Spectral, combinatorial and analytic methods in some problems in number theory

Dulcinea Raboso

- Ph.D defense -

Advisor: Fernando Chamizo

July 8th, 2014

Index

I. *Spectral methods*

- On the Kuznetsov formula
- Exotic approximate identities and Maass forms

II. *Combinatorial methods*

- Rowland's Sequence
- Distributional properties of powers of matrices

III. *Analytical methods*

- Van der Corput's method and optical illusions
- Lattice points in the 3-dimensional torus

Non-holomorphic modular forms

In 1949, H. Maass introduced these forms to study L-functions in real quadratic fields.

The problem: Are there modular forms corresponding to these L-functions?

Classic modular forms

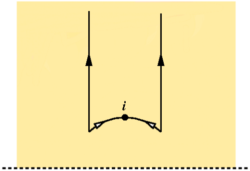
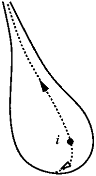
Holomorphic ($\Delta = 0$).
Finite vector spaces.

Non-holomorphic forms

Eigenfunctions of Δ.
Hilbert space (Spectral theory).

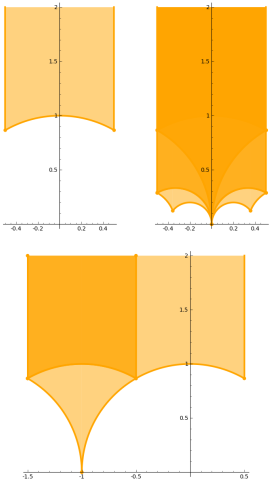
Geometrically:

In the upper half plane $\mathbb{H}$, we consider the hyperbolic distance d. When a Fuchsian group Γ acts on $\mathbb{H}$, the quotient space $\Gamma\backslash\mathbb{H}$ acquires a Riemannian structure.

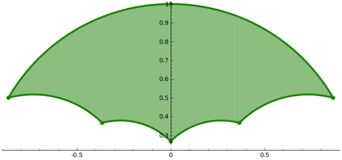
$\mathbb{H} =$  $\longrightarrow$ $\Gamma\backslash\mathbb{H} =$ 

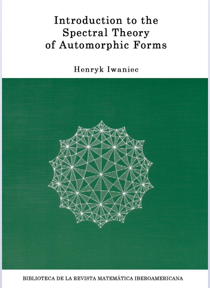
The non-holomorphic modular forms are the functions of $\Gamma\backslash\mathbb{H}$.

Non-compact case



Compact case





Fourier

Any periodic function can be represented by a series of sines and cosines

$$f(x) = \sum a_n e^{2\pi i n x}$$

$$\Delta e^{2\pi i n x} = -4\pi^2 n^2 e^{2\pi i n x}, \qquad \Delta = d^2/dx^2$$

Maass

Any automorphic function can be expanded into eigenfunctions

$$f(z) = \underbrace{\sum a_j u_j(z)}_{\text{discrete spectrum}} + \left(\begin{array}{c}\text{contribution of the} \\ \text{continuous spectrum}\end{array}\right)$$

$$\Delta u_j = -\lambda_j u_j, \qquad \begin{array}{l}\Delta = \text{hyperbolic Laplacian} \\ u_j = \text{Maass form}\end{array}$$

Fourier

Any periodic function can be represented by a series of sines and cosines

$$f(x) = \sum a_n e^{2\pi inx}$$

$$\Delta e^{2\pi inx} = -4\pi^2 n^2 e^{2\pi inx}, \qquad \Delta = d^2/dx^2$$

Maass

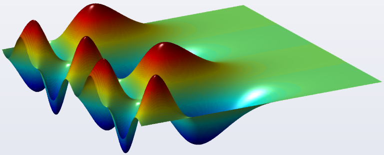
Any automorphic function can be expanded into eigenfunctions

$$f(z) = \underbrace{\sum a_j u_j(z)}_{\text{discrete spectrum}}, \qquad \text{if } \Gamma\backslash\mathbb{H} \text{ is compact.}$$

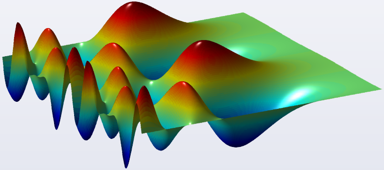
$$\Delta u_j = -\lambda_j u_j,$$

Δ = hyperbolic Laplacian
u_j = Maass form

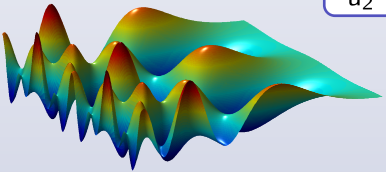
- *The constant eigenfunction:* $u_0(z) = |\Gamma\backslash\mathbb{H}|^{-1/2}$
- *First nontrivial Maass forms:*



u_1



u_2



u_3

Automorphic kernel

Given a function $k : [0, \infty) \longrightarrow \mathbb{R}$

$$K(z,w) = \sum_{\gamma \in \Gamma} k\big(d(\gamma z, w)\big), \qquad z, w \in \mathbb{H}$$

is automorphic in z and w: $K(z,w) = K(\gamma z, w) = K(z, \gamma w)$.

Pretrace formula

$$K(z,w) = \sum_{j \geq 0} h(t_j) u_j(z) \overline{u_j(w)} + \dots$$

where h is the Selberg transform of k (up to a change of variables).

I. *Spectral methods*

- On the Kuznetsov formula
- Exotic approximate identities and Maass forms

II. *Combinatorial methods*

- Rowland's Sequence
- Distributional properties of powers of matrices

III. *Analytical methods*

- Van der Corput's method and optical illusions
- Lattice points in the 3-dimensional torus

The Kuznetsov formula $\mathrm{SL}_2(\mathbb{Z})$

$$\sum_j h(t_j)\nu_j(n)\overline{\nu_j(m)} + \cdots = \sum_{c=1}^{\infty} \frac{1}{c} S(n,m;c)\, H\left(\frac{4\pi\sqrt{|mn|}}{c}\right) + \ldots$$

- A consequence of the Kuznetsov formula is that there is cancellation among Kloosterman sums for different moduli.
- This can also be used to deduce spectral results from arithmetic results via Kloosterman sums.

The Kuznetsov formula $\mathrm{SL}_2(\mathbb{Z})$

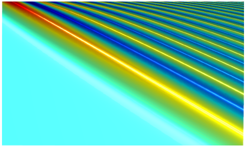
$$\sum_j h(t_j)\nu_j(n)\overline{\nu_j(m)} + \cdots = \sum_{c=1}^{\infty} \frac{1}{c} S(n,m;c)\ H\left(\frac{4\pi\sqrt{|mn|}}{c}\right) + \ldots$$

$$H(x) = \begin{cases} 2i\displaystyle\int_{-\infty}^{\infty} th(t)\frac{J_{2it}(x)}{\cosh(\pi t)}\,dt, & \text{if} \quad mn > 0 \\ \dfrac{4}{\pi}\displaystyle\int_{-\infty}^{\infty} th(t)K_{2it}(x)\sinh(\pi t)\,dt, & \text{if} \quad mn < 0 \end{cases}$$

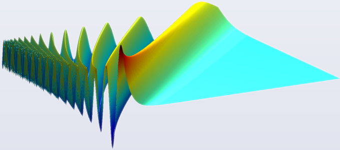
- Asymmetry between the cases $mn > 0$ and $mn < 0$.
- Difficulties to invert the integral transform $h \to H$.

