbola a bounded distance apart, for example $(m, m+1)$ and $(m+1, m)$ when $N = m(m+1)$). We expect that by the methods of [5b] this lower bound can be improved to $\gg N^{1/4}$.

Acknowledgment.. This work is part of the second author' s Ph. D. Thesis. He would like to thank his advisor, Javier Cilleruelo, for suggesting the problem and

for his interest. The second author wishes to thank as well Andrew Granville for his invitation to work with him in the University of Georgia at Athens and University of Michigan at Ann Arbor, and for his constant encouragement during this period. Both universities were very kindly in their hospitality. Finally he would like to thank Trevor Wooley for his attention in the University of Michigan, Henryk Iwaniec for his invitation to go to Rutgers University, Fernando Chamizo for checking some calculations concerning the appendix, and Christian Ballot for remembering some properties of the resultant.

2. The transfinite diameter of $[0,1]$

The *transfinite diameter* of the interval $[0,1]$ is defined as

$$D = \lim_{k\to\infty} \max \prod_{i<j} (\delta_j - \delta_i)^{2/k(k-1)},$$

and it is known that $D = 1/4$ (see [6] and chapter 11 of [13] and [17]). This also follows from Proposition 1 and Stirling's formula.

The proof of Proposition 1. Let us suppose that

$$F(\delta_1, \delta_2, \cdots, \delta_k) := \prod_{1\le i<j\le k} (\delta_j - \delta_i)$$

attains its maximum in this range at $\eta_1, \eta_2, \cdots, \eta_k$. Define

$$H(x) := \prod_{i=1}^{k} (x - \eta_i).$$

so that our maximum equals $\Delta(H)$, the discriminant of H. ($H(x)$ is a certain *Jacobi polynomial*, and its roots are known as the *Fekete numbers of order* k.)

First note that $\eta_1 = 0$ and $\eta_k = 1$, else $\eta_k - \eta_1 < 1$ and so taking $\delta_i := (\eta_i - \eta_1)/(\eta_k - \eta_1)$ we have $\delta_j - \delta_i = (\eta_j - \eta_i)/(\eta_k - \eta_1) > \eta_j - \eta_i$ implying that $F(\delta_1, \cdots, \delta_k) > F(\eta_1, \cdots, \eta_k)$, a contradiction.

F is differentiable function, and so attains its maximum in the closed set $0 \le \delta_2 \le \cdots \le \delta_{k-1} \le 1$ (evidently $\eta_i \ne \eta_j$ else $F = 0$). Therefore the maximum occurs at a critical point, so for $2 \le i \le k-1$ we have

$$0 = \frac{1}{F}\frac{\partial F}{\partial \delta_i}(\eta_2, \cdots, \eta_{k-1}) = \sum_{j\ne i} \frac{1}{\eta_i - \eta_j} = \frac{1}{2}\frac{H''(\eta_i)}{H'(\eta_i)},$$

and thus $H''(\eta_i) = 0$. Since $H''(x)$ is a polynomial of degree $k-2$, its roots are exactly $\eta_2, \eta_3, \cdots, \eta_{k-1}$, which are exactly the roots of $H(x)$, other than 0 and 1. Therefore $x(x-1)H''(x) = CH(x)$ for some constant C: Since H is monic of degree k, the leading coefficient of $H''(x)$ is $C = k(k-1)$, and so

$$x(x-1)H''(x) = k(k-1)H(x). \tag{5}$$

(This equation can be used to show that the roots of H are symmetric about $1/2$.)

By comparing coefficients of both sides in (5), we find that

$$H(x) = \sum_{j=1}^{k} (-1)^{k-j} \frac{\binom{k}{j}\binom{k-1}{j-1}}{\binom{2k-2}{k-j}} x^j.$$

which may be verified by substituting into (5).

