Dear Professor X,

Recently I came across your interesting paper with Y and Z "On Bohr's inequality", ***, (3) **85** (2002), 493–512.

In 1962 I wrote a little paper "Sopra un teorema di H. Bohr and G. Ricci sulle funzioni maggioranti delle serie di potenze", *Boll. Unione Matematica Italiana*, (III), **17** (1962), 276–282, on theorems like Bohr's on majorants of power series in one variable. Since this paper is published in a foreign language in an obscure journal I summarize it briefly here, in the hope you may find it useful.

One considers power series $f(z) = \sum_{n=0}^{\infty} a_n z^n$ in the unit disk $|z| \leq 1$ with bounded norm $\|f\|_\infty \leq 1$ there, and in particular the subclass $F_0(\lambda)$ of functions with $f(0) = \lambda$. One wants to study the majorant series $\mathcal{M}(f,r) = \sum_{n=0}^{\infty} |a_n| r^n$. Without loss of generality we may restrict our attention to $0 \leq \lambda < 1$. Let $B(\lambda,\sigma)$ be the largest r for which $\mathcal{M}(f,r) \leq \sigma$ for $f \in F_0(\lambda)$, and define $B(\sigma) = \inf_\lambda B(\lambda,\sigma)$.

THEOREM. *If $\lambda < \sigma \leq 2\lambda$ we have*

$$B(\lambda,\sigma) = \frac{\sigma - \lambda}{1 + \sigma\lambda - 2\lambda^2}$$

and for $\lambda < \sigma \leq 2\lambda$ the extremal functions are $f(z) = (\lambda - e^{i\phi}z)/(1 - \lambda e^{i\phi}z)$.

If instead $\sigma \geq 2\lambda$ then

$$B(\lambda,\sigma) \geq \frac{\sigma - \lambda}{\sqrt{\sigma^2 - 2\lambda\sigma + 1}}.$$

Finally, if $1 \leq \sigma \leq \sqrt{2}$ we have

$$B(\sigma) = \frac{1}{3\sigma - 2\sqrt{2(\sigma^2 - 1)}}$$

and if $\sigma \geq \sqrt{2}$ we have

$$B(\sigma) \geq \frac{\sqrt{\sigma^2 - 1}}{\sigma}.$$

COROLLARY. *For f regular in $|z| \leq 1$ and $r \in [\frac{1}{3}, \frac{1}{\sqrt{2}}]$ we have*

$$\mathcal{M}(f,r) \leq \frac{3 - \sqrt{8(1 - r^2)}}{r} \|f\|_\infty$$

and this inequality is sharp.

This solves the problem raised in your Remark 1 if $r \in [\frac{1}{3}, \frac{1}{\sqrt{2}}]$. If $r \in [\frac{1}{\sqrt{2}}, 1]$ I get the same constant $1/\sqrt{1-r^2}$ as you do, which I don't think is optimal.

A related problem, studied originally by Giovanni Ricci in 1955 in another obscure paper (G. Ricci, "Complementi a un teorema di H. Bohr riguardante le serie di potenze", *Revista de la Union Matematica Argentina y de la Asociacion Fisica Argentina* **17** (1955), 185–195), is to consider the similar quantities $B_h(\lambda, \sigma)$ associated to functions $f(z) = \lambda z^h + \dots$ which have a zero of order h at the origin and again satisfy $|f(z)| \leq 1$.

Let us write for simplicity $B_h(\lambda)$ for $B_h(\lambda, 1)$ and $B_h = \sup_\lambda B_h(\lambda)$. Since

$$B(\lambda, B_h^{-h}(\lambda)) = B_h(\lambda),$$

one determines exactly $B_1 = 1/\sqrt{2}$ and also $B_h(\lambda)$ in the interval $2^{-1/(h+1)} \leq \lambda < 1$, for every h. Of course, $B_1 = 1/\sqrt{2}$ is the special case of Corollary 2.9 of your paper.

LEMMA 1. *Let $h(z)$ be regular in $|z| < 1$ with at least one zero there and let ζ_0 be a zero of $h(z)$ of smallest modulus $c_0 = |\zeta_0|$. Then for $c_0 < r < 1$ we have*

$$c_0 \geq r|h(0)|/\left[\frac{1}{2\pi}\int_0^{2\pi} |h(re^{i\theta})|^2\, d\theta\right]^{1/2}.$$

PROOF: (E. Landau, *Vorlesungen über Zahlentheorie*, Leipzig 1927, Satz 443) Let c_i, $i = 0, \dots, n$, be the absolute values of the zeros of $h(z)$ in $|z| < r$. By Jensen's theorem we have

$$\log(r/c_0) \leq \sum_{i=0}^{n} \log(r/c_i) = \frac{1}{2\pi}\int_0^{2\pi} \log|h(re^{i\theta})|\, d\theta - \log|h(0)|$$

and the result follows from a well-known convexity inequality, again due to Jensen. QED

LEMMA 2.

$$B(\lambda, \sigma) \geq \max_{r \leq 1} \min\left(r; (\sigma - \lambda)r/\left[\sup \frac{1}{2\pi}\int_0^{2\pi} |f(re^{i\theta})|^2\, d\theta + \sigma^2 - 2\lambda\sigma\right]^{1/2}\right)$$

where the supremum is taken over the functions $f \in F_0(\lambda)$.

PROOF: Let $f(z) = \lambda + a_1 z + \dots$ and $g(z) = \lambda + |a_1| z + \dots$. Then $B(\lambda, \sigma)$ is the infimum of c for which $g(c) = \sigma$, as f varies in $F_0(\lambda)$. Consider the function $h(z) = g(z) - \sigma$. Since the coefficients of $g(z)$ are all non negative, we have $|g(z)| < \sigma$ for $|z| < c$, hence c is the smallest modulus of a zero of $h(z)$ in $|z| < 1$. Thus we may apply LEMMA 1 to $h(z)$ and get for $c < r < 1$:

$$c \geq (\sigma - \lambda)r/\left[\frac{1}{2\pi}\int_0^{2\pi} |h(re^{i\theta})|^2\, d\theta\right]^{1/2}.$$

On the other hand,

$$\frac{1}{2\pi}\int_0^{2\pi} |h(re^{i\theta})|^2\,d\theta = (\sigma-\lambda)^2 + |a_1|^2r^2 + \ldots = \sigma^2 - 2\lambda\sigma + \frac{1}{2\pi}\int_0^{2\pi} |f(re^{i\theta})|^2\,d\theta.$$

If $c < r < 1$ is not verified we still get $c \geq r$. QED

LEMMA 3. *If $f \in F_0(\lambda)$ we have*

$$\frac{1}{2\pi}\int_0^{2\pi} |f(re^{i\theta})|^2\,d\theta \leq \frac{r^2+\lambda^2-2r^2\lambda^2}{1-r^2\lambda^2}$$

with equality if and only if $f(z) = (\lambda - e^{i\phi}z)/(1-\lambda e^{i\phi}z)$.

PROOF: We may assume that $f(0) = \lambda$. The function $s(z) = (\lambda - f(z))/(1-\lambda f(z))$ is regular in the unit disk and satisfies $|s(z)| \leq 1$ there. Since $s(0) = 0$, Schwarz's lemma shows that $|s(z)| \leq |z|$, hence $|f(re^{i\theta}) - \lambda| \leq r\,|1 - \lambda f(re^{i\theta})|$. Setting

$$I = \frac{1}{2\pi}\int_0^{2\pi} |f(re^{i\theta})|^2\,d\theta$$

we verify that

$$\frac{1}{2\pi}\int_0^{2\pi} |f(re^{i\theta}) - \lambda|^2\,d\theta = |a_1|^2r^2 + \ldots = I - \lambda^2$$

and in the same way

$$\frac{1}{2\pi}\int_0^{2\pi} |1 - \lambda f(re^{i\theta})|^2\,d\theta = 1 - 2\lambda^2 + \lambda^2 I.$$

The lemma now follows from $|f(re^{i\theta}) - \lambda| \leq r\,|1 - \lambda f(re^{i\theta})|$. QED

PROOF OF THEOREM: Immediate from LEMMA 2 and LEMMA 3, taking $r^2 = (\sigma-\lambda)/(\lambda + \lambda^2\sigma - 2\lambda^3)$ if $\sigma/2 < \lambda < \sigma$, $r = 1$ if $\lambda \leq \sigma/2$, for a lower bound. For the upper bound, we take as usual $f(z) = (\lambda - z)/(1-\lambda z)$. QED

These are the only exact constants I know for this problem.

Sincerely,

Enrico Bombieri

A REMARK ON BOHR'S INEQUALITY

E. BOMBIERI and J. BOURGAIN

I. INTRODUCTION

Let us consider bounded holomorphic functions $f(z) = \sum a_n z^n$ in the unit disk $|z| < 1$, with associated norm $\|f\|_\infty$, and let $\mathcal{M}(f,r) = \sum |a_n| r^n$ be the associated majorant series. A classical result of H. Bohr states that

$$\mathcal{M}(f, \frac{1}{3}) \leq \|f\|_\infty .$$

The constant $\frac{1}{3}$ is sharp. More generally, one defines

$$m(r) = \sup \{\mathcal{M}(f,r)/\|f\|_\infty\}$$

where the supremum is taken over all such $f \not\equiv 0$. We note here the exact value $m(r) = (3 - \sqrt{8(1-r^2)})/r$ in the range $[\frac{1}{3}, \frac{1}{\sqrt{2}}]$, proved in [2] (stated for the inverse function of $m(r)$). Further results on this and related topics can be found in the recent paper [13] by Paulsen, Popescu and Singh.