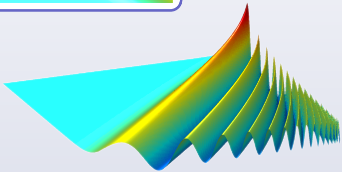
The kernel of these transforms is by no means simple

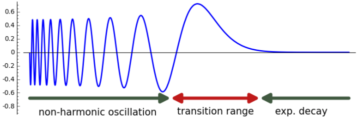
$$f(x,t) = e^{\pi t/2} K_{it}(x)$$



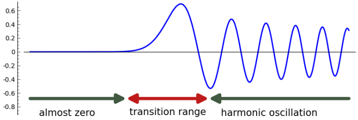
$$mn < 0$$







t large, x variable



x large, t variable

The Kuznetsov formula $\mathrm{SL}_2(\mathbb{Z})$

$$\sum_j h(t_j)\nu_j(n)\overline{\nu_j(m)} + \cdots = \sum_{c=1}^{\infty} \frac{1}{c} S(n,m;c)\, H\Big(\frac{4\pi\sqrt{|mn|}}{c}\Big) + \ldots$$

Theorem

For all $x > 0$, $H(x) = G(x)$ where

$$G(x) = 4\pi x \int_0^{\infty} k(r) J_0\big(x\sqrt{r+\epsilon_0}\big)\, dr,$$

with $\epsilon_0 = 1$ if $mn > 0$ and $\epsilon_0 = 0$ if $mn < 0$.

Why a new formulation?

- The application of the Kuznetsov formula becomes simpler than with the original statement, because the transforms $h \to k$ and $k \to G$ are almost as simple as Fourier transforms.

$$\begin{array}{l} B_0 \text{ bounds } \widehat{h} \\ B_1 \text{ bounds } \widehat{h}' \end{array} \quad \Longrightarrow \quad k^2\Big(\sinh^2 \frac{x}{2}\Big) \le C\frac{B_0(x)B_1(x)}{\sinh x}$$

Example:

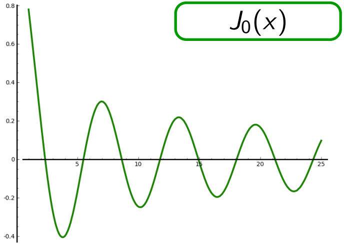
For $h(t) = e^{-t^2/T^2}$ we obtain a quick proof of

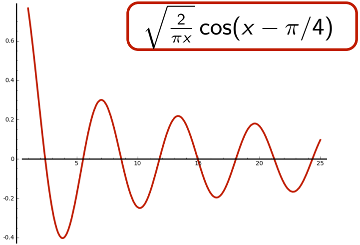
$$\sum |\nu_j(n)|^2 e^{-t_j^2/T^2} + \cdots \sim \pi^{-1}T^2$$

uniformly for $|n| < CT^{2-\delta}$, $\delta > 0$.

Why a new formulation?

- The application of the Kuznetsov formula becomes simpler than with the original statement because the transforms $h \to k$ and $k \to G$ are almost as simple as Fourier transforms.
- We find an extra-short and natural proof of the Kuznetsov formula. This proof avoids any knowledge about special functions except the definition of J_0.





Why a new formulation?

- The application of the Kuznetsov formula becomes simpler than with the original statement because the transforms $h \to k$ and $k \to G$ are almost as simple as Fourier transforms.
- We find an extra-short and natural proof of the Kuznetsov formula. This proof avoids any knowledge about special functions except the definition of J_0.
- It allows to use pairs k and h given by closed formulas.

Example:

$$G(x) = 4\pi x \mu^{-1} e^{-x^2/4\mu}, \qquad \mu > 0$$

$$k(r) = e^{-\mu r} \quad \longleftrightarrow \quad h(t) = 4e^{\mu/2}\sqrt{\frac{\pi}{\mu}}K_{it}(\mu/2)$$

Why a new formulation?

- The application of the Kuznetsov formula becomes simpler than with the original statement because the transforms $h \to k$ and $k \to G$ are almost as simple as Fourier transforms.
- We find an extra-short and natural proof of the Kuznetsov formula. This proof avoids any knowledge about special functions except the definition of J_0.
- It allows to use pairs k and h given by closed formulas.
- The reversed Kuznetsov formula becomes more natural.

  We can think of it as a Fourier inversion.

$$G(x) = 4\pi x \int_0^\infty k(r) J_0\big(x\sqrt{r+\epsilon_0}\big)\, dr$$

I. *Spectral methods*

- On the Kuznetsov formula
- Exotic approximate identities and Maass forms

II. *Combinatorial methods*

- Rowland's Sequence
- Distributional properties of powers of matrices

III. *Analytical methods*

- Van der Corput's method and optical illusions
- Lattice points in the 3-dimensional torus

Two well-known examples of approximate identities

Both are linked to the Fourier expansion of classical modular forms. The first through the function θ and the second through the j-invariant.

1

$$\frac{1}{4}\Big(\sum_{n=-15}^{15} e^{-n^2/4}\Big)^2 = 3.14159265358979328\ldots$$

$$\pi = 3.14159265358979238\ldots$$

2

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999250\ldots$$

$$744 + 640320^3 = 262537412640768744$$

F. Chamizo and D. Raboso, *Modular forms and almost integers* (Spanish). Gac. R. Soc. Mat. Esp. 13 (2010), no. 3, 539–555.

Two examples of our identities

$$r(n) = \#\{(a,b) \in \mathbb{Z}^2 \ : \ a^2 + b^2 = n\}$$

$$S = \sum_{n=0}^{\infty} \left(3 + (-1)^n\right) \frac{r(n)r(n+4)}{2(n+4)^2}, \quad J = \int_{-\infty}^{\infty} \frac{\frac{1}{4} + t^2}{\cosh(\pi t)} |f(t)|^2 \, dt$$

$$f(t) = \zeta(s)L(s,\chi_4)/\zeta(2s) \qquad \text{with} \quad s = \tfrac{1}{2} + it.$$

1

$$\frac{S-3}{J} = \pi - \epsilon \qquad \text{with } 0 < \epsilon < 4 \cdot 10^{-14}.$$

2

$$\sum_{n=1}^{\infty} r(n)r(3n+2)\sqrt{n}e^{-(\frac{1}{4}\log n)^2} = 72e^9\sqrt{\pi}(1-\epsilon), \ \epsilon \approx 3 \cdot 10^{-7}.$$

Spectral theory *(pretrace formula)*

$$K(z,w) = \sum_{\gamma\in\Gamma} k\big(d(\gamma z, w)\big) = a_0 + a_1 u_1(z)\overline{u_1(w)} + \cdots \approx a_0.$$

We choose k, Γ, z and w such that $K(z,w)$ has an arithmetically meaning.

1

The group is $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. The error depends on the third eigenvalue ($\lambda_3 = 190.13$) due to certain symmetries of the eigenfunctions.

2

The group is used to construct Shimura curve $X(6,1)$. The error depends on the first eigenvalue ($\lambda_1 = 6.96$) because in this case there are no symmetries.

Where do the products $r(n)$ come from?

$$K(z,w) = \sum_{\gamma\in\Gamma} k\big(d(\gamma z, w)\big).$$

It turns out that $d\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)i, i\right)$ is a function of $a^2+b^2+c^2+d^2$ and $ad-bc=1$. Note that

$$\begin{cases} a^2+b^2+c^2+d^2 = n \\ ad-bc=1 \end{cases} \longleftrightarrow \begin{cases} (a-d)^2+(c+b)^2 = n-2 \\ (a+d)^2+(c-b)^2 = n+2 \end{cases}$$

and the number of solutions is essentially $r(n+2)r(n-2)$.