Given polynomial f of degree n and polynomial g of degree $m \le n$, define $R(f,g)$ to be the absolute value of the resultant of f and g. To determine $\Delta(H)$, we will use the fact that $\Delta(H)^2 = R(H,H')$. We need several facts about resultants (see [11]); for example, $R(f,cg) = c^n R(f,g)$ for any constant c. Also, if g has leading coefficient b, and $h \equiv f \pmod g$ where h has degree $r \le n$, then $R(f,g) = b^{n-r}R(g,h)$.

We will define a sequence of polynomials $H_{2k} = H(x), H_{2k-1} = H'(x)$ and

$$H_{2m-i+1} = (-1)^{k-1} \frac{(k-1)!(m)^i}{\binom{2k-2}{k} m!} \sum_{j=i}^{m} (-1)^{i-j} \binom{m+j-i}{m-j} \binom{2j-i}{j} x^j$$

for $0 \le 2m-i+1 \le 2k-2$, where $i = 0$ or 1, and m is an integer. By comparing coefficients one shows that these polynomials satisfy

$$\begin{aligned} H_{2k-2} &= kH_{2k} - xH_{2k-1}, \\ H_{2k-3} &= H_{2k-1} + 2H_{2k-2}, \\ H_{2k-4} &= (k-1)H_{2k-2} - (2k-3)xH_{2k-3}, \quad \text{and} \\ H_{2m-i-1} &= mH_{2m-i+1} + (-1)^i 2^{1-i}(2m-1)^i H_{2m-i}x^i \end{aligned}$$

for $i = 0$ or 1, and $1 \le m \le k-3$. We will write these relationships as $H_{l-2} = \beta_l H_l + \gamma_l H_{l-1}$ where $\beta_l = [l/2]$ except for $\beta_{2k-1} = 1$. Note also that the degree of H_l is $[l/2]$, and write A_l for the leading coefficient of H_l. Therefore

$$R(H_{l+1}, H_l) = A_l \beta_{l+1}^{-[l/2]} R(H_l, H_{l-1}),$$

for each $l \ge 1$, and since $R(H_2, H_1) = (k-1)!/\binom{2k-2}{k}$, we deduce that

$$\begin{aligned} \Delta^2(H) = R(H_{2k}, H_{2k-1}) &= \frac{(k-1)!}{\binom{2k-2}{k}} \prod_{l=2}^{2k-1} A_l \prod_{j=2}^{k} (\beta_{2j}\beta_{2j-1})^{-(j-1)} \\ &= \frac{(k-1)^k (k-1)! \prod_{m=1}^{k-1} \binom{2m}{m}^2}{(2k)^{k-1} \binom{2k-2}{k}^{2k-1}} \end{aligned}$$

which gives our result after some re-arrangement.

3. Combinatorial number theory

Our next objective is to prove Proposition 2. To do this we first prove the following well-known result, giving a proof which arose in discussion with Konyagin:

Lemma 1. *For any set of integers $b_1, b_2, \cdots, b_n$, we have that $\prod_{m\le n-1} m! = \prod_{1\le i<j\le n}(j-i)$ divides $\prod_{1\le i<j\le n}(b_j - b_i)$.*

Proof. Let D be the determinant of the n-by-n matrix with (i,j)th entry $\binom{b_j}{i-1}$. Each entry of this matrix is an integer, and so D is an integer (as can be seen from expanding minors to compute D). The entries of the ith row of the matrix are all the same polynomial of degree $i-1$ in b_j; thus we can subtract appropriate rational multiples of rows $1, 2, \ldots, I-1$ from the Ith row (these rational multiples being independent of the b_j) to get a matrix with the same determinant, but whose (i,j)th entry is $b_j^{i-1}/(i-1)!$. Multiplying through the i row by $(i-1)!$ we are left with a Vandermonde matrix whose determinant is $D\prod_{i\le n}(i-1)! = \prod_{1\le i<j\le n}(b_j - b_i)$. The result follows from this equation.