The object of this paper is to study the behaviour of $m(r)$ as $r \to 1$. The inequality

$$m(r) \leq \frac{1}{\sqrt{1-r^2}}$$

is an immediate consequence of Cauchy's inequality, as was pointed out in a letter of E. Landau to G.H. Hardy of 23 February 1913, see [5], p.77. On the other hand, the question of finding the order of $m(r)$ as $r \to 1$ turns out to be not entirely trivial. Hardy and Littlewood [6], pp.219–220, noted that the function $g(z) = \sum e^{n^2 \pi i \xi} z^n$, with ξ any irrational number with bounded partial quotients in its continued fraction, is $\ll (1-r)^{-\frac{1}{2}}$ on $|z| = r$. Thus the true order magnitude of $m(r)$ is $(1-r)^{-\frac{1}{2}}$. Our first result is

THEOREM 1. *If $r > 1/\sqrt{2}$ we have $m(r) < 1/\sqrt{1-r^2}$.*

This answers a question raised in [13]. We also get a lower bound

THEOREM 2. *Let $\varepsilon > 0$. Then for some positive constant $C(\varepsilon) > 0$ we have as $r \to 1$ the lower bound*

$$m(r) \geq \frac{1}{\sqrt{1-r^2}} - C(\varepsilon)\left(\log \frac{1}{1-r}\right)^{\frac{3}{2}+\varepsilon}.$$

Problems in the same circle of ideas but for polynomials have been studied for some time. The strongest result is due to J.-P. Kahane [10], with the construction of the so-called "ultraflat" polynomials, namely polynomials $p_n(z) = \sum a_j z^j$ of degree n with $|a_j| = 1$ for every j and such that $|p_n(e^{2\pi i\theta})| \sim \sqrt{n}$ as $n \to \infty$, uniformly in θ. This is quite a delicate result to prove, due to the stringent condition imposed on the coefficients and on the polynomial. An easier problem is to show that there exists a polynomial p_n of degree n such that $|p_n(e^{2\pi i\theta})| \lesssim \sqrt{n}$ and $\sum |a_j| \sim n$. Results in this direction and solutions were obtained by J.E. Littlewood [11], D.J. Newman [12], Beller and Newman [1], J.S. Byrnes [3], the sharpest being J.-P. Kahane's Proposition 1 in [10], which would correspond to an error term $O((1-r)^{-\frac{1}{6}})$ in our theorem. Anyway, these results motivated our conjecture that $m(r) \sim 1/\sqrt{1-r^2}$.

II. PROOF OF THEOREM 1

We begin by noting that an extremal function f for which $\mathcal{M}(f,r) = m(r)\,\|f\|_\infty$ exists, because the functions with $\|f\|_\infty \leq 1$ form a normal family in Montel's sense (use for example Hayman [7], Th.6.5, p.163).

Hence let $f(z) = \sum a_n z^n$ be an extremal for this problem. Landau's argument for $m(r) \leq 1/\sqrt{1-r^2}$ is quite simple:

$$\begin{aligned}\mathcal{M}(f,r) &= \sum |a_n|\, r^n \leq \sqrt{\sum |a_n|^2}\,\sqrt{\sum r^{2n}} \\ &= \frac{\|f\|_2}{\sqrt{1-r^2}} \leq \frac{\|f\|_\infty}{\sqrt{1-r^2}}.\end{aligned}$$

If equality holds we need $|a_n|$ proportional to r^n and also $\|f\|_2 = \|f\|_\infty$. Therefore, we may assume $|f(e^{2\pi i\theta})| = 1$ and we must have $|a_n| = r^n\sqrt{1-r^2}$.

as wanted. However, in order to complete the proof we still have to take care of the possibility that $h > b$ or $h > -a$. This can be done by extending $F(x)$ beyond $[a, b]$ to a new function $\widetilde{F}$ in $\widetilde{I} = [a, b] \cup [-h, h]$. For example, if $h > b$ we set

$$\widetilde{F}(x) = \sum_{j=0}^{3} \frac{F^{(j)}(b)}{j!} (x - b)^j \qquad \text{for} \quad b < x \leq h.$$

The argument above applies to $\widetilde{F}$, because the bound for $|\widetilde{F}^{(3)}(x)|$ is still m and because $\widetilde{F}''(x) \neq 0$ remains valid as long as $h < 1/m$, which we were assuming during the course of the proof. The correction introduced in the integral is handled using Lemma A, obtaining a bound $\ll 1/|F'(b)|$. Q.E.D.

IV. Auxiliary Lemmas

In analogy with the Littlewood or Kahane polynomials, we start by constructing a bounded function $g(z) = \sum b_n z^n$ such that $|b_n| = r^n$ and try to adjust the phases $\Phi(n)$ of the coefficients $b_n = r^n e^{2\pi i \Phi(n)}$ so that $|g(e^{2\pi i\theta})|$ is as small as possible for θ outside a small set. To achieve this we use Poisson's summation to transform the sum into a sum of oscillatory integrals, evaluated by the method of stationary phase. Early tries showed that a choice of the phase Φ in direct analogy with the quadratic phases occurring in the case of polynomials did not work optimally here and the problem shifted on finding the correct phase to use.

The following discussion motivates our choice of Φ. We expect $|g(e^{2\pi i\theta})|$ to be nearly constant for an optimal function g, hence only one oscillatory integral should have stationary phase, occurring at only one point. This remark almost determines $\Phi(n)$, as we shall see in a moment.

We fix a smooth increasing positive function $\chi(x)$ such that $\chi(x) = 0$ for $x < 0$, $\chi(x) = 1$ for $x > 1$ and apply Poisson's summation to $\sum \chi(n) r^n e^{2\pi i(\Phi(n) + \theta n)}$, getting

$$g(e^{2\pi i\theta}) - 1 = \sum_{k=-\infty}^{\infty} \int_0^{\infty} \chi(x) r^x e(\Phi(x) + (\theta - k)x)\, dx\,. \tag{6}$$

The stationary phase equation is

$$\Phi'(x) = k - \theta$$

and we want this to have at most one solution (k, x) for any given θ. Thus the function $\Phi'(x)$ must be monotonic and its range must be contained in an interval of length 1. This condition is met if $\Phi'(x)$ is decreasing and $\Phi'(0) = 1$, $\Phi'(\infty) = 0$, ensuring that the equation $\Phi'(x) = k - \theta$, $\theta \neq 0$, is soluble only in the two cases

$$k = 0 \quad \text{if} \quad -\frac{1}{2} \leq \theta < 0, \qquad k = 1 \quad \text{if} \quad 0 < \theta \leq \frac{1}{2}. \tag{7}$$

If $x_k > 0$ is the solution, the corresponding integral is

$$\frac{\chi(x_k) r^{x_k}}{\sqrt{|\Phi''(x_k)|}} e^{2\pi i(\Phi(x_k) + (\theta - k)x_k \pm \frac{1}{8})} + \text{error term}, \tag{8}$$

with $\pm = \operatorname{sign} \Phi''(x_k)$.

A reasonable candidate for the function $\Phi(x)$ can be guessed as follows. Since we want $|g(e^{2\pi i\theta})| \sim const./\sqrt{1-r}$ on most of the unit circle, equations (6) and (8) give

$$|\Phi''(x_k)| \sim const. \times r^{2x_k};$$

the value of the constant is determined by $\Phi'(0) = 1$. Therefore, we choose

$$\Phi(x) = \frac{r^{2x}}{2 \log r}. \tag{9}$$

LEMMA 1. *Let $k = 0$ or 1, $\xi_k = \theta - k$, $t = 1/|\log r|$, and*

$$\Phi_k = \frac{t}{2} \{|\xi_k| \log |\xi_k| - |\xi_k|\}.$$

Then

$$g(e^{2\pi i\theta}) = e^{-\frac{\pi i}{4}} \sqrt{\frac{t}{2}}\, e(\Phi_k) + O\left(\frac{1}{|\theta|}\right)$$

with $k = 0$ if $\theta < 0$ and $k = 1$ if $\theta > 0$.

Moreover, we always have $g(e^{2\pi i\theta}) \ll 1/\sqrt{1-r}$.

PROOF: The estimation of the integrals in the right-hand side of equation (6) is routine but we give it here for completeness. The integrals for $k \neq 0, 1$ are $O(1/k^2)$ uniformly in θ for $|\theta| \leq \frac{1}{2}$, as one sees integrating by parts twice. Hence their

the integrals over $[0,a]$ and $[b,1]$ trivially by $1/\sqrt{t}$. Q.E.D.

V. A First Bound

In this section we give a simple argument to deduce a lower bound for $m(r)$ from Lemma 1. This is not as sharp as what is stated in Theorem 2, the proof of which requires substantial modifications to the original construction of $g(z)$ and which will be the object of the subsequent sections. The result obtained here is

$$m(r) = \frac{1}{\sqrt{1-r^2}} + O\left(\frac{1}{\sqrt[4]{1-r}}\right). \tag{10}$$

Proof of (10): The bound for $g(e^{2\pi i\theta})$ in Lemma 1 is good unless θ is small. So we modify $g(z)$ by multiplying it by a function close to 1 on most of $|z|=1$ and small otherwise.