H. Iwaniec, *Spectral Methods of Automorphic Forms.*
Grad. Stud. Math. 53, Amer. Math. Soc., Providence, RI, 2nd ed., 2002.

In the second example $r(n)$ appears using a quaternion group:

$$G_3 = \left\{ \frac{1}{2} \begin{pmatrix} a + b\sqrt{3} & c + d\sqrt{3} \\ -c + d\sqrt{3} & a - b\sqrt{3} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \right\}$$

with $a, b, c, d \in \mathbb{Z}$ of the same parity.

The equations become

$$\begin{cases} 3(b^2 + d^2) = m \\ a^2 + c^2 = m + 4 \end{cases} \xrightarrow{m=6n} \begin{cases} b^2 + d^2 = 2n \\ a^2 + c^2 = 6n + 4 \end{cases}$$

Using $r(n) = r(2n)$, the number of solutions is $r(n)r(3n+2)$.

Rowland's Sequence

$$a_k = a_{k-1} + \gcd(k, a_{k-1}) \qquad \text{with} \quad a_1 = 7.$$

k	1	2	3	4	5	6	7	8	9	10	11	...
a_k	7	8	9	10	15	18	19	20	21	22	33	...
$a_k - a_{k-1}$		1	1	1	5	3	1	1	1	1	11	...

Theorem — E.S. Rowland

$a_k - a_{k-1}$ is 1 or prime for every $k \geq 1$.

E.S. Rowland, *A natural prime-generating recurrence.*
J. Integer Seq., 11(2): Article 08.2.8, 13, 2008.

Auxiliary sequences

$$\begin{cases} c_n^* = c_{n-1}^* + \mathrm{lfp}(c_{n-1}^*) - 1 \\ c_1^* = 5 \end{cases} \qquad \text{and} \qquad r_n^* = \frac{c_n^* + 1}{2}$$

where $\mathrm{lfp}(\cdot)$ is the least prime factor of an integer.

Proposition

$$a_k - a_{k-1} = \begin{cases} \mathrm{lfp}(c_{n-1}^*), & \text{if } \ k = r_n^* \ \text{ for some } \ n > 1. \\ 1, & \text{otherwise.} \end{cases}$$

$\{a_k - a_{k-1}\}_{k>1}$ contains infinitely many primes.

Generalized Rowland's sequence

$$a_k = a_{k-1} + \gcd(k, a_{k-1}) \quad \text{with} \quad a_1 > 3 \text{ odd}.$$

k	1	2	3	4	5	6	7	8	9
a_k	805	806	807	808	809	810	811	812	813
$a_k - a_{k-1}$		1	1	1	1	1	1	1	1

10	11	12	13	14	15	16	17	18	...
814	825	828	829	830	835	836	837	846	...
1	11	3	1	1	5	1	1	9	...

Auxiliary sequences

$$\begin{cases} r_{n+1} = \min\left\{k > r_n : \gcd(k, c_n) \neq 1\right\} \\ r_1 = 1 \end{cases}, \begin{cases} c_{n+1} = c_n + \gcd(c_n, r_{n+1}) - 1 \\ c_1 = a_1 - 2 \end{cases}$$

Proposition

$$a_k = c_n + k + 1 \quad \text{for} \quad r_n \leq k < r_{n+1}.$$

$$a_k - a_{k-1} = \begin{cases} \gcd(c_{n-1}, r_n), & \text{if} \quad k = r_n \quad \text{for some} \quad n > 1. \\ 1, & \text{otherwise.} \end{cases}$$

Conjecture A

For any generalized Rowland's sequence, there exists a positive integer N such that $a_k - a_{k-1}$ is 1 or prime for every $k > N$.

Fixed $a_1 > 3$ odd, the Conjecture A holds if any of these conditions is satisfied:

- There is an n such that $2r_n - 1 = c_n$.
- There is an m such that c_m is prime.

$$r_{n+1} = \min\left\{k > r_n : \gcd(k, c_n) \neq 1\right\}, \quad c_{n+1} = c_n + \gcd(c_n, r_{n+1}) - 1$$

n	1	2	3	4	5	6	7	8	9	10	...
r_n	1	5	6	11	12	23	24	47	48	50	...
c_n	5	9	11	21	23	45	47	93	95	99	...

♦ ◊

n	1	2	3	4	5	6	7	8	9	10	...
r_n	1	3	5	6	41	42	83	84	167	168	...
c_n	33	35	39	41	81	83	165	167	333	335	...

♦ ◊

n	1	2	3	4	5	6	7	8	9	...
r_n	1	5	7	10	12	131	132	263	264	...
c_n	115	119	125	129	131	261	263	525	527	...

♦ ◊

$$r_{n+1} = \min \left\{ k > r_n : \gcd(k, c_n) \neq 1 \right\}, \quad c_{n+1} = c_n + \gcd(c_n, r_{n+1}) - 1$$

Conjecture A

For any generalized Rowland's sequence, there exists a positive integer N such that $a_k - a_{k-1}$ is 1 or prime for every $k > N$.

$$n_0 = \inf\{n \in \mathbb{Z}^+ : c_n = 2r_n - 1\}, \quad m_0 = \inf\{n \in \mathbb{Z}^+ : c_n \text{ is prime}\}.$$

Conjecture B

(i) $n_0 < \infty$, (ii) $m_0 < \infty$, (iii) $n_0 = m_0 + 1 < \infty$.

Conjecture B $\Rightarrow$ Conjecture A

$$r_{n+1} = \min\left\{k > r_n : \gcd(k, c_n) \neq 1\right\}, \quad c_{n+1} = c_n + \gcd(c_n, r_{n+1}) - 1$$

Rowland's chains

They are finite sublists of primes inside of a sequence $\{a_k - a_{k-1}\}$.

For $a_1 = 7$, the first 15 primes of the sequence are

$$\mathcal{C}_{15} = \{5, 3, 11, 3, 23, 3, 47, 3, 5, 3, 101, 3, 7, 11, 3\}.$$

We give a characterization which allows to verify whether $\mathcal{C}_m$ is a Rowland's chain. For example:

✓ $\mathcal{C}_4 = \{3, 19, 5, 3\}$

✗ $\mathcal{C}_3 = \{17, 5, p\} \quad \forall\, p > 3$

✗ $\mathcal{C}_{2m} = \{p_1, \dots, p_m, p_1, \dots, p_m\}$ with $p_1, \dots, p_m$ distinct primes.

We start with an example

- We choose a "large" prime

$$p = 2311.$$

- Given a matrix M, we take the pseudorandom points

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = M^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

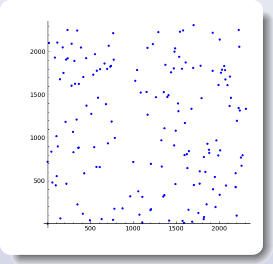
reduced modulo p.