Proof of Proposition 2. Define $v_p(r)$ to be the exact power of prime p which divides integer r, and let $v_p(r/s) = v_p(r) - v_p(s)$.

For a given prime p select $\ell = \ell_p$ so that $v_p(a_\ell)$ is maximal. By definition $v_p(a_\ell) = v_p(\mathrm{LCM}[a_1, \cdots, a_k])$. Moreover if $i \ne \ell$ then $v_p(a_\ell - a_i) \ge v_p(a_i)$, and so

$$v_p\left(\frac{\mathrm{LCM}[a_1,\cdots,a_k]}{a_\ell}\cdot\prod_{\substack{1\le i\le k\\ i\ne\ell}}\frac{(a_\ell - a_i)}{a_i}\right)\ge 0.$$

Taking $\{b_1, \cdots, b_{k-1}\} = \{a_i : \ i \ne \ell\}$ in Lemma 1, we see that

$$v_p\left(\prod_{\substack{1\le i<j\le k\\ i,j\ne\ell}}(a_j - a_i)\right)\ge v_p\left(\prod_{m\le k-2} m!\right).$$

Adding these two results we find that $v_p(\Lambda_2) \ge v_p(\prod_{m\le k-2} m!)$ for all primes p, and so the result follows.

4a. Proposition 2 is "best possible"

Given $k \ge 2$, let $P := \mathrm{LCM}[1, \cdots, k]$ and $\alpha_1 = 0$. We shall select $0 < \alpha_2 < \alpha_3 < \cdots < \alpha_k$, then determine a large positive integer z, and finally take each $a_i = z + \alpha_i$. So, given $\alpha_1, \alpha_2, \ldots, \alpha_{r-1}$, let Q be the set of primes $> k$ which divide $\prod_{1\le i<j\le r-1}(\alpha_j - \alpha_i)$, and define $\omega(p)$ to be the number of distinct residue classes of $\alpha_1, \alpha_2, \ldots, \alpha_{r-1} \pmod p$ for each $p \in Q$.

The sieve of Eratosthenes-Legendre gives that for any y and N, the number of integers α in the range $y < \alpha \le y + NP^2$ for which $\alpha \equiv r-1 \pmod{P^2}$, and $\alpha \not\equiv \alpha_1, \alpha_2, \ldots, \alpha_{r-1} \pmod p$ for any prime $p \in Q$ is

$$N\prod_{p\in Q}\left(1-\frac{\omega(p)}{p}\right) + O(r^{|Q|}) \gg \frac{N}{\log^r |Q|} + O(r^{|Q|}). \tag{6}$$

We take $y = \alpha_{r-1}$ here, and see that for sufficiently large N, there must exist such an integer α, which we denote α_r.

After we have determined $\alpha_1, \alpha_2, \dots, \alpha_k$ we let z be a positive integer for which $z \equiv 0 \pmod{P^2}$, and $z \equiv -\alpha_j \pmod{p^s}$ for any prime power p^s dividing $\alpha_j - \alpha_i$ with $p > k$, for any $1 \le i < j \le k$. We claim that such an integer exists, by the Chinese Remainder Theorem, since any common prime divisors of $\alpha_j - \alpha_i$ and $\alpha_J - \alpha_I$, with $\{i,j\} \ne \{I,J\}$, must be $\le k$, by construction.

Since each $a_i \equiv i - 1 \pmod{P^2}$, it is easy to show that for any prime $p \le k$ we have $v_p(\Lambda_2) = v_p(\prod_{m \le k-2} m!)$. On the other hand if prime $p > k$ divides some difference $a_j - a_i = \alpha_j - \alpha_i$ then this pair is unique by our construction. Also $a_i \equiv a_j = z + \alpha_j \equiv 0 \pmod{p^s}$, where p^s is the exact power of p dividing $a_j - a_i$. Thus

$$v_p(\Lambda_2) = v_p(\mathrm{LCM}[a_i, a_j]) + v_p(a_i - a_j) - v_p(a_i) - v_p(a_j) = 0.$$

Therefore, this construction gives examples with $\Lambda_2(a_1, \cdots, a_k) = \prod_{m \le k-2} m!$.