We write g for $g(e^{2\pi i\theta})$ and similarly for f and W. Let us define the outer function $W(z)$ so that on $|z|=1$ it is given by

$$W = \exp\left\{ -\log^+\left(\sqrt{1-r^2}\,|g|\right) - i\,\mathcal{H}\left[\log^+\left(\sqrt{1-r^2}\,|g|\right)\right] \right\}$$

where $\mathcal{H}$ denotes the periodic Hilbert transform defined by

$$\mathcal{H}(e(n\theta)) = \begin{cases} \frac{1}{i}\,\mathrm{sign}(n)\,e(n\theta) & \text{if} \quad n \neq 0 \\ 0 & \text{if} \quad n = 0. \end{cases}$$

Thus

$$f = g\,W$$

satisfies

$$|f| \leq |g| \,\min\left(1, \frac{1}{\sqrt{1-r^2}\,|g|}\right) \leq \frac{1}{\sqrt{1-r^2}}\,. \tag{11}$$

Also, using the fact that the Hilbert transform is a bounded operator in L^2, we have

$$\|f-g\|_2 \leq \|g\|_\infty \,\|1-W\|_2 \ll \frac{1}{\sqrt{1-r}}\,\left\|\log^+\left(\sqrt{1-r^2}\,|g|\right)\right\|_2\,. \tag{12}$$

By Lemma 1,

$$\sqrt{1-r^2}\,|g| \le 1 + O\left(\frac{\sqrt{1-r}}{|\theta|}\right) \tag{13}$$

and in any case $\sqrt{1-r^2}\,|g| = O(1)$. Therefore,

$$\left\|\log^+\left(\sqrt{1-r^2}\,|g|\right)\right\|_2 \ll \left\|\min\left(1, \frac{\sqrt{1-r}}{|\theta|}\right)\right\|_2 \ll \sqrt[4]{1-r}\,.$$

By (12), this implies

$$\|f-g\|_2 \ll \frac{1}{\sqrt[4]{1-r}}\,. \tag{14}$$

Let $f(z) = \sum a_n z^n$. By (14) and recalling that $|b_n| = r^n$ for every n, we have

$$\begin{aligned} m(r)\,\|f\|_\infty &\ge \mathcal{M}(f,r) \\ &= \sum |a_n| r^n \ge \sum |b_n| r^n - \sum |b_n - a_n| r^n \\ &\ge \frac{1}{1-r^2} - \Big\{\sum |b_n - a_n|^2\Big\}^{\frac{1}{2}} (1-r^2)^{-\frac{1}{2}} \\ &= \frac{1}{1-r^2} - \|f-g\|_2\,(1-r^2)^{-\frac{1}{2}} \\ &\ge \frac{1}{1-r^2}\,\left\{1 - O(\sqrt[4]{1-r})\right\}. \end{aligned} \tag{15}$$

The desired bound now follows from (11). Q.E.D.

VI. A Refinement: First Steps

The error term $O((1-r)^{-\frac{1}{4}})$ arises from the error term $O(1/|\theta|)$ in Lemma 1. An examination of the proof shows that this error term comes exclusively from the evaluation of the integral with $k = 1$, while the error term arising from the integral with $k = 0$ is only $O(1/\sqrt{|\theta|})$. It turns out that we may improve the first error term by truncating and smoothing the series defining $g(z)$.

We repeat the preceding argument keeping the same phase $\Phi(x)$ but with the new function

$$g(z,\alpha) = \sum_{n=1}^{\infty} r^n \chi_\alpha(r^n)\, e(\Phi(n))\, z^n$$

On a conjecture of Borisov

Enrico Bombieri and Jean Bourgain

Abstract: This paper settles a conjecture of A. Borisov on linear combinations of the floor function.

MSC 2000: primary 42A05; secondary 42A61.

Keywords: Number theory; terminal singularities.

1. Introduction and results

Let

$$f(t) := \sum_{k=1}^{K} c_k \lfloor \nu_k x \rfloor \tag{1.1}$$

with $\nu_k > 0$ and $\nu_j \neq \nu_k$ for $j \neq k$.

The following conjecture was made by A. Borisov in [1], Conjecture 4.

Conjecture 1. *Let $f(t)$ be as in (1.1) with $1/\nu_k$ and c_k integers for all k. Suppose that $|f(t)| < a$ for all $x > 0$. Then*

$$\sum_{k=1}^{K} |c_k| < C(a) \tag{1.2}$$

where $C(a)$ is bounded solely in terms of a. □

Define

Definition 1. Set

$$\langle x \rangle := x - \lfloor x \rfloor - \frac{1}{2} \tag{1.3}$$

and, for a function $F(x)$ defined for $x > 0$, set

$$⨍ F := \lim_{T \to \infty} \frac{1}{T} \int_0^T F(t)\, \mathrm{d}t \tag{1.4}$$

provided the limit exists. □

Definition 2. Let α, β be strictly positive real numbers. We say that α divides β, and write $\alpha | \beta$, if $\beta/\alpha \in \mathbb{N}$. □

E-mail address: eb@math.ias.edu

Theorem 1. *Let*

$$g(t) = \sum_{k=1}^{K} c_k \langle \nu_k t \rangle \tag{1.5}$$

with $|c_k| \geq 1$ and distinct positive real numbers ν_k. Let λ_d, $d \in \mathbb{N}$, be real numbers such that

$$\lambda_1 = 1, \qquad \sum_{d=1}^{\infty} \frac{|\lambda_d|}{d} < \infty, \qquad \theta := \frac{\|\mathbf{c}\|^2 - 1}{2} \max_j \sum_{k<j}^{*} \frac{\left(\sum_{d|\nu_j/\nu_k} \lambda_d\right)^2}{(\nu_j/\nu_k)^2} < 1 \tag{C1}$$

where $\sum^*$ means that $\nu_k | \nu_j$. Then

$$\|\mathbf{c}\| \leq \frac{\sqrt{2}\,\pi}{1-\sqrt{\theta}} \left(\sum_{d=1}^{\infty} \frac{|\lambda_d|}{d}\right) \left(⨍ g(t)^2\right)^{\frac{1}{2}}. \quad \square \tag{1.6}$$

Corollary 1. *Let $g(t)$ be as in Theorem 1. If $|g(t)| \leq A$ for every $t > 0$, it holds*

$$K \leq \sum_{k=1}^{K} |c_k|^2 \ll \big(A \log(A+2)\big)^2 \tag{1.7}$$

where the implied constant is absolute. $\square$

2. Proofs

Lemma 1. *Let $a, b > 0$. Then*

$$⨍ \langle at \rangle \langle bt \rangle = \frac{1}{2\pi^2} \sum_{\substack{m=1 \\ am=bn}}^{\infty} \sum_{n=1}^{\infty} \frac{1}{mn}. \quad \square \tag{2.1}$$

Corollary 2. *For $g(t)$ as in Theorem 1 it holds*

$$\sum_{\xi>0} \left| \sum_{\substack{k=1 \\ m=\xi/\nu_k}}^{K} \sum_{m=1}^{\infty} \frac{c_k}{m} \right|^2 = ⨍ g(t)^2. \quad \square \tag{2.2}$$

Proof of Corollary 2. Clear from (2.1) because $am = bn$ is equivalent to $m = \xi/a$, $n = \xi/b$ for some $\xi > 0$. ■

Proof of lemma. We recall the Fourier series expansion

$$\langle x \rangle = \frac{1}{\pi} \sum_{n=1}^{\infty} \frac{\sin(2\pi n x)}{n} \tag{2.3}$$

which is uniformly convergent for $\varepsilon \le |x| \le \frac{1}{2}$ for any fixed $\varepsilon > 0$, and also we note the that the partial sums of this sum are uniformly bounded for all x.

Hence

$$\begin{aligned}\fint \langle at\rangle\langle bt\rangle &= \frac{1}{\pi^2}\lim_{M\to\infty}\sum_{m=1}^{M}\sum_{n=1}^{M}\frac{1}{mn}\fint \sin(2\pi mat)\sin(2\pi nbt)\\ &= \frac{1}{2\pi^2}\sum_{\substack{m=1\\ am=bn}}^{\infty}\sum_{n=1}^{\infty}\frac{1}{mn}. \quad \blacksquare\end{aligned} \tag{2.4}$$

Proof of Theorem 1. Let $\lambda_d \in \mathbb{R}$, $d \in \mathbb{N}$, be such that

$$\lambda_1 = 1, \qquad \sum_{d=1}^{\infty}\frac{|\lambda_d|}{d} < \infty. \tag{2.5}$$

We compute using Cauchy's inequality

$$\begin{aligned}\sum_{\xi>0}\left|\sum_{\substack{k=1\\ m=\xi/\nu_k}}^{K}\sum_{m=1}^{\infty}\left(\sum_{d|m}\lambda_d\right)\frac{c_k}{m}\right|^2 &= \sum_{\xi>0}\left|\sum_{d=1}^{\infty}\frac{\lambda_d}{d}\sum_{\substack{k=1\\ r=\xi/(d\nu_k)}}^{K}\sum_{r=1}^{\infty}\frac{c_k}{r}\right|^2\\ &\le \sum_{\xi>0}\left(\sum_{d=1}^{\infty}\frac{|\lambda_d|}{d}\right)\left(\sum_{d=1}^{\infty}\frac{|\lambda_d|}{d}\left|\sum_{\substack{k=1\\ r=\xi/(d\nu_k)}}^{K}\sum_{r=1}^{\infty}\frac{c_k}{r}\right|^2\right)\\ &= \left(\sum_{d=1}^{\infty}\frac{|\lambda_d|}{d}\right)^2 2\pi^2\fint g(t)^2\end{aligned} \tag{2.6}$$

the last step by Corollary 2 (note that $\xi > 0$ is equivalent to $\xi/d > 0$).

Let

$$\mathcal{N} = \{\nu_1, \dots, \nu_K\} \tag{2.7}$$

and let us order the numbers ν_k in increasing order.