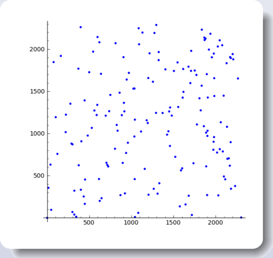
$$\exp_p(M) = \text{order of } M \text{ modulo } p.$$

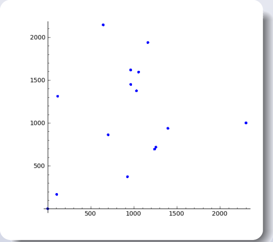
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



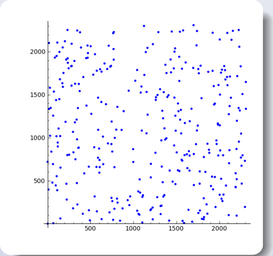


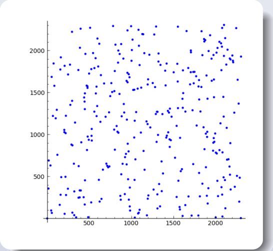


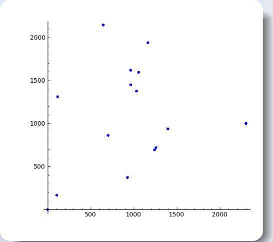
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



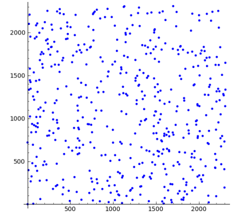


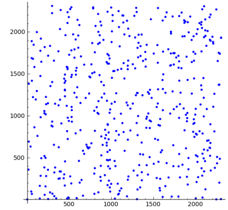


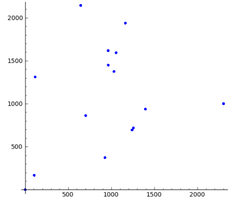
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



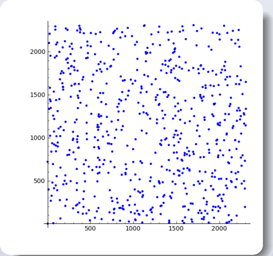


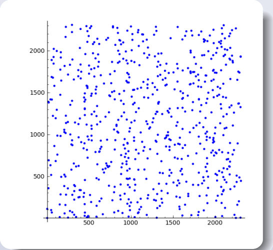


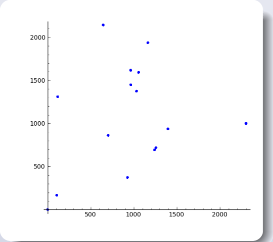
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



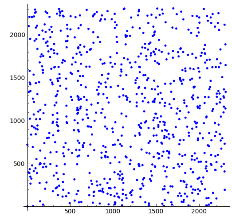


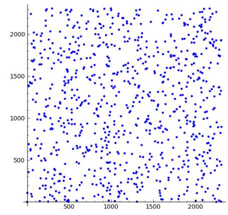


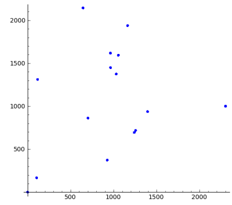
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



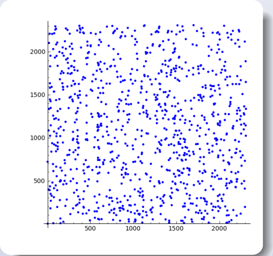


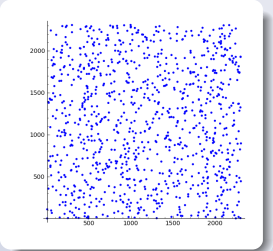


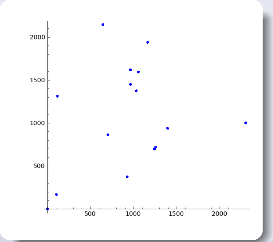
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



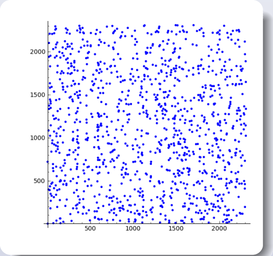


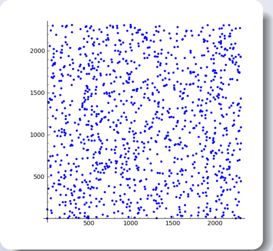


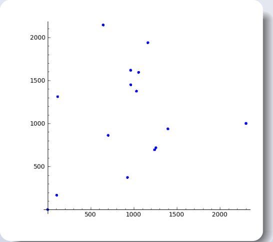
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



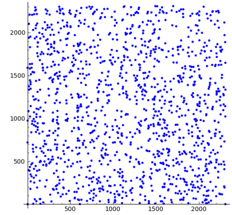


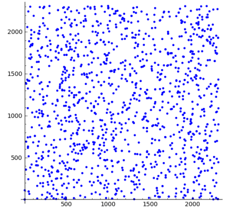


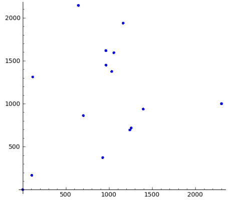
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



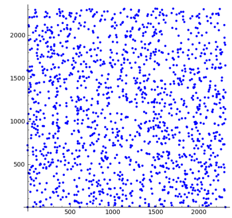


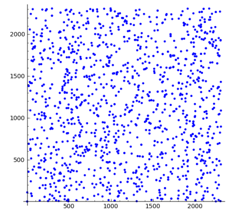


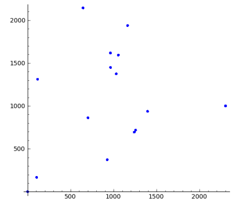
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



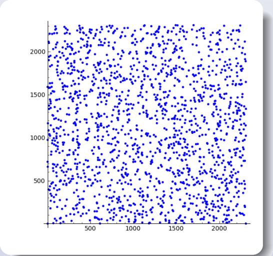


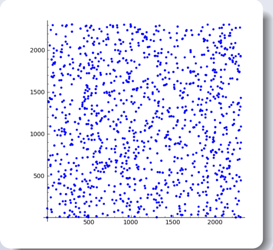


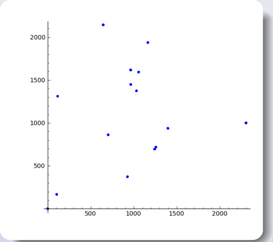
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



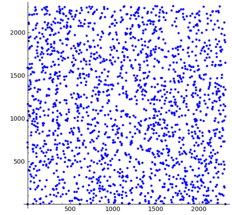


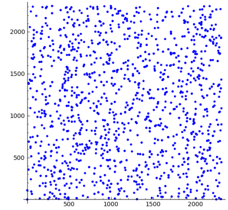


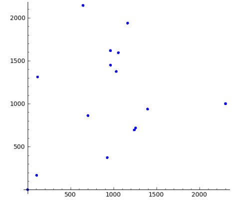
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



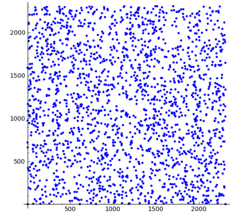


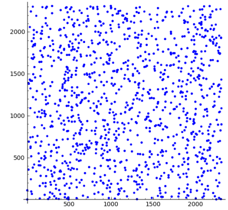


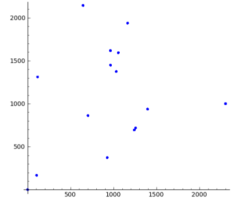
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



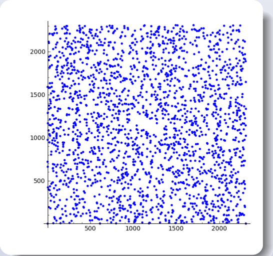


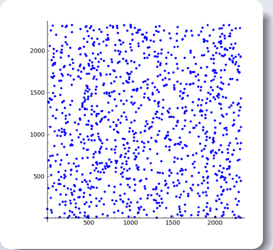


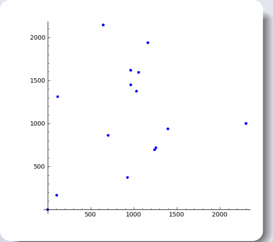
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