4b. Proof of Theorem 2

We proceed, more-or-less, with the construction above, though we change the range in which we look for our α_i. In particular, given L, we select α_i, for each $i \ge 2$ to be the largest number $< \eta_i L - 2\sqrt{L}$ which satisfies the given congruences.

Each $\alpha_j - \alpha_i$ is $\le L$, and so has $\ll \log L / \log\log L$ prime factors. Taking $N = \sqrt{L}$, we find that (6) is $\gg N/(\log\log L)^k - L^{O(1/\log\log L)} > 0$, and so we can find α_i in the interval $[\eta_i L - 2\sqrt{L}, \eta_i L - \sqrt{L}]$. Therefore Λ_1, and thus Λ, is within $1 + O(1/\sqrt{L})$ of the maximum possible (since the above construction gives $\Lambda_2 = \prod_{m \le k-2} m!$).

Finally we take z satisfying all the given congruences. The modulus for these congruences is $\ll_k L^{\binom{k}{2}}$, so guarantee finding such an $X (= a_1)$, with $X \ll_k L^{\binom{k}{2}}$.

4c. A construction with polynomials

Consider the integers $b_j = 2kj^3 + j^2$ for $j \le k$ which verify that $(b_j - b_i)/(j - i)$ are all different. We will take $a_j = a_1 + (j-1) + P^2 b_j t$ (where P is as above). Thus each $a_j - a_i$ equals $j - i + P^2(b_j - b_i)t$, and these polynomials are all distinct by our choices of the b_j. Select polynomial a_1 of minimal degree satisfying $a_1 \equiv -((j-1) + P^2 b_j t) \pmod{j - i + P^2(b_j - b_i)t}$ in $\mathbb{Z}[t]$ for all $1 \le i < j \le k$. As $t \to \infty$ running through integer values, one finds that $\mathrm{lcm} \sim \tau_k a_1^k / t^{\binom{k}{2}}$ for some constant τ_k, justifying the remarks made shortly before the statement of Theorem 3.

5. Asymptotics for C_k.

The estimate (3) for the asymptotic behaviour of the constant C_k defined in (2) is easily deduced from the estimate

$$\prod_{m=1}^{l-1} m! = \eta^{1/2} \left(\sqrt{2\pi}\right)^l \left(e^{-3/2} l\right)^{l^2/2 - 1/12} e^{O(1/l)}, \tag{7}$$

where $\eta := \sqrt{2\pi} \exp(-23/12 + \gamma/3 + \sum_{j \ge 2} (\zeta(j) - 1)/(j+2))$, by noting that $\prod_{m=1}^{l} (2m)!^2 = 2^l l! \prod_{m=1}^{2l} m!$ (since $(2m)! = 2m(2m-1)!$), and using Stirling's formula, $m! = \sqrt{2\pi m}(m/e)^m e^{1/12m + O(1/m^2)}$, and the estimate $(k-1)^k = k^k e^{-1 + O(1/k)}$.

To establish (7) take $f(x) = x^2/2$ in the identity

$$l^{f(l)} \prod_{m=1}^{l-1} m^{f(m)-f(m+1)} = \prod_{m=2}^{l} \left(\frac{m}{m-1}\right)^{f(m)},$$

so that $f(m) - f(m+1) = -m - 1/2$, to obtain

$$\begin{aligned} \prod_{m=2}^{l} \left(\frac{m}{m-1}\right)^{m^2/2} &= l^{l^2/2} \prod_{m=1}^{l-1} m^{-m-1/2} \\ &= \frac{l^{l^2/2}}{(l-1)!^{l+1/2}} \prod_{m=1}^{l-1} m^{l-m} = \frac{l^{(l+1)^2/2}}{l!^{l+1/2}} \prod_{m=1}^{l-1} m! \end{aligned} \tag{8}$$