We restrict now our attention to $\xi \in \mathcal{N}$. Then from (2.6) we have, since $\lambda_1 = 1$ and the ν_k are distinct:

$$\sum_{k=1}^{K}|c_k|^2 = \sum_{\xi\in\mathcal{N}}\left|\sum_{\substack{k=1\\ m=\xi/\nu_k}}^{K}\sum_{m=1}^{\infty}\left(\sum_{d|m}\lambda_d\right)\frac{c_k}{m} - \sum_{\substack{k=1\\ m=\xi/\nu_k}}^{K}\sum_{m>1}\left(\sum_{d|m}\lambda_d\right)\frac{c_k}{m}\right|^2. \tag{2.8}$$

In view of (2.6), it follows by Minkowski's inequality that

$$\left(\sum_{k=1}^{K}|c_k|^2\right)^{\frac{1}{2}} \le \left(\sum_{\xi\in\mathcal{N}}\left|\sum_{\substack{k=1\\ m=\xi/\nu_k}}^{K}\sum_{m=1}^{\infty}\left(\sum_{d|m}\lambda_d\right)\frac{c_k}{m}\right|^2\right)^{\frac{1}{2}} + \left(\sum_{\xi\in\mathcal{N}}\left|\sum_{\substack{k=1\\ m=\xi/\nu_k}}^{K}\sum_{m>1}\left(\sum_{d|m}\lambda_d\right)\frac{c_k}{m}\right|^2\right)^{\frac{1}{2}}$$

$$\le \left(\sum_{d=1}^{\infty}\frac{|\lambda_d|}{d}\right)\sqrt{2}\,\pi\left(\int g(t)^2\right)^{\frac{1}{2}} + \left(\sum_{j=1}^{K}\left|\sum_{k<j}{}^{*}\left(\sum_{d|\nu_j/\nu_k}\lambda_d\right)\frac{c_k}{\nu_j/\nu_k}\right|^2\right)^{\frac{1}{2}}. \tag{2.9}$$

We estimate the last sum in (2.9) as follows.

By Cauchy's inequality we find

$$\sum_{j=1}^{K}\left|\sum_{k<j}{}^{*}\left(\sum_{d|\nu_j/\nu_k}\lambda_d\right)\frac{c_k}{\nu_j/\nu_k}\right|^2 \le \sum_{j=1}^{K}\left(\sum_{k<j}{}^{*}\frac{\left(\sum_{d|\nu_j/\nu_k}\lambda_d\right)^2}{(\nu_j/\nu_k)^2}\right)\left(\sum_{k<j}{}^{*}|c_k|^2\right)$$

$$\le \left(\max_j\sum_{k<j}{}^{*}\frac{\left(\sum_{d|\nu_j/\nu_k}\lambda_d\right)^2}{(\nu_j/\nu_k)^2}\right)\frac{\|\mathbf{c}\|^2(\|\mathbf{c}\|^2-1)}{2}; \tag{2.10}$$

here the last step comes from the inequality

$$\sum_{k=1}^{K}(K-k)x_k \le \frac{(\sum x_k)(\sum x_k - 1)}{2} \tag{2.11}$$

valid for $x_k \ge 1$ (the difference of the right-hand side and the left-hand side of (2.11) is an increasing function of x_k in the given range and equality holds if $x_k = 1$ for every k).

If we set

$$\theta := \frac{\|\mathbf{c}\|^2-1}{2}\max_j\sum_{k<j}{}^{*}\frac{\left(\sum_{d|\nu_j/\nu_k}\lambda_d\right)^2}{(\nu_j/\nu_k)^2} \tag{2.12}$$

Theorem 1 follows from (2.11), (2.10), and (2.9). ■

Proof of Corollary 1. We take $\lambda_d = \mu(d)$ (the Möbius function) when $d > 1$ has no prime factor larger than z, and 0 otherwise. Then $\sum_{d|m}\lambda_d = 0$ unless $m = 1$ or all prime factors m are larger than z, in which case $|\sum_{d|m}\lambda_d| = 1$. With this choice, we have

$$\sum_{d=1}^{\infty}\frac{|\lambda_d|}{d} = \prod_{p\le z}\left(1+\frac{1}{p}\right). \tag{2.13}$$

In computing θ only terms where ν_j/ν_k is a product of primes larger than z will contribute, thus if $z < p_1 < p_2 < \cdots < p_K$ are the first K primes larger than z then

$$\theta \leq \frac{\|\mathbf{c}\|^2 - 1}{2} \sum_{k=1}^{K-1} \frac{1}{p_k^2} < \|\mathbf{c}\|^4 z^{-2}. \tag{2.14}$$

Moreover, if $z \geq 2$ it holds

$$\prod_{p \leq z} \left(1 + \frac{1}{p}\right) \sim \frac{6}{\pi^2} e^{\gamma} \log z \ll \log z. \tag{2.15}$$

If we combine together (2.15), (2.14), (2.12), then Theorem 1 yields:

$$\|\mathbf{c}\|^2 \ll (\log z)^2 (1 - \|\mathbf{c}\|^2/z)^{-2} A^2 \tag{2.16}$$

and taking for example $z = 2\|\mathbf{c}\|^2$ we get $\sqrt{K} \leq \|\mathbf{c}\| \ll A \log(A+2)$. ■

3. A conjecture of Vasyunin

We consider now the special case of bounded functions $f(t)$ where all c_k are integers and which take only the values 0 and 1.

Lemma 2 (Vasyunin). *If $f(t)$ is bounded then*

$$\sum_{k=1}^{K} c_k \nu_k = 0. \tag{3.1}$$

If all c_k are integers and $f(t)$ takes only the values 0 and 1 it also holds

$$\sum_{k=1}^{K} c_k = -1. \tag{3.2}$$

Moreover, the associated function $g(t) = \sum c_k \langle \nu_k t \rangle$ takes only the values $\pm\frac{1}{2}$. □

Proof. The first statement of the lemma is obvious. Therefore, if $f(t)$ is bounded we have

$$g(t) = -f(t) - \frac{1}{2} \sum_{k=1}^{K} c_k. \tag{3.3}$$

It follows that

$$⨍ \left(f(t) + \frac{1}{2} \sum_{k=1}^{K} c_k \right) = -⨍ g(t) = 0 \tag{3.4}$$

and

$$-1 < \frac{1}{2}\sum_{k=1}^{K} c_k < 0 \tag{3.5}$$

with the strict inequalities, because $f(t)$ is almost periodic, not constant, with values 0 or 1. Since $\sum c_k$ is an integer, this proves the last statement of the lemma. ■

On the basis of extensive numerical calculations, Vasyunin [2] conjectured that if $f(t)$ takes only the values 0 and 1 then $\sum |c_k| \leq 9$. Since $\sum |c_k|$ is odd, the possible values for $\sum |c_k|$ should be $3, 5, 7, 9$; solutions are known in each case and a complete list of solutions has been obtained if the sum is 3 or 5 (the case of 5 has been treated only by a long enumeration and subdivision of cases and a simpler treatment is desirable). Up to permutations, solutions are as follows.

For $\sum |c_k| = 3$, we have the two-parameter solution

$$(c_1, c_2, c_3) = (1, -1, -1), \qquad (\nu_1, \nu_2, \nu_3) = (x + y, x, y) \tag{3.6}$$

for positive x and y. Every solution is of this type. By specialization, we have the solution with $K = 2$

$$(c_1, c_2) = (1, -2), \qquad (\nu_1, \nu_2) = (2x, x). \tag{3.7}$$

For $\sum |c_k| = 5$, there is the two-parameter solution

$$(c_1, c_2, c_3, c_4, c_5) = (1, 1, -1, -1, -1), \qquad (\nu_1, \nu_2, \nu_3, \nu_4, \nu_5) = (2x, 2y, x, y, x + y) \tag{3.8}$$

and 29 exceptional one-parameter solutions which are not obtained by specialization of the previous two-parameter solution (see [1]).

For $\sum |c_k| = 7$ Vasyunin found 21 solutions and for $\sum |c_k| = 9$ he found 2 solutions. On the basis of extensive numerical calculations, he conjectured that his list is complete.

Corollary 1 shows that $\sum |c_k|$ is bounded. In the case at hand, we have $|g(t)| = \frac{1}{2}$ for all t. We use Selberg's sieve to minimize the quadratic form $\sum_m (\sum_{d|m} \lambda_d)^2/m^2$ subject to the conditions

$$\lambda_1 = 1, \quad \lambda_d = 0 \quad \textit{if} \quad d > z. \tag{3.9}$$

We dispense with the details of the calculation, which are quite standard, and simply give the optimal choice

$$\lambda_m = \frac{\mu(m)}{b(m)} \left(\sum_{\substack{l \leq z/m \\ (l,m)=1}} \frac{\mu^2(l)}{b(l)\, l^2} \right) \Big/ \left(\sum_{l \leq z} \frac{\mu^2(l)}{b(l)\, l^2} \right); \tag{3.10}$$

here $b(n)$ is the arithmetical function

$$b(n) = \prod_{p|n} \left(1 - \frac{1}{p^2}\right). \tag{3.11}$$

With this choice, the minimum of the quadratic form is

$$\sum_{m\le z}\frac{\left(\sum_{d|m}\lambda_d\right)^2}{m^2}=\zeta(2)\times\left(\sum_{l\le z}\frac{\mu^2(l)}{b(l)\,l^2}\right)^{-1}. \tag{3.12}$$

Now Theorem 1 shows that

$$\|\mathbf{c}\|\le\frac{\pi}{\sqrt{2}(1-\sqrt{\theta})}\sum_{m\le z}\frac{|\lambda_m|}{m} \tag{3.13}$$

provided

$$\theta:=\frac{|\,\mathbf{c}\|^2-1}{2}\left(\zeta(2)\Big/\sum_{l\le z}\frac{\mu^2(l)}{b(l)\,l^2}-1\right)<1. \tag{3.14}$$

A numerical calculation with Mathematica using (3.10), (3.13), (3.14), taking $z=1141$, shows that

$$K\le\sum_{k=1}^{K}|c_k|^2<196. \tag{3.15}$$

References

[1] A. Borisov, Quotient singularities, integer ratios of factorials and the Riemann hypothesis, *preprint* (2007), 1–17.