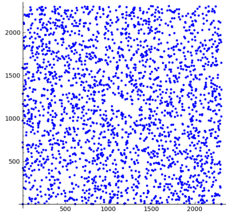


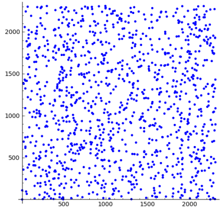


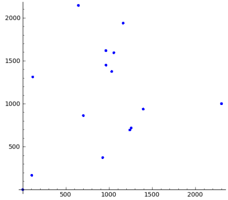
$p = 2311$

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix} \qquad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \qquad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$$\exp_p(A) = p - 1 \qquad \exp_p(B) = \frac{p-1}{2} \qquad \exp_p(C) = \frac{p-1}{154}$$



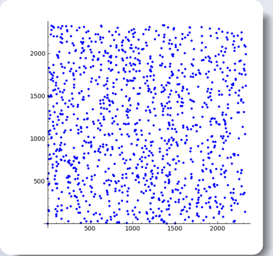


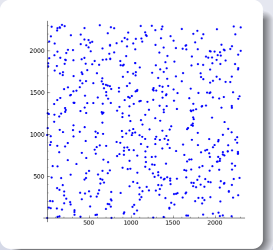


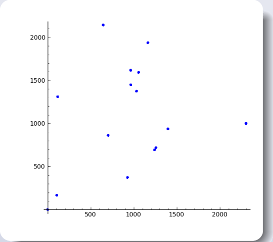
By changing the prime

$$C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

$p = 2333$	$p = 2309$	$p = 2311$
$\exp_p(C) = \frac{p+1}{2}$	$\exp_p(C) = \frac{p-1}{4}$	$\exp_p(C) = \frac{p-1}{154}$







Types of sieving

Sieve of Eratosthenes
classical sieve

The large sieve

The larger sieve

Primes

2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40,
41, 42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59, 60,
61, 62, 63, 64, 65, 66, 67, 68, 69, 70,
71, 72, 73, 74, 75, 76, 77, 78, 79, 80,
81, 82, 83, 84, 85, 86, 87, 88, 89, 90,
...

Types of sieving

Sieve of Eratosthenes
classical sieve

The large sieve

The larger sieve

Primes

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, 9, ~~10~~,
11, ~~12~~, 13, ~~14~~, 15, ~~16~~, 17, ~~18~~, 19, ~~20~~,
21, ~~22~~, 23, ~~24~~, 25, ~~26~~, 27, ~~28~~, 29, ~~30~~,
31, ~~32~~, 33, ~~34~~, 35, ~~36~~, 37, ~~38~~, 39, ~~40~~,
41, ~~42~~, 43, ~~44~~, 45, ~~46~~, 47, ~~48~~, 49, ~~50~~,
51, ~~52~~, 53, ~~54~~, 55, ~~56~~, 57, ~~58~~, 59, ~~60~~,
61, ~~62~~, 63, ~~64~~, 65, ~~66~~, 67, ~~68~~, 69, ~~70~~,
71, ~~72~~, 73, ~~74~~, 75, ~~76~~, 77, ~~78~~, 79, ~~80~~,
81, ~~82~~, 83, ~~84~~, 85, ~~86~~, 87, ~~88~~, 89, ~~90~~,
...

$$2 \mid n$$

Types of sieving

Sieve of Eratosthenes
classical sieve

The large sieve

The larger sieve

Primes

2,	3,	5,	7,	~~9~~,
11,	13,	~~15~~,	17,	19,
~~21~~,	23,	25,	~~27~~,	29,
31,	~~33~~,	35,	37,	~~39~~,
41,	43,	~~45~~,	47,	49,
~~51~~,	53,	55,	~~57~~,	59,
61,	~~63~~,	65,	67,	~~69~~,
71,	73,	~~75~~,	77,	79,
~~81~~,	83,	85,	~~87~~,	89,
...				

$3 \mid n$

Types of sieving

Sieve of Eratosthenes
classical sieve

The large sieve

The larger sieve

Primes

	2,	3,		5,		7,		
11,		13,				17,		19,
		23,						29,
31,						37,		
41,		43,				47,		
		53,						59,
61,						67,		
71,		73,						79,
		83,						89,
...								

We eliminate one class by prime.

Types of sieving

Sieve of Eratosthenes
classical sieve

The large sieve

The larger sieve

Squares

2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40,
41, 42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59, 60,
61, 62, 63, 64, 65, 66, 67, 68, 69, 70,
71, 72, 73, 74, 75, 76, 77, 78, 79, 80,
81, 82, 83, 84, 85, 86, 87, 88, 89, 90,
...

Types of sieving

Sieve of Eratosthenes

classical sieve

The large sieve

The larger sieve

Squares

~~2~~, 3, 4, ~~5~~, 6, 7, ~~8~~, 9, 10,
~~11~~, 12, 13, ~~14~~, 15, 16, ~~17~~, 18, 19, ~~20~~,
21, 22, ~~23~~, 24, 25, ~~26~~, 27, 28, ~~29~~, 30,
31, ~~32~~, 33, 34, ~~35~~, 36, 37, ~~38~~, 39, 40,
~~41~~, 42, 43, ~~44~~, 45, 46, ~~47~~, 48, 49, ~~50~~,
51, 52, ~~53~~, 54, 55, ~~56~~, 57, 58, ~~59~~, 60,
61, ~~62~~, 63, 64, ~~65~~, 66, 67, ~~68~~, 69, 70,
~~71~~, 72, 73, ~~74~~, 75, 76, ~~77~~, 78, 79, ~~80~~,
81, 82, ~~83~~, 84, 85, ~~86~~, 87, 88, ~~89~~, 90,
...

$$\left(\frac{n}{3}\right) = -1$$

Types of sieving

Sieve of Eratosthenes

classical sieve

The large sieve

The larger sieve

Squares

~~3~~, 4, 6, ~~7~~, 9, 10,
~~12~~, ~~13~~, 15, 16, ~~18~~, 19,
21, ~~22~~, 24, 25, ~~27~~, ~~28~~, 30,
31, ~~33~~, 34, 36, ~~37~~, 39, 40,
~~42~~, ~~43~~, 45, 46, ~~48~~, 49,
51, ~~52~~, 55, ~~57~~, ~~58~~, 60,
61, 63, 64, 66, 67, 69, 70,
~~72~~, ~~73~~, 75, 76, ~~78~~, ~~79~~, ~~80~~,
81, ~~82~~, 84, 85, ~~87~~, ~~88~~, 90,
...

$$\left(\frac{n}{5}\right) = -1$$

Types of sieving

Sieve of Eratosthenes
classical sieve

The large sieve

The larger sieve

Squares

4, 9, 16, 25, 36, 49, 64, 81, ...

We eliminate many classes by prime.

Types of sieving

Sieve of Eratosthenes
classical sieve

The large sieve

The larger sieve

We eliminate many more classes by prime.

Types of sieving

Sieve of Eratosthenes
classical sieve

The large sieve

The larger sieve

Number of classes close to prime.

$$\exp_p(n) = \begin{cases} \text{order of } n & \text{in } \mathbb{F}_p^* \\ 0 & \text{if } p \mid n \end{cases}$$

It is very unlikely to find n such that $\exp_p(n)$ is small for many consecutive primes.

