Counting with L-functions
24^{th} Jarník's Lecture

Gergely Harcos

Alfréd Rényi Institute of Mathematics
https://users.renyi.hu/∼gharcos/

30 September 2025
Charles University, Prague

An ancient Diophantine problem

Diophantus: Arithmetica, Book V, Problem 11

Find three rational squares, each exceeding 3, whose sum is 10.

Some solutions

$$(1240/711)^2 + (1303/711)^2 + (1349/711)^2 = 10$$
$$(1259/711)^2 + (1273/711)^2 + (1360/711)^2 = 10$$
$$(1276/711)^2 + (1303/711)^2 + (1315/711)^2 = 10$$
$$(1285/711)^2 + (1288/711)^2 + (1321/711)^2 = 10$$

The last example is from Diophantus' book.

Smallest solutions

$$(33/19)^2 + (35/19)^2 + (36/19)^2 = 10$$
$$(85/49)^2 + (87/49)^2 + (96/49)^2 = 10$$
$$(100/57)^2 + (103/57)^2 + (109/57)^2 = 10$$

Lattice points on spheres

Let n be a positive integer, and consider the integral solutions of

$$x^2 + y^2 + z^2 = n.$$

A solution $(x, y, z) \in \mathbb{Z}^3$ is called primitive if $\gcd(x, y, z) = 1$.

Geometrically, the solutions are the lattice points on the sphere of radius $\sqrt{n}$ centered at the origin. The primitive solutions are the visible lattice points on this sphere.

Questions

1. How many (primitive) solutions are there?
2. How are the (primitive) solutions distributed?

Examples for primitive solutions

Let $r(n)$ be the number of integral solutions of

$$x^2 + y^2 + z^2 = n.$$

Let $r^*(n)$ be the number of primitive solutions.

n	radius	$r^*(n)$	primitive solutions up to permutation
1	1	6	$(\pm 1, 0, 0)$
9	3	24	$(\pm 2, \pm 2, \pm 1)$
25	5	24	$(\pm 4, \pm 3, 0)$
81	9	72	$(\pm 8, \pm 4, \pm 1)$, $(\pm 7, \pm 4, \pm 4)$
225	15	96	$(\pm 14, \pm 5, \pm 2)$, $(\pm 11, \pm 10, \pm 2)$
2025	45	288	$(\pm 44, \pm 8, \pm 5)$, $(\pm 40, \pm 19, \pm 8)$, $(\pm 40, \pm 16, \pm 13)$, $(\pm 37, \pm 20, \pm 16)$, $(\pm 35, \pm 28, \pm 4)$, $(\pm 29, \pm 28, \pm 20)$

Local density of primitive solutions (1 of 2)

Once can express $n \mapsto r(n)$ from $n \mapsto r^*(n)$, and vice versa:

$$r(n) = \sum_{m^2 | n} r^*(n/m^2), \qquad r^*(n) = \sum_{m^2 | n} \mu(m) r(n/m^2).$$

For example, by the table on the previous slide,

$$r(2025) = \sum_{k|45} r^*(k^2) = 6 + 24 + 24 + 72 + 96 + 288 = 510.$$

There is a beautiful formula for $r^*(n)$ due to Gauss (1801) and Dirichlet (1839). We shall understand it as a special case of the mass formula of Siegel (1935).

As a first approximation to $r^*(n)$, we consider

$$\begin{aligned}\sigma_\infty(n) &= \lim_{h \to 0} \frac{\mathrm{vol}\left(\{(x,y,z) \in \mathbb{R}^3 : n \leqslant x^2 + y^2 + z^2 \leqslant n + h\}\right)}{h} \\ &= \frac{d}{dt}\left(\frac{4}{3}\pi t^{3/2}\right)_{|t=n} = 2\pi\sqrt{n}.\end{aligned}$$

Local density of primitive solutions (2 of 2)

The approximation $r^*(n) \approx \sigma_\infty(n)$ is very crude: it does not take into account the distribution of $x^2 + y^2 + z^2$ in various congruence classes. For example, $r^*(n) = 0$ for $n \equiv 0, 4, 7 \pmod 8$.