[2] V.I. Vasyunin, On a system of step functions, (Russian) *Zap. Nauchn. Sem. S-Petersburg. Otdel. Mat. Inst. Steklov (POMI)* **262** (1999), *Issled. po Linein. Oper. i Teor. Funkts.* **27**, 49–70, 231–232; English translation *J. Math. Sci. (New York)* **110** (2002), 2930–2943.

version of June 30, 2007

Roots of Polynomials in Subgroups of $\mathbb{F}_p^*$ and Applications to Congruences

E. Bombieri[1], **J. Bourgain**[1], **and S.V. Konyagin**[2]

[1]School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540, USA, [2]Department of Mechanics and Mathematics, Moscow State University, Moscow 119992, Russia

Correspondence to be sent to: J. Bourgain, School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540, USA. e-mail: bourgain@ias.edu

The study of congruences $(\mathrm{mod}\, p)$ for sparse polynomials in one variable arises in several contexts and an important special case occurs when differences between exponents of the monomials have large common factors with $p-1$. In this situation, usual techniques based on Fourier analysis $(\mathrm{mod}\, p)$ and Weil's bounds for exponential sums do not work well and new methods are needed. In this paper we introduce a new technique based on a new result (Proposition 1) that shows in a precise quantitative way that it is not possible to describe a 'large' subgroup of $\mathbb{F}_p^*$ using only polynomial equations of small degree and small height; such a result may be viewed as yet another example of the 'independence' between addition and multiplication in a finite field. Besides showing in Theorem 17 that the number of solutions of the congruences studied here admits a lower bound of the expected order in 'small boxes', an example is given in which the actual number of solutions is much larger than what can be expected from a probabilistic counting. The reduction of the original problem to the principle alluded to above involves the geometry of intersections of varieties of Fermat type, arithmetic formulations of Bézout's Theorem and of Hilbert's Nullstellensatz, as well as certain higher dimensional versions of Proposition 1.

1. Introduction

Let $\mathbb{F}_p$ be the finite field with p elements and let $\{a_1, \ldots, a_r\} \in (\mathbb{F}_p^*)^r$. The study of the distribution of points $(a_1 x^{k_1}, \ldots, a_r x^{k_r})$ as x varies in $\mathbb{F}_p^*$ is of importance in several questions. While for bounded exponents k_i there is recourse to Weil's estimates for exponential sums and Fourier analysis $(\mathrm{mod}\ p)$, such a method loses strength quickly if the exponents k_i become comparable with a power of p and new

ideas are needed to study the problem.

The origin of this paper is in the question of the distribution of $(a_1x^{k_1}, a_2x^{k_2})$ in small rectangular boxes $([l_1, N_1+l_1] \times [l_2, N_2+l_2]$, where small means that N_1 and N_2 can be as small as $p^{1-\delta}$ for some positive δ, while k_1 and k_2 are allowed to be large and, under certain necessary conditions, of order as big as p. Indeed, since $x^{p-1} = 1$ in $\mathbb{F}_p^*$, in order for x^{k_i} to span a large set of values an obvious necessary condition is that k_i should not have too large a common factor with $p-1$, say of order $p^{1-o(1)}$. Moreover, if $k_i - k_j$ has a very large common factor with $p-1$, namely of the same order as p, the powers x^{k_i} and x^{k_j} become correlated because then x^{k_i}/x^{k_j} can take only a bounded number of values. In this case, the usual Fourier analysis $(\mathrm{mod}\ p)$ for studying the distribution of points fails. Proposition 15 (whose proof depends on new methods in arithmetic combinatorics quite different from the techniques of this paper) does provide an appropriate bound for the exponential sums in the Fourier analysis, but still is not strong enough to capture the case where $k_i - k_j$ has a common divisor with $p-1$ proportional to $p-1$, a situation which occurs in the decimation problem in computer science.

The reduction of this difficult case to a situation where Proposition 15 becomes applicable provides the motivation for this paper and this is brought to completion, without further unnecessary conditions, in the final Theorem 17. The case $r = 2$ is the simplest one and is considered separately in the last section of this paper. The case $r \geq 3$ presents new difficulties.

This led to a new problem, namely showing that for all non-zero polynomials $f(z) \in \mathbb{Z}[x]$ of degree at most d with coefficients bounded by H, and any subgroup $G < \mathbb{F}_p^*$ of order larger than a function of d alone, the set consisting of the zeros of all such polynomials $(\mathrm{mod}\ p)$ must avoid a large chunk of the group G, provided p is larger than some function of d and H, of polynomial growth in H; a faster growing bound will not do the job.

This may be viewed as a quantitative form of a principle that it is not possible to describe a multiplicative subgroup of $\mathbb{F}_p^*$ set theoretically by means of a set of polynomial equations of small degree and small coefficients. (Here 'small coefficients' means smaller than a small power of p.) It is yet another example of the 'independence' between addition and multiplication.

The reduction of the initial problem at hand to the principle above is done by fairly elementary means, but it is not simple and occupies the largest part of this paper. The content of this paper is therefore divided in the following sections.

Section 2 deals with the principle just mentioned. Proposition 1 is a precise statement showing that there is some element of G which is not a root of any polynomial with bounded degree and small coefficients; its proof is based on the

5. The main result

In this section we apply Proposition 14 to prove that certain systems of congruences are soluble in small ranges of the variables. We begin by quoting an auxiliary result from [4].

Proposition 15. *Given $r \in \mathbb{N}$ and $\varepsilon > 0$, there are $\delta > 0$ and C_{14}, depending only on r and ε, with the following property. If $p > C_{14}$ is a prime and $1 \le k_1 < \cdots < k_r < p-1$ satisfy*

$$(k_i, p-1) < p^{1-\varepsilon} \quad (1 \le i \le r) \tag{64}$$

$$(k_i - k_j, p-1) < p^{1-\varepsilon} \quad (1 \le j < i \le r) \tag{65}$$

then for $(a_1, \dots, a_r) \in \mathbb{F}_p^r \setminus \{0\}$ it holds

$$\left| \sum_{x \in \mathbb{F}_p} e_p\big(a_1 x^{k_1} + \cdots + a_r x^{k_r}\big) \right| < p^{1-\delta}. \quad \square \tag{66}$$

Remark 16. Condition (65) is essential, as for instance the example $x - x^{(p+1)/2}$ shows.

Theorem 17. *Given $r \ge 2$ and $\varepsilon > 0$ there are $B = B(r,\varepsilon) > 0$, $c = c(r,\varepsilon) > 0$, $\delta = \delta(r,\varepsilon) > 0$, such that the following holds. Let $1 \le k_1 < \cdots < k_r < p-1$ be such that*

$$(k_i, p-1) < p^{1-\varepsilon} \quad (1 \le i \le r) \tag{67}$$

$$(k_i - k_j, p-1) < \frac{p}{B} \quad (1 \le j < i \le r). \tag{68}$$

Let N_i, $(i = 1, \dots, r)$, be such that

$$N_i \ge p^{1-\delta} \quad (i = 1, \dots, r). \tag{69}$$

Then for $p \ge C_{15} = C_{15}(r,\varepsilon)$ and all $a_1, \dots, a_r \in [1, p-1]$ and $l_1, \dots, l_r \in [1, p]$ the system of congruences

$$a_i x^{k_i} \equiv l_i + y_i \pmod{p} \tag{70}$$

has at least $cN_1 \cdots N_r / p^{r-1}$ solutions in the box

$$(x, y_1, \dots, y_r) \in [1, p-1] \times \prod_{i=1}^{r} [1, N_i]. \quad \square \tag{71}$$

Enrico Bombieri · Jean Bourgain

On Kahane's Ultraflat Polynomials

Received September 3, 2008

Abstract. This paper is devoted to the construction of polynomials of almost constant modulus on the unit circle, with coefficients of constant absolute value. In particular one obtains a much improved estimate for the error term. A major part of this paper deals also with the long-standing problem of the effective construction of ultraflat polynomials.

Keywords: Trigonometric polynomials, probabilistic methods, exponential sums

1. Introduction

In 1957 Erdős put forward several problems on polynomials which have since then attracted much attention. One of them asked what is the smallest maximum modulus of an exponential polynomial $P(\theta) = \sum a_m e^{2\pi i m\theta}$ of degree n with coefficients $|a_m| = 1$ of modulus 1. Such polynomials are called unimodular. Erdős thought that the maximum of an exponential unimodular polynomial of degree n was at least $(1+c)\sqrt{n}$ for some fixed positive constant c.

In 1966 Littlewood [17] constructed exponential unimodular polynomials with

$$|P(\theta)| = (1 + o(1))\sqrt{n} \tag{1.1}$$

on the unit circle, except in a rather small neighborhood of $\theta = 0$ where a bound $O(\sqrt{n})$ would hold. In view of this result, he was led to conjecture that there were exponential unimodular polynomials of degree n with maximum modulus $(1 + o(1))\sqrt{n}$ on the unit circle, which would disprove Erdős's conjecture.

Further results in this circle of ideas were obtained by Newman [18], Beller and Newman [2], and Byrnes [6][1] . The next important progress was done by Körner [16]

E. Bombieri, J. Bourgain, School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540, USA; e-mail: eb@ias.edu, bourgain@ias.edu

Mathematics Subject Classification (2000): Primary: 42A05; Secondary: 42A61.

[1] Note that Theorem 2 of [6] is incorrect (as pointed out to the authors by Bahman Saffari, see [19]) and the use of Byrnes's claim invalidates the proofs of Theorems 6 and 7 of [16]. However, the important Lemma 2 of [16], which is a basic tool for achieving unimodularity, does not depend on [6] and remains valid.

who introduced ideas from probability theory to show how to achieve unimodularity starting from polynomials with coefficients only bounded by 1.