For p in a reasonably large range, $k \to n^k \pmod{p}$ is a good pseudorandom number generator for almost any choice of n.

P.X. Gallagher, *A larger sieve.* Acta Arith., 18:77–81, 1971.

Set (Interval):

$$\mathrm{GL}_2(\mathbb{Z})[N] = \left\{A \in \mathrm{GL}_2(\mathbb{Z}) \ : \ 0 \leq a_{ij} \leq N\right\}$$

Choose $0 < \theta < \gamma$

Primes:

$$\{p \text{ prime } \ : \ p < N^\gamma\}$$

Elements that remain after sieving:

$$\left\{A \in \mathrm{GL}_2(\mathbb{Z})[N] \ : \ \exp_p(A) \leq N^\theta, \ \ p < N^\gamma\right\}$$

For a fixed prime p, we consider

$$\{A \in \mathrm{GL}_2(\mathbb{F}_p) \ : \ \det A = m\}$$

How many matrices have $\exp_p(A) = n$?

- *Diagonalizable case*

$$\begin{pmatrix} \alpha & 0 \\ 0 & m\alpha^{-1} \end{pmatrix} \quad \alpha \in \mathbb{F}_p^* \qquad\qquad \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix} \quad \alpha \in \mathbb{F}_{p^2} - \mathbb{F}_p$$

- *Non-diagonalizable case*

$$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix} \qquad \alpha \in \mathbb{F}_p^*$$

Canonical form ←----→ *Trace*

Gallagher's sieve applied to the traces gives

Theorem

Given $\varepsilon > 0$ and $0 < \theta < \gamma \leq 1$, the number of matrices $A \in \mathrm{GL}_2(\mathbb{Z})[N]$ such that $\exp_p(A) \leq N^\theta$ for all $p < N^\gamma$, is

$$< CN^{2\theta+1+\varepsilon}$$

Theorem

Under the same conditions, with $A \in \mathrm{SL}_2(\mathbb{Z})[N]$, the number of matrices is

$$< CN^{\theta+1+\varepsilon}$$

Using exponential sum techniques we also prove that there are "nearby" matrices with the same order.

I. Spectral methods

- On the Kuznetsov formula
- Exotic approximate identities and Maass forms

II. Combinatorial methods

- Rowland's Sequence
- Distributional properties of powers of matrices

III. Analytical methods

- Van der Corput's method and optical illusions
- Lattice points in the 3-dimensional torus

Many problems in number theory lead to the estimation of trigonometric sums

$$S = \sum_{a \leq n \leq b} e\big(f(n)\big),$$

where $e(x) = e^{2\pi i x}$ and f is a real function.

Van der Corput's method

- A-process: This corresponds to divide the range of summation applying Cauchy's inequality to reduce the oscillations, at the cost of certain loss of accuracy in the estimation.
- B-process: We transform the new sum by Poisson summation combined with the stationary phase principle.

Some examples

1

If $f'' \asymp \lambda$, $$\sum_{n=1}^{N} e\big(f(n)\big) < C\big(N\lambda^{1/2} + \lambda^{-1/2}\big).$$

2

If f' is monotonic and $|f'| \leq 1/2$,

$$\sum_{n=1}^{N} e\big(f(n)\big) = \int_{1}^{N} e\big(f(x)\big)\, dx + O(1).$$

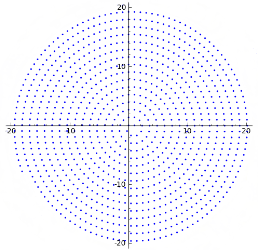
Our trigonometric sum

$$S(N;\alpha) = \sum_{n=1}^{N} e(\alpha\sqrt{n}) \qquad \text{with } \alpha > 0 \text{ fixed.}$$

2

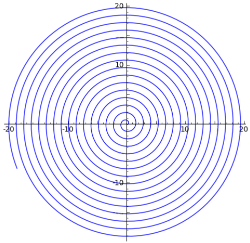
The derivative of $\alpha\sqrt{x}$ decreases to 0, so we expect a good approximation by

$$\int_1^N e(\alpha\sqrt{x})\ dx = \frac{\sqrt{N}}{\pi\alpha} e(\alpha\sqrt{N} - 1/4) + O(1).$$



$\alpha = 1/2$

$\longleftrightarrow$



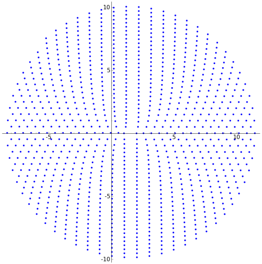
Archimedean spiral

Consequently a spiral should show up for every α,

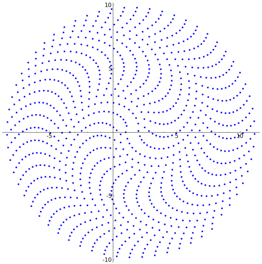
$$\{S(n;\alpha)\}_{n=1}^{N} \longleftrightarrow \frac{1}{2}(\pi\alpha)^{-2}t(\sin t, -\cos t)$$

with $t \in [1, 2\pi\alpha\sqrt{N}]$

But...

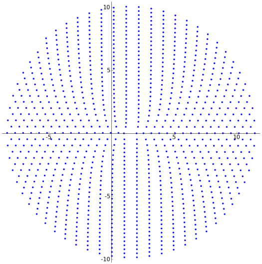


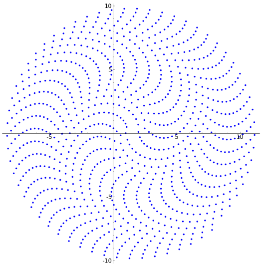
$\alpha = 1$



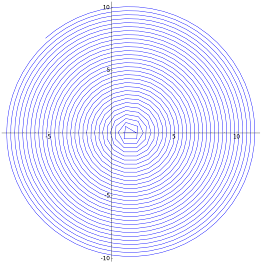
$\alpha = 65/64$

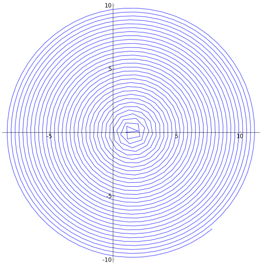
But...





Wait ...





The approximation of the exponential sum

$$S(x;\alpha) = \mathcal{A}(x;\alpha) + (\text{translation}),$$

where

$$\mathcal{A}(x;\alpha) = \frac{e\left(\alpha\sqrt{x} - 1/4\right)}{\pi\alpha}\left(\sqrt{x} + i\cosh\log(\pi\alpha)\right),$$

that when x varies approximates an Archimedean spiral of width $1/\pi\alpha$.

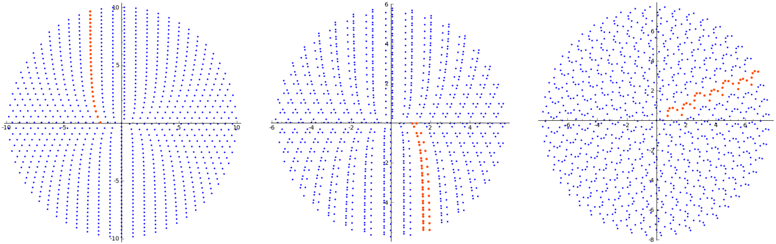
Optical illusions?