We adjust $\sigma_\infty(n)$ by the following p-adic densities (for p prime):

$$\sigma_p(n) = \lim_{j\to\infty} \frac{\#\left\{\text{primitive solutions of } x^2+y^2+z^2 \equiv n \pmod{p^j}\right\}}{p^{2j}}.$$

The fraction stabilizes on the right-hand side, and one obtains that

$$\sigma_2(n) = \begin{cases} 3/2, & n \equiv 1,2,5,6 \pmod 8; \\ 1, & n \equiv 3 \pmod 8; \\ 0, & n \equiv 0,4,7 \pmod 8; \end{cases}$$

$$\sigma_p(n) = \frac{1 - \frac{1}{p^2}}{1 - \left(\frac{-n}{p}\right)\frac{1}{p}}, \qquad p > 2.$$

Siegel's maass formula for $r^*(n)$

Theorem (Siegel 1935)

$$r^*(n) = \sigma_\infty(n) \prod_p \sigma_p(n).$$

If $n \equiv 0, 4, 7 \pmod 8$, then $\sigma_2(n) = 0$. Otherwise, let us introduce

$$D = \begin{cases} -4n, & n \equiv 1, 2, 5, 6 \pmod 8; \\ -n, & n \equiv 3 \pmod 8. \end{cases}$$

Then D is a negative discriminant, and $\chi_D(m) = \left(\frac{D}{m}\right)$ is a quadratic Dirichlet character modulo $|D|$. Let

$$L(s, \chi_D) = \sum_{m=1}^{\infty} \frac{\chi_D(m)}{m^s} = \prod_p \left(1 - \frac{\chi_D(p)}{p^s}\right)^{-1}$$

be the corresponding Dirichlet L-function. Then

$$\prod_p \sigma_p(n) = 2 \prod_p \frac{1 - \frac{1}{p^2}}{1 - \frac{\chi_D(p)}{p}} = \frac{12}{\pi^2} L(1, \chi_D).$$

The Dirichlet–Gauss formula for $r^*(n)$

Theorem (Gauss 1801, Dirichlet 1839)

Assume that $n \equiv 1, 2, 3, 5, 6 \pmod 8$. *Then*

$$r^*(n) = \frac{24}{\pi} \sqrt{n}\, L(1, \chi_D).$$

Corollary

Assume that $n \equiv 1, 2, 3, 5, 6 \pmod 8$ *and* $k \equiv 1 \pmod 2$. *Then*

$$r^*(nk^2) = r^*(n) k \prod_{p \mid k} \left(1 - \frac{\chi_D(p)}{p}\right).$$

Example

Let $n = 1$ and $k = 45$. Then $D = -4$, and we infer that

$$r^*(2025) = 6 \cdot 45 \cdot \left(1 + \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 288.$$

Estimating $r^*(n)$ and $r(n)$

We can estimate $r^*(n)$ and $r(n)$ by bounding $L(1, \chi_D)$.

Theorem (Siegel 1935)

If D is a fundamental discriminant, then

$$L(1, \chi_D) = |D|^{o(1)}.$$

Here $o(1)$ abbreviates a quantity that tends to zero as $|D| \to \infty$.

Corollary

Assume that $n \equiv 1, 2, 3, 5, 6 \pmod 8$. Then

$$r^*(n) = n^{1/2+o(1)} \qquad \text{and} \qquad r(n) = n^{1/2+o(1)}.$$

Theorem (Tatuzawa 1951)

Fix $\varepsilon > 0$, and let D be a fundamental discriminant. Then

- $L(1, \chi_D) < \log |D| < (1/\varepsilon)|D|^{\varepsilon}$;
- $L(1, \chi_D) > (\varepsilon/10)|D|^{-\varepsilon}$ *with one possible exception.*

Distribution of lattice points on a large sphere

It turns out that if a large sphere contains many lattice points, then those points are approximately equidistributed in solid angles.

Theorem (Iwaniec 1987, Golubeva–Fomenko 1987)

Assume that $n \equiv 1, 2, 3, 5, 6 \pmod 8$, *and let* P *be a non-constant harmonic polynomial. Consider*

$$r(n, P) = \sum_{x^2+y^2+z^2=n} P\left(\frac{x}{\sqrt{n}}, \frac{y}{\sqrt{n}}, \frac{z}{\sqrt{n}}\right).$$

There exists an absolute constant $\delta > 0$ *such that*

$$r(n, P) \ll_P n^{1/2-\delta}.$$

The same result holds for the primitive version $r^*(n, P)$. The proof utilizes the fact that $n^{(\deg P)/2} r(n, P)$ is the n-th Fourier coefficient of a cusp form of weight $3/2 + \deg P$. The Shimura correspondence is used to reduce the case of general n to the case of square-free n.