Finally, the solution of Erdős's problem was provided by Kahane [14] with the construction of the so-called "ultraflat" polynomials, namely exponential unimodular polynomials $P(\theta)$ of degree n such that (1.1) held uniformly in θ. The $o(1)$ term was made precise in the same paper [14] as $O(n^{-\frac{1}{17}}\sqrt{\log n})$. Other important results on exponential unimodular polynomials, in particular the behaviour of derivatives, the consideration of other norms, and a thorough discussion of the literature, can be found in Queffelec and Saffari [19].

In this paper we prove the following four results. We write $e(\theta) = e^{2\pi i\theta}$, $\| \ \|_\infty$ for the maximum norm on the the unit circle, and $\|\widehat{P}\|_{\ell^1}$ for the ℓ^1-norm of the vector $\widehat{P}$ of Fourier coefficients of the polynomial P.

Definition 1.

$$\mu(n) = \sup \frac{\|\widehat{P}\|_{\ell^1}}{|P\|_\infty}$$

where the supremum is over all non-zero exponential polynomials of degree n.

It is known (H. Shapiro, S. Neuwirth and E. Ricard) that

$$\mu(n) \le \sqrt{n}. \tag{1.2}$$

A short proof, communicated to us by H. Queffelec, goes as follows. We write $P(\theta) = \sum \widehat{P}(m)(m\theta)$. Then

$$\frac{1}{n}\sum_{m=0}^{n} |P(\theta + m/n)|^2 = |\widehat{P}(0) + \widehat{P}(n)e(n\theta)|^2 + \sum_{m=1}^{n-1} |\widehat{P}(m)|^2.$$

Optimizing with respect to θ we get

$$(|\widehat{P}(0)| + |\widehat{P}(n)|)^2 + \sum_{m=1}^{n-1} |\widehat{P}(m)|^2 \le \|P\|_\infty^2.$$

Also,

$$\|P\|_{\ell^1}^2 \le n\left((|\widehat{P}(0)| + |\widehat{P}(n)|)^2 + \sum_{m=1}^{n} |\widehat{P}(m)|^2\right)$$

by the Cauchy-Schwartz inequality and(1.2) follows.

Theorem 2. *Let* $\varepsilon > 0$. *Then*

$$\mu(n) \ge \sqrt{n} - O\big((\log n)^{3/2+\varepsilon}\big).$$

More precisely, let

$$\alpha := n^{-1/2}(\log n)^{3/2+\varepsilon}$$

and $A \geq 0$. Then there is a polynomial in $e(\theta)$ given by

$$P(\theta) = \sum \widehat{P}(m)\, e(m\theta)$$

with $\mathrm{supp}(\widehat{P}) = [0, n]$, *with* $|\widehat{P}(m)| = 1$ *for* $2\alpha n < m < (1 - 2\alpha)n$, *and* $|\widehat{P}(m)| \leq 1$ *otherwise, such that*

$$\begin{aligned} |P(\theta)| &= \sqrt{n} + O(n^{-A}) \qquad \text{if } \theta| \leq 1/2 - 2\alpha \\ |P(\theta)| &\leq \sqrt{n} + O(n^{-A}) \qquad \text{if } 1/2 - 2\alpha < |\theta| \leq 1/2. \end{aligned}$$

Theorem 3. *Let $\varepsilon > 0$ and $\alpha = n^{-1/2}(\log n)^{3/2+\varepsilon}$. Then there is*

$$P(\theta) = \sum \widehat{P}(m)\, e(m\theta)$$

with $\mathrm{supp}(\widehat{P}) = [0, n]$ *and* $|\widehat{P}(m)| = 1$ *there, such that*

$$\begin{aligned} |P(\theta)| &= \sqrt{n} + O\big(n^{1/4}(\log n)^{\frac{3}{4}+\varepsilon}\big) \quad \text{if } |\theta| \leq 1/2 - 2\alpha \\ |P(\theta)| &\leq \sqrt{n} + O\big(n^{1/4}(\log n)^{\frac{3}{4}+\varepsilon}\big) \quad \text{if } 1/2 - 2\alpha < |\theta| \leq 1/2. \end{aligned}$$

Theorem 4. *Let $\varepsilon > 0$. For every $n \geq 1$ there is*

$$P(\theta) = \sum \widehat{P}(m)\, e(m\theta)$$

with $\mathrm{supp}(\widehat{P}) \subset [0, n]$ *and* $|\widehat{P}(m)| = 1$ *there, such that*

$$|P(\theta)| = \sqrt{n} + O\big(n^{\frac{1}{2}-\frac{1}{9}+\varepsilon}\big)$$

for every θ.

Remark 5. The proof can be refined so as to replace n^{ε} by a power of $\log n$.

These theorems improve the corresponding results of Kahane in [14] and represent the limit of our methods.

Remark 6. As such, the proofs of Theorems 3 and 4 are not constructive because they use a randomizing construction (twice for Theorem 4). An effective construction of a polynomial such as in Theorem 3 with the slightly worse error term $O(n^{1/4}(\log n)^{\frac{9}{4}+\varepsilon})$ is possible, as it will be indicated in Section 13.

The last part of the paper from Section 14 onwards is dedicated to an effective construction of a polynomial satisfying Theorem 4, a problem which has been around for some time. We state

Theorem 7. *Let $\varepsilon > 0$. For every $n \geq 1$ there is an effectively constructible polynomial satisfying the hypotheses and conclusion of Theorem 4.*

The proof of the lemma is completed by splitting the sum in the Poisson summation formula (7.3) in two pieces, one for $|h| < H$, the other for the tail $|h| > H$ with H satisfying $H \geq 2 + 2N/M$, for example $H = N^{A+1}$ with $A \geq 1$.

By (7.4) and this choice of H, the tail is estimated as $O(N^{-A-1})$.

By (7.8) and (7.10), the sum over h with $1 \leq |h| < N^{A+1}$ is estimated as $O(N^{A+1-2\varepsilon J})$, which is small if J is large.

Therefore, by (7.14) with a sufficiently small η, the contribution for $h = 0$ yields the main term of the two estimates of the lemma. It remains to prove the last statement of the lemma. This will follow from (7.12) if each derivative $\beta^{(2j)}(x)$ for $j < J$ has finitely many maxima and minima, which is indeed not a serious restriction on $\beta(x)$. □

8. The Körner correction

Suppose we have an exponential polynomial

$$P(\theta) := \sum_{n=p+1}^{q} a_n e(n\theta)$$

with coefficients $|a_n| \leq 1$. We want to find a new exponential polynomial

$$P^*(\theta) := \sum_{n=p+1}^{q} a_n^* e(n\theta)$$

with coefficients $|a_n^*| = 1$ such that the maximum norm $\|P^* - P\|_\infty$ is small.

The *Körner construction* is as follows. Let a_n, $p < n \leq q$ be complex numbers with $a \leq |a_n| \leq b$ and choose a_n^* to be

$$a_n^* = \begin{cases} a_n \pm ie^{i\arg(a_n)}\sqrt{b^2 - |a_n|^2} & \text{if } a_n \neq 0 \\ \pm b & \text{if } a_n = 0 \end{cases}$$

where the sign $\pm$ is chosen at random with probability $1/2$. Thus a_n is the mid-point of the chord of the circle $|z| = b$ perpendicular to the radius through the point a_n, with end-points at the two choices for a_n^*.

Lemma 15 (Körner's correction). *Let*

$$Q(\theta) = \sum_{n=p+1}^{q} a_n e(n\theta)$$

be an exponential polynomial with coefficients $0 \leq a \leq |a_n| \leq b$ for every n. Then there is a choice of signs $\pm$ such that the new polynomial $Q^*(\theta) = \sum a_n^* e(n\theta)$ obtained by Körner's construction satisfies

$$\|Q^* - Q\|_\infty \ll \sqrt{b^2 - a^2}\,\sqrt{(q-p)\log(q-p+1)}.$$

A Problem on Sums of Two Squares

Enrico Bombieri and Jean Bourgain

School of Mathematics, Institute for Advanced Study, 1 Einstein Drive, Princeton, N.J. USA

Correspondence to be sent to: e-mail: eb@ias.edu

Krishnapur et al. [15] studied the length of the fluctuations of nodal lengths of random Laplace eigenfunctions on the standard 2-torus. A key step in the paper is a non-trivial bound for the sixth order correlation of the integer solutions of the equation $m = x^2 + y^2$. This is a problem about a certain diophantine equation, studied here in depth using a variety of methods.

1 Introduction

In a recent paper, Krishnapur et al.[15] studied the length of the fluctuations of nodal lengths of random Laplace eigenfunctions on the standard 2-torus $\mathbb{T} = \mathbb{R}^2/\mathbb{Z}^2$. This problem is obviously related to a study of the fine distribution of solutions of the diophantine equation $x^2 + y^2 = m$, to be solved in integers x and y. A crucial point of their paper depends on showing that the variance of the nodal length (as defined in [15]) is small. This reduces (see [15], Section 2 and Theorem 2.2) to the following estimate.

Let Λ_m be the set of Gaussian integers λ with norm $\lambda\overline{\lambda} = m$ and let $N = |\Lambda_m|$. Define $S_6(m)$ to be the set of 6-correlations

$$S_6(m) = \left\{(\lambda_1, \dots, \lambda_6) \in \Lambda_m^6 \,:\, \lambda_1 + \lambda_2 + \lambda_3 = \lambda_4 + \lambda_5 + \lambda_6\right\}.$$

Then $S_6(m) = o(N^4)$ when $N \to \infty$.