Now

$$\sum_{m=2}^{l} m^2 \log\left(\frac{m}{m-1}\right) = -\sum_{m=2}^{l} m^2 \log\left(1 - \frac{1}{m}\right) = \sum_{m=2}^{l} m^2 \sum_{j\geq 1} \frac{1}{j m^j},$$

$$\sum_{m=2}^{l} \frac{1}{m} = \log l + \gamma - 1 + O\left(\frac{1}{l}\right),$$

and $\sum_{j\geq 4} \sum_{m\geq l+1} 1/jm^{j-2} \ll \sum_{m>l} 1/m^2 \ll 1$. Thus exponentiating gives

$$\prod_{m=2}^{l} \left(\frac{m}{m-1}\right)^{m^2} = l^{1/3} \exp\left(l^2/2 + l - 11/6 + \gamma/3 + \sum_{j\geq 2} \frac{\zeta(j)-1}{j+2} + O\left(\frac{1}{l}\right)\right).$$

Combining this with (8) gives (7), using Stirling's formula.

References

1. J. Cilleruelo, *Arcs containing no three lattice points*, Acta Arith. **LIX.1** (1991), 87–90.
2. J. Cilleruelo and A. Córdoba, *Trigonometric Polynomials and Lattice Points*, Proc. of Amer. Math. Soc. **115.4** (1992), 899–905.
3. J. Cilleruelo and A. Córdoba, *Lattice Points on Ellipses*, Duke Math. Jour. **76.3** (1994), 741–750.
4. J. Cilleruelo and J. Jiménez-Urroz, *Lattice points on Hyperbolas*, Jour. Num. Theor. **63, 2** (1997), 267–274.
5. H. M. Edwards, *Riemanns Zeta Function*, Pure and Applied Math. 58 Academic Press, New York, 1974.

5b. P. Erdős and M. Rosenfeld, Acta Arithm. **79** (1997), 353–359.

6. G. Faber, *Tschebyscheffsche Polynome*, Jour. für die reine und ange. Math. **150** (1919), 79–106.
7. M. Fekete, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Z. **17** (1923), 228–249.
8. G. Grekos, *Sur le nombre de points entiers dune courbe convexe*, Bull. Sc. math. 2^e série **112** (1988), 235–254.
9. G. H. Hardy and E.M. Wright, *Introduction to the theory of numbers, 4th ed.*, Clarendon Press, Oxford, 1960.

10. D. Hilbert, *Über die Diskriminante der im Endlichen abbrechenden hypergeometrischen Reihe*, Jour. für die reine und ange. Mathe. **103** (1888), 337–345.
11. S. Lang, *Algebra*, Addison-Wesley: Reading, Massachusets, 1965.
12. H. W. Lenstra, Jr., *Divisors in residue classes*, Math. of Comp. **42. 165** (1984), 331–340.
13. Chr. Pommerenke, *Univalent Functions*, Vandenhoeck & Ruprecht, Göttingen. Studia Mathematica Bd **xxv**, 1975.
14. T. Popoviciu, *Sur certains problémes de maximum de Stieltjes*, Bull. math. Soc. Roum. Sci. **38** (1936), 73–96.
15. I. Schur, *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome*, Jour. für die reine und ange. Mathe. **165** (1931), 52–58.
16. T.J. Stieltjes, *Ouvres Completes*, Vol 1, 440–444.
17. G. Szegö, *Orthogonal Polynimials* (1939), jour Amer. Math. Soc. 23, Providence, Rhode Island.

Department of Mathematics, University of Georgia, Athens, Georgia 30602, USA
E-mail address: andrew@math.uga.edu

Departamento de Matemáticas, Facultad de Ciencias, Universidad Autónoma de Madrid, 28049 Madrid, España
E-mail address: jorge.jimenez@uam.es