- The separation between successive turns tends to be $1/\pi\alpha^2$.
- When $\alpha > \pi^{-1}$ the width of the spiral is smaller than the distance between consecutive values of the discretization.
- $\mathcal{A}(n_1;\alpha)$ and $\mathcal{A}(n_2;\alpha)$ with $n_1, n_2 \in \mathbb{Z}^+$ become geometrically consecutive if $\alpha\sqrt{n_1} \approx \alpha\sqrt{n_2} + 1$.

Branch

It is a sequence $\left\{\mathcal{A}(t_k;\alpha)\right\}_{k=0}^{\infty}$ where t_k satisfies the recurrence relation

$$t_{k+1} = t_k + \left\lfloor \frac{2\alpha\sqrt{t_k}+1}{\alpha^2} + \frac{1}{2} \right\rfloor .$$



$\alpha = 1$ $\qquad$ $\alpha = \sqrt{3}$ $\qquad$ $\alpha = 1.3$

The recurrence relation $(\alpha^2 = n)$

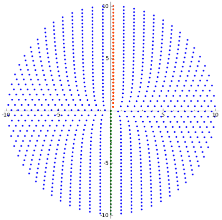
$$t_{k+1} = t_k + \left\lfloor \frac{2\sqrt{nt_k}+1}{n} + \frac{1}{2} \right\rfloor.$$

We find an explicit solution of the recurrence when n is even.

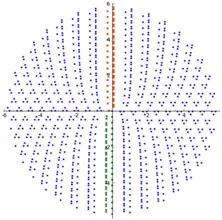
The simplest case is $n = 2$,

$$t_k = \frac{k(k+1)}{2} + \lfloor \sqrt{2t_0} \rfloor k + t_0.$$

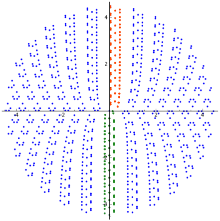
What happens if n is odd?