The proof of this result in Section 6 of [15], provided by J. Bourgain, depends on subtle sum-product theorems. The argument provides a quantitative version, with a rather small gain as a function of N.

On the other other hand, the problem of estimating $S_6(m)$ is a diophantine question, which may be explicitly written in the following elementary form.

Problem. Give a non-trivial upper bound for the number of integer solutions (x_i, y_i) $(i = 1, 2, \dots, 6)$ of the system of equations

$$x_i^2 + y_i^2 = m \ (i = 1, 2, \dots, 6), \quad \xi_i = x_i + \sqrt{-1}\, y_i, \tag{1}$$
$$\xi_1 + \xi_2 + \xi_3 = \xi_4 + \xi_5 + \xi_6. \qquad \square$$

m and proves a large deviation estimate with Lemma 20. This is fundamental in the proof of the next rather technical but very important Lemma 21. Section 17 prepares Sections 18 and 19 where it is shown that for curves associated to numbers m with $r \sim A^{-1} \log m / \log\log m$ factors, all in a same dyadic interval, the probability of the rank to be of order $\log m / \log\log m$ is less than δ^r for any fixed $\delta > 0$, provided $A > 24$. This is sufficient to conclude the proof of the final Theorem 25, proving the conjectural bound $O(N^{3+\varepsilon})$ for a random m in the given family, conditionally to the Birch and Swinnerton-Dyer conjecture and the Riemann hypothesis for the associated L-functions.

2 Combinatorics

We denote by $\mathcal{X}$ the set of integer pairs $\mathbf{x} = (x, y)$ such that $x^2 + y^2 = m$ and by $N = |\mathcal{X}|$ its cardinality.

It is readily seen that $O(N^4)$ is the trivial bound and that we may assume $\mathbf{x}_i \neq \pm\mathbf{x}_j$ for $i \neq j$, because the contribution of such solutions is the optimal $O(N^3)$.

Theorem 1. The number of integer solutions of the system of equations

$$x_i^2 + y_i^2 = m (i = 1, 2, \dots, 6), \quad \xi_i = x_i + \sqrt{-1} y_i,$$
$$\xi_1 + \xi_2 + \xi_3 = \xi_4 + \xi_5 + \xi_6,$$

is at most $O(N^{\frac{7}{2}})$. □

Before embarking in the proof of this theorem, we need a simple lemma. Fix ξ_4, ξ_5, ξ_6. Then

$$\xi_1 + \xi_2 + \xi_3 = A + \sqrt{-1}\, B$$

is a known quantity. Thus we have five equations at our disposal:

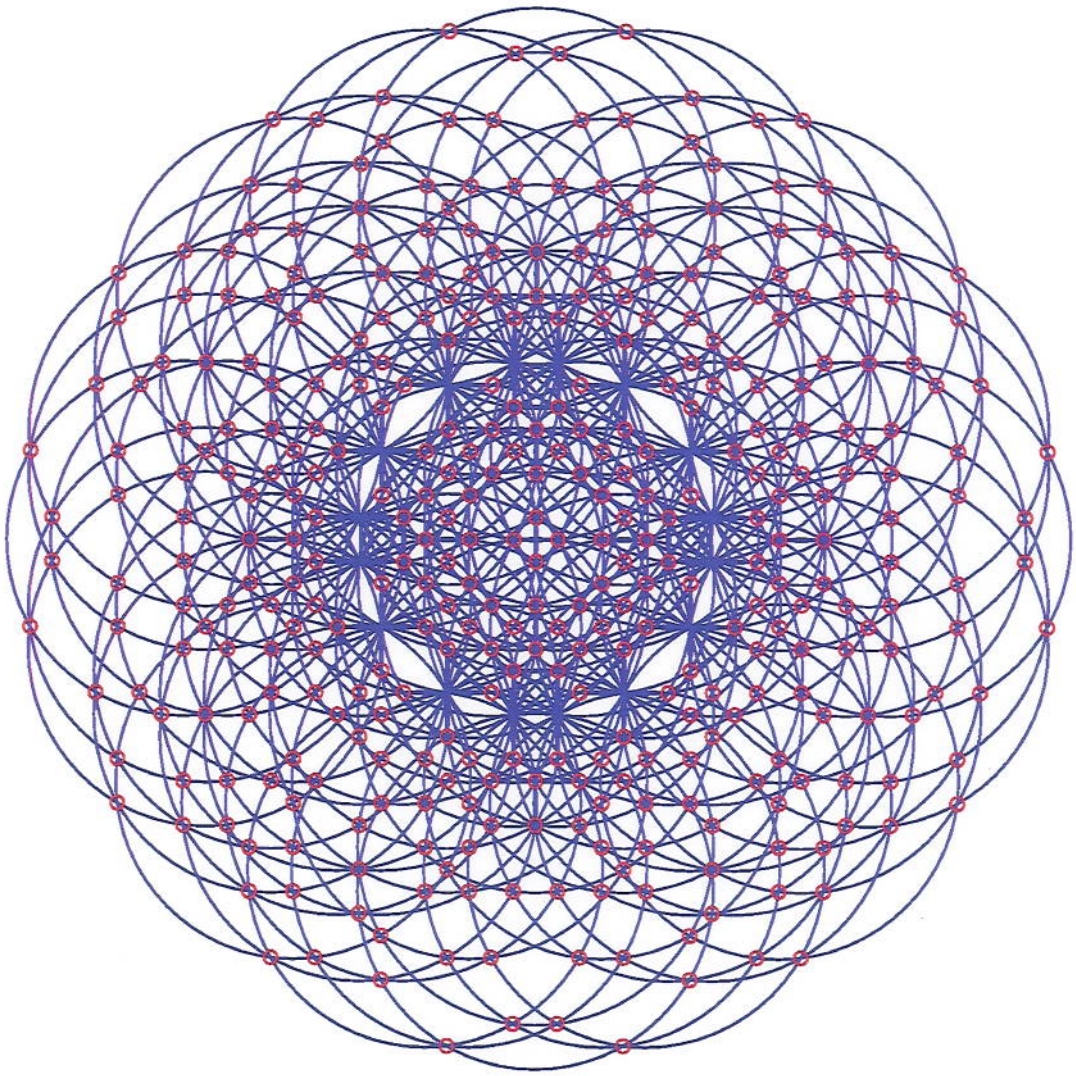
$$x_1 + x_2 + x_3 = A, \quad y_1 + y_2 + y_3 = B, \tag{2}$$
$$y_1^2 = m - x_1^2, \quad y_2^2 = m - x_2^2, \quad y_3^2 = m - x_3^2, \tag{3}$$

in the six unknowns $x_1, x_2, \dots, y_3$. We start by eliminating variables, in order to get an algebraic relation between the first coordinates $x_1$and x_2 of the two points $\mathbf{x}_1 = (x_1, y_1)$ and $\mathbf{x}_2 = (x_2, y_2)$.

We begin by introducing new coordinates (u, t) defined by

$$u = x_1 + x_2, \quad t = y_1 + y_2. \tag{4}$$

The following is a picture of the incidence in the simplest case $m = 5 \times 13$. We present the dual picture, circles centered at $\mathcal{P}$ and points at $\mathcal{C}$.



Circles of radius $\sqrt{65}$ centered at $\mathcal{P}$, incidences as small circles centered at (A, B)

The set $\mathcal{X}$ consists of the 16 solutions $(\pm 1, \pm 8)$, $(\pm 4, \pm 7)$, $(\pm 7, \pm 4)$, $(\pm 8, \pm 1)$. We have $|\mathcal{P}| = 112$ and $|\mathcal{C}| = 372$.

4 Elliptic Curves

We give a reduction of the problem to the study of certain curves of genus 1. This will provide evidence in favor of the conjecture that the number of solutions is $O(N^{3+\varepsilon})$ for every fixed $\varepsilon > 0$. We start with the equations

$$x_1^2 + y_1^2 = m, \quad x_2^2 + y_2^2 = m, \quad (A - x_1 - x_2)^2 + (B - y_1 - y_2)^2 = m,$$

and eliminate y_1, y_2 by taking resultants, getting a polynomial relation between x_1 and x_2. Our calculations turn out to be simpler after making the affine change of variables

$$x_1 = \frac{1}{2}(u + v), \quad x_2 = \frac{1}{2}(u - v),$$

thus $u = x_1 + x_2$ and $v = x_1 - x_2$, and write

$$K = m - A^2 - B^2.$$

Using these coordinates, we obtain a plane sextic Φ in the (u, v)-plane, given by an equation

$$f(u, v) := U_6(u) + U_4(u)v^2 + U_2(u)v^4 = 0 \tag{13}$$

where U_2, U_4, U_6 are certain polynomials of degree 2, 4, and 6 in u. We find

$$\begin{aligned} U_6(u) &= (K + 2Au - u^2)^2 \times \\ &\quad \left(K^2 + 16A^2m + 8Km + 4A(K - 4m)u - 4(K - m)u^2\right), \qquad (14) \\ U_4(u) &= -4A^2K^2 - 2K^3 - 4K^2m - 4AK(4A^2 + K + 4m)u + \\ &\quad (32A^2K + 6K^2 - 32A^2m)u^2 - 8A(3K - 4m)u^3 + 8(K - m)u^4, \qquad (15) \\ U_2(u) &= K^2 + 4AKu - 4(K - m)u^2. \qquad (16) \end{aligned}$$

A very remarkable feature of this change of variables is that the polynomial $f(u, v)$ is only linear in m. This gives rise to a very interesting geometry.

We compute the genus of the plane curve Φ defined the equation $f(u, v) = 0$, by looking at its singularities. We use homogeneous coordinates $[u : v : w]$ and write $F(u, v, w) = w^6 f(u/w, v/w)$ for the homogeneous form of $f(u, v)$.