Stronger bounds for equidistribution

The work of Iwaniec (1987) shows that any $\delta < 1/28$ is admissible.

The work of Waldspurger (1981, 1991) and Baruch–Mao (2007) implies that $\delta > 0$ is admissible as long as the following $\mathrm{GL}_2 \times \mathrm{GL}_1$-type subconvex bound is valid over $\mathbb{Q}$:

$$L(1/2, \pi \otimes \chi_D) \ll_\pi |D|^{1/2-2\delta}.$$

Blomer–Harcos (2008) allows $\delta < 1/16$; see also Yang (2023).
Conrey–Iwaniec (2000) allows $\delta < 1/12$; see also Nelson (2019).

We can also make a nice connection to the opening slide. Let us restrict n to the square class $10k^2$: then the above bounds yield

$$r(10k^2, P) \ll_P k^{1-2\delta}.$$

In fact, for this special case, the results of Shimura (1973) and Deligne (1974) yield directly that any $\delta < 1/4$ is admissible. Hence for every sufficiently large odd k, there are plenty of reduced triples $(x/k, y/k, z/k) \in \mathbb{Q}^3$ that solve Diophantus' problem.

Primes in arithmetic progressions

The convergence and non-vanishing of

$$L(1,\chi_D)=\sum_{m=1}^{\infty}\frac{\chi_D(m)}{m}=\prod_p\left(1-\frac{\chi_D(p)}{p}\right)^{-1}$$

shows that $\chi_D(p)=1$ happens for about half of the primes p.

Dirichlet (1837) realized that generalizing this statement to all Dirichlet characters $\chi:(\mathbb{Z}/q\mathbb{Z})^\times\to\mathbb{C}^\times$ yields the equidistribution of primes in reduced residue classes modulo q. In fact, for all $\varepsilon>0$, there exists an ineffective constant $c_1=c_1(\varepsilon)>0$ such that

$$|L(\sigma+it,\chi)|\geqslant c_1(q+|t|)^{-\varepsilon},\qquad \sigma\geqslant 1-c_1(q+|t|)^{-\varepsilon}.$$

Theorem (Siegel 1935, Walfisz 1936)

Let $A>0$ be arbitrary, and let $a \pmod q$ be a reduced residue class modulo q. Then

$$\sum_{\substack{p\leqslant x\\ p\equiv a \pmod q}}\log p=\frac{x}{\varphi(q)}+O_A\left(\frac{x}{(\log x)^A}\right).$$

Chebotarev's density theorem

Chebotarev (1923) proved a far-reaching generalization of Dirichlet's theorem, originally conjectured by Frobenius (1896).

Let L/K be a Galois extension of number fields with Galois group G. To each prime ideal $\mathfrak{p}$ in K, we can associate a conjugacy class $\mathrm{Frob}(\mathfrak{p}) \subset G$. The theorem states that if $C \subset G$ is any conjugacy class, then $\{\mathfrak{p} : \mathrm{Frob}(\mathfrak{p}) = C\}$ has relative density $|C|/|G|$.

Using the L-functions of Artin (1923), which are associated to (characters of) the representations of G, we can formulate and prove Chebotarev's density theorem as follows.

Theorem (Chebotarev 1923, Artin 1923 & 1927)

For any $g \in G$, consider the complex function

$$U_G(s,g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{L'}{L}(s,\chi)\overline{\chi}(g).$$

Then $U_G(s,G)$ is meromorphic on $\mathbb{C}$ with simple poles, and it has a simple pole at $s=1$ with residue -1.

A refinement of Chebotarev's density theorem (1 of 2)

The key idea of the proof is that $U_G(s,g) = U_{\langle g\rangle}(s,g)$, which can be proved by Frobenius reciprocity. Hence we can assume $G = \langle g\rangle$, in which case the statement follows from Artin reciprocity.

Along these lines, one can also show that each residue of $U_G(s,g)$ is upper bounded in absolute value by the corresponding residue of $\zeta_L(s)$. This then leads to the following refinement.

Theorem (Foote–Murty 1989, Harcos–Soundararajan 2023)

For any conjugacy class $C \subset G$, consider the Dirichlet series

$$F_G(s,C) := \sum_{\mathrm{Frob}(\mathfrak{p})=C} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^s} - \frac{|C|}{|G|}\sum_{\mathfrak{p}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^s}.$$

Then $F