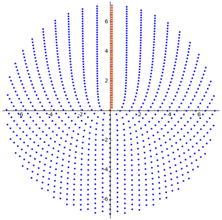
$\alpha = 1$



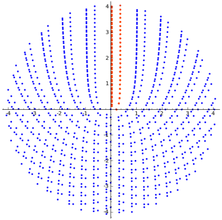
$\alpha = \sqrt{3}$



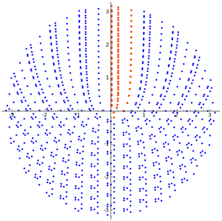
$\alpha = \sqrt{5}$



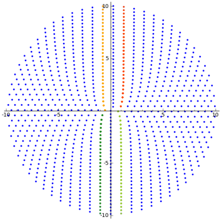
$\alpha = \sqrt{2}$



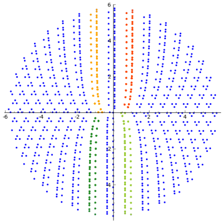
$\alpha = \sqrt{6}$



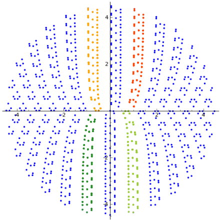
$\alpha = \sqrt{10}$



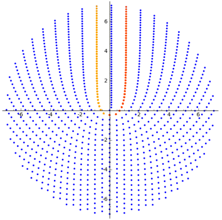
$\alpha = 1$



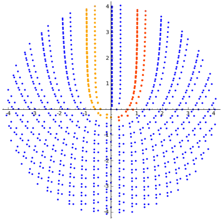
$\alpha = \sqrt{3}$



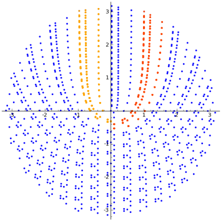
$\alpha = \sqrt{5}$



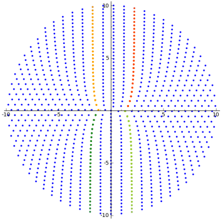
$\alpha = \sqrt{2}$



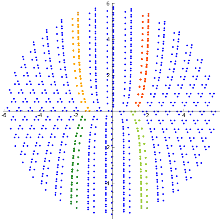
$\alpha = \sqrt{6}$



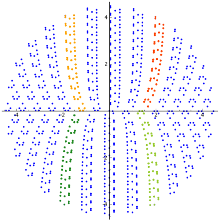
$\alpha = \sqrt{10}$



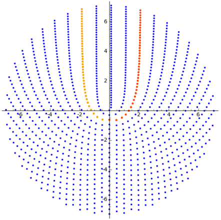
$\alpha = 1$



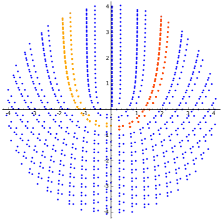
$\alpha = \sqrt{3}$



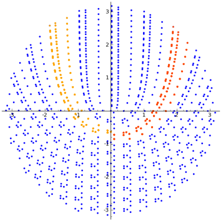
$\alpha = \sqrt{5}$



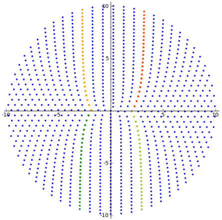
$\alpha = \sqrt{2}$



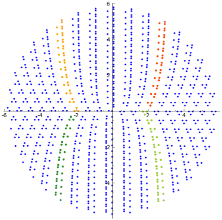
$\alpha = \sqrt{6}$



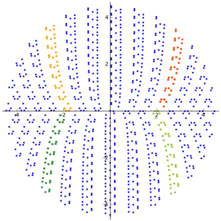
$\alpha = \sqrt{10}$



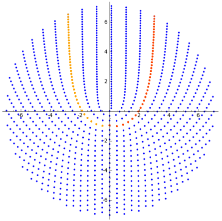
$\alpha = 1$



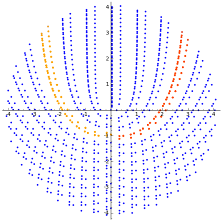
$\alpha = \sqrt{3}$



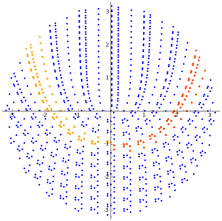
$\alpha = \sqrt{5}$



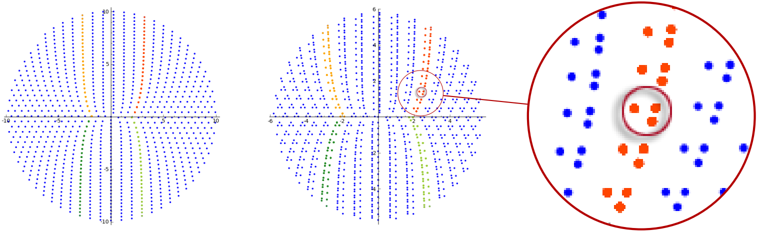
$\alpha = \sqrt{2}$



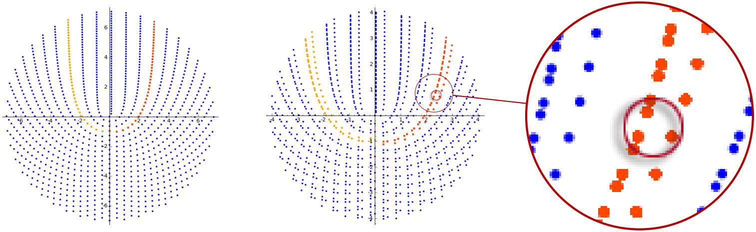
$\alpha = \sqrt{6}$



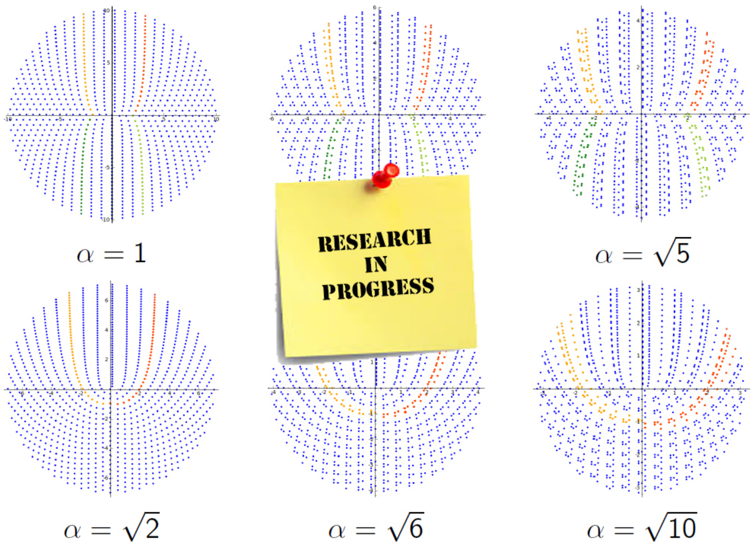
$\alpha = \sqrt{10}$



$\alpha = 1$ $\alpha = \sqrt{3}$ $\alpha = \sqrt{5}$



$\alpha = \sqrt{2}$ $\alpha = \sqrt{6}$ $\alpha = \sqrt{10}$


$\alpha = 1$
RESEARCH IN PROGRESS
$\alpha = \sqrt{5}$
$\alpha = \sqrt{2}$
$\alpha = \sqrt{6}$
$\alpha = \sqrt{10}$

Lattice points

The problem: Estimation of the number of points with integer coordinates in large closed domains.

For example, given a domain $\mathcal{D} \in \mathbb{R}^2$, we study the number of points of $\mathbb{Z}^2$ in $R\mathcal{D}$ when $R \in \mathbb{R}^+$ increases.

The number of lattice points in $R\mathcal{D}$ is

$$\sum_{\vec{n} \in \mathbb{Z}^2} \chi(R^{-1}\vec{n}) = R^2 \sum_{\vec{n} \in \mathbb{Z}^2} \widehat{\chi}(R\vec{n}),$$

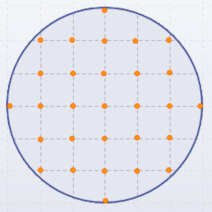
where χ is the characteristic function of $\mathcal{D}$.

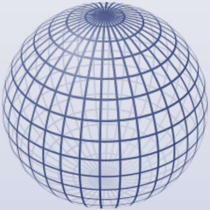
$\vec{n} = \vec{0}$ ←- - - - → main term: $|\mathcal{D}|R^2$.
$\vec{n} \neq \vec{0}$ ←- - - - → error term.

The circle problem — M.N. Huxley

$$\#\{\vec{n} \in \mathbb{Z}^2 \ : \ \|\vec{n}\| \leq R\} = \pi R^2 + O_\epsilon\left(R^{131/208+\epsilon}\right)$$

for every $\epsilon > 0$.





The sphere problem — D.R. Heath-Brown

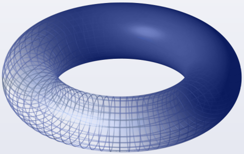
$$\#\{\vec{n} \in \mathbb{Z}^3 \ : \ \|\vec{n}\| \leq R\} = \frac{4}{3}\pi R^3 + O_\epsilon\left(R^{21/16+\epsilon}\right)$$

for every $\epsilon > 0$.

Lattice points in the R-scaled torus

$$\mathbb{T} = \left\{(x,y,z) \in \mathbb{R}^3 \ : \ \left(\rho' - \sqrt{x^2+y^2}\right)^2 + z^2 \le \rho^2\right\}$$

where $0 < \rho < \rho'$ are fixed constants. Say $\rho' = 1$.



$$\mathcal{N}(R) = \#\left\{\vec{n} \in \mathbb{Z}^3 \ : \ R^{-1}\vec{n} \in \mathbb{T}\right\}, \quad R > 1$$

Theorem

$$\mathcal{N}(R) = |\mathbb{T}|R^3 + M_R R^{3/2} + O_\epsilon\left(R^{4/3+\epsilon}\right)$$

for every $\epsilon > 0$, where M_R is a bounded periodic function.

Poisson summation formula

$$\mathcal{N}(R) = \sum_{\vec{n}\in\mathbb{Z}^3} \chi\left(R^{-1}\vec{n}\right) \text{``}=\text{''}\, R^3 \sum_{\vec{n}\in\mathbb{Z}^3} \widehat{\chi}(R\vec{n}).$$

$\vec{n} = (0,0,0)$	←- - - - -→ main term	$\widehat{\chi}(\vec{0})R^3$
$\vec{n} = (0,0,n)$	←- - - - -→ secondary main term	$R^3 \sum_{n\neq 0} \widehat{\chi}(0,0,Rn)$
Otherwise	←- - - - -→ error term	$R^3 \sum_{n=-\infty}^{\infty} \sum_{m=1}^{\infty} r(m)\widehat{\chi}(0, R\sqrt{m}, Rn)$

Poisson summation formula

$$\mathcal{N}(R) = \sum_{\vec{n}\in\mathbb{Z}^3} \chi\left(R^{-1}\vec{n}\right) \text{``}=\text{''}\, R^3 \sum_{\vec{n}\in\mathbb{Z}^3} \widehat{\chi}(R\vec{n})$$

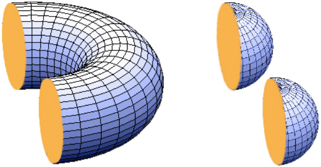
$\vec{n} = (0,0,0)$	←----→ main term	$2\pi^2\rho^2R^3$
$\vec{n} = (0,0,n)$	←----→ secondary main term	$4\pi\rho R^2 \sum_{n=1}^{\infty} \frac{J_1(2\pi R\rho n)}{n}$
Otherwise	←----→ error term	$O\left(R^{4/3+\epsilon}\right)$

An idea about the estimation of the error term

- Stationary phase principle to get a new exponential sum.
- Using the symmetries we "glue" the variables.
- After some manipulations the sum becomes one appearing in the sphere problem.

Geometrically

The sections of a torus and a sphere are alike and differ in a translation which introduce a phase in the Fourier transform side and is eliminated with Cauchy's inequality.



F. Chamizo and H. Iwaniec, *On the sphere problem.*
Rev. Mat. Iberoamericana 11(2): 417–429, 1995.

References

Part I

- F. Chamizo and D. Raboso. *On the Kuznetsov formula*. Preprint (2013). Submitted.
- F. Chamizo, D. Raboso, and S. Ruiz-Cabello. *Exotic approximate identities and Maass forms*. Acta Arith. 159 (2013), no. 1, 27–46.
- D. Raboso. *When the modular world becomes non-holomorphic*. Preprint (2013). To appear in Contemporary Mathematics.

Part II

- F. Chamizo, D. Raboso, and S. Ruiz-Cabello. *On Rowland's sequence*. Electron. J. Combin. 18 (2011), no. 2, Paper 10, 10 pp.
- F. Chamizo and D. Raboso. *Distributional properties of powers of matrices*. Preprint (2013). To appear in Czechoslovak Mathematical Journal.

Part III

- F. Chamizo and D. Raboso. *Van der Corput method and optical illusions*. Preprint (2014).
- F. Chamizo and D. Raboso. *Lattice points in the 3-dimensional torus*. Preprint (2014).