The line at infinity $w = 0$ intersects the curve in three points, namely, $[0 : 1 : 0]$, $[1 : 1 : 0]$, $[1 : -1 : 0]$; these points are singular points. At the point $[0 : 1 : 0]$ we have

$$F(u, 1, w) = 4(m - K)u^2 + 4AKuw + K^2w^2 + \textit{ higher order terms,}$$

hence we have an ordinary double point if $K(A^2 + K - m) \neq 0$.

In a similar way, we verify that $[1:1:0]$ is an ordinary double point if $K(A^2+K-m)\neq 0$. The analysis for the other point $[1:-1:0]$ is the same, with the same result. We conclude that if $K(A^2+K-m)\neq 0$, then the three points at infinity are ordinary double points of Φ. There are six other finite singular points, which in the generic case are again ordinary double points. They are, writing for simplicity $T=A^2+K$:

$$(A\pm\sqrt{T},0),\quad \left(\frac{A+\sqrt{T}}{2},\pm\frac{A-3\sqrt{T}}{2}\right),\quad \left(\frac{A-\sqrt{T}}{2},\pm\frac{A+3\sqrt{T}}{2}\right).$$

This gives a total of nine ordinary double points, so for generic A, K, m, the curve $f(u,v)=0$ has genus 1.

We label the singular points as follows:

(i) P_{-1}, P_0 and P_1 for the three double points at infinity,

(ii) P_+, P_- for the two finite double points with $v=0$,

(iii) P_{++}, P_{+-}, P_{-+}, P_{--}, for the remaining four double points,

according to the signs of the square-root in the coordinates of the point. These nine points appear in a configuration of seven lines and nine points with every line containing three points, namely, the triplets of points $\{P_{-1},P_-,P_{+-}\}$, $\{P_{-1},P_{-+},P_+\}$, $\{P_0,P_{-+},P_{--}\}$, $\{P_0,P_{++},P_{+-}\}$, $\{P_1,P_{++},P_-\}$, $\{P_1,P_+,P_{--}\}$, $\{P_{-1},P_0,P_1\}$.

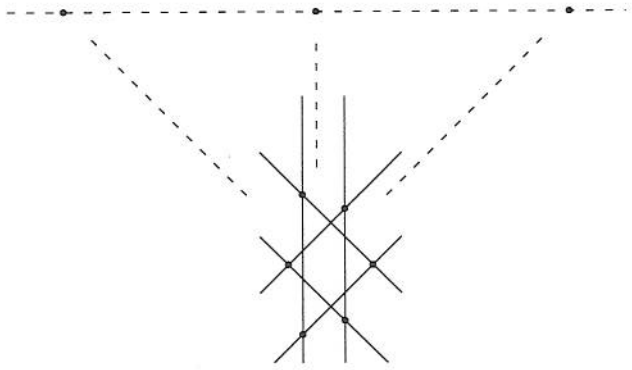


Fig. 2. Seven lines and nine double points ($A=1$, $K=8$). The top dashed line is $w=0$. The six full lines form a fully reducible sextic, occurring when $m=0$.

These points are defined over the field $\mathbb{Q}(A,\sqrt{A^2+K})$, which for general integers A, K, m, will be a quadratic extension of $\mathbb{Q}$. In that case, the field automorphism $\sigma:\sqrt{A^2+K}\to-\sqrt{A^2+K}$ transforms a singular point into its conjugate over $\mathbb{Q}(\sqrt{A^2+K})$.

The same estimate holds replacing $2^{s\Phi(s)}$ by K, because in any case $K < p_1 < p_s$.

It remains to sum this bound for all values of s and show that the total is negligible compared with $|\Omega_{M,K}|$, provided $K \to \infty$ sufficiently slowly. As in the proof of the lemma, we split the range of s into small values, large values, and intermediate values, and more precisely the ranges $s\sqrt{\Phi(s)} < \log K$, $s > \log\log M$, and the complementary range.

The contribution from large values is $O(M/(\log M)^A)$, as in the proof of the lemma.

For intermediate values, we use the bound $O(M/\sqrt{\log M})$ for the number of $m < M$ which are sum of two squares, getting a total of

$$O\left(\frac{M}{\sqrt{\log M}} \sum_{\sqrt{\Phi(s)}\log K < s\Phi(s)} 64^s 2^{-s\Phi(s)}\right).$$

Since $\Phi(s)$ is independent of K and increasing to ∞ as $s \to \infty$, the sum is $O(K^{-A})$ for arbitrarily large A, so the total is negligible compared with $|\Omega_{M,K}|$ when $K \to \infty$.

For small values, we use the estimate (60) with K in place of $2^{s\Phi(s)}$. Then the bound is

$$O\left(\frac{M}{K\sqrt{\log M}} \sum_{s\sqrt{\Phi(s)} < \log K} 64^s\right),$$

and the sum is $O(K^\delta)$ for any fixed $\delta > 0$, so again the total is negligible compared with $|\Omega_{M,K}|$ when $K \to \infty$. ■

Now we are ready to prove

Theorem 17. As $M \to \infty$, for almost all elements $m \in \Omega_M$ the system (1) has only $O(8^{\omega_{4,1}(m)})$ solutions. More precisely, the number of trivial solutions is of order $8^{\omega_{4,1}(m)}$, the number of non-trivial degenerate solutions is $O(4^{\omega_{4,1}(m)})$, and there are at most $O(2^{\omega_{4,1}(m)})$ non-degenerate solutions. □

Proof. Let $\mathcal{P}_K = \prod_{p \leqslant K} p$. For $m \in \Omega_M$ we write uniquely $m = dh$ with $d \in \mathcal{P}_K$ and $h \in \Omega_{M/d,K}$. A decomposition $\xi\overline{\xi} = m$ of m as a sum of two squares can be written as $\xi = \alpha\beta$ with $\alpha\overline{\alpha} = d$ and $\beta\overline{\beta} = h$. This decomposition is unique up to multiplication of α and β by ± 1.

This being said, we proceed as in the proof of Theorem 14. We want to count the total number of solutions of the equation

$$\pm\alpha_1\beta_1 \pm \alpha_2\beta_2 \pm \alpha_3\beta_3 \pm \alpha_4\beta_4 \pm \alpha_5\beta_5 \pm \alpha_6\beta_6 = 0. \tag{61}$$

for any fixed $\eta > 0$ and $\delta > 0$, provided $A > 24$.

Finally, we are ready to determine the average behavior of the number of solutions of the system (1) for $m \in \mathcal{M}$ as defined in Section 19.

Theorem 25. Assume the Riemann hypothesis and the Birch and Swinnerton-Dyer conjecture for the L-functions of elliptic curves over $\mathbb{Q}$.

For fixed $A > 24$ and squarefree $m \in \mathcal{M}$ chosen at random according to the distribution $\psi[\mu]$ as defined in Section 16, the number of solutions of

$$P_1 + P_2 + P_3 = P_4 + P_5 + P_6, \quad |P_i|^2 = m, \quad P_i \in \mathbb{Z}[\sqrt{-1}]$$

is at most $N^{3+\varepsilon}$ as $M \to \infty$, where $N = 2^{\omega(m)}$. □

Proof. At the beginning of Section 15 it was defined for m squarefree the quantity

$$\begin{aligned} &Q(m) := \qquad (87)\\ &\left|\left\{(P_1, \dots, P_6) \in (\mathbb{Z}[\sqrt{-1}])^6 : |P_i|^2 = m \text{ and } P_1 + P_2 + P_3 = P_4 + P_5 + P_6\right\}\right| \\ &\qquad \leqslant \sum_{P_1, P_2, P_3} \min\left(\left|C_{A,B} \cap \mathbb{Z}^2\right|, 2^{(1+\varepsilon)r}\right) \end{aligned}$$

with $r = \log M / \log K \sim \omega(m)$, hence up to a factor $2^{o(r)}$ this is the number of solutions of the system (1). Then on the assumption of the Riemann hypothesis for the L-function of elliptic curves over $\mathbb{Q}$ and the Birch and Swinnerton-Dyer conjecture we had obtained in Corollary 19 the estimate

$$Q(m) \leqslant \sum_{P_1, P_2, P_3} \min\left(\left(\frac{c_{13}}{\varepsilon}\right)^{\frac{1}{2}r(\lambda)}, 2^{(1+\varepsilon)r}\right) + O\left(N^{3+c_{12}A\varepsilon \log \frac{1}{\varepsilon}}\right) \qquad (89)$$

for $m \in \mathcal{M}$ and $M \to \infty$.

The average of $Q(m)$ with respect to the distribution $\psi[\mu]$ is done by appealing to Equation (89). By Equation (140) with $\delta = 1/16$, for any fixed $\eta > 0$ as $M \to \infty$ we have $r(\lambda) < 4\eta r$ outside of a set of μ-measure 16^{-r}. In this exceptional set, we use the trivial bound $2^{(1+\varepsilon)r}$ in taking the minimum in Equation (89). In the non-exceptional set, we use instead the non-trivial bound $C^{\frac{1}{2}r(\lambda)} < C^{2\eta r}$, with $C = c_{13}/\varepsilon$. This gives the bound

$$\begin{aligned} \int Q(m) \mathrm{d}\mu &\leqslant \int \left[\sum_{P_1, P_2, P_3} \min\left(C^{\frac{1}{2}r(\lambda)}, 2^{(1+\varepsilon)r}\right)\right] \mathrm{d}\mu + O(N^{3+c_{12}A\varepsilon \log \frac{1}{\varepsilon}}) \\ &\ll N^3 (c_{13}/\varepsilon)^{2\eta r} + 16^{-r} N^3 2^{(1+\varepsilon)r} + N^{3+c_{12}A\varepsilon \log \frac{1}{\varepsilon}}. \end{aligned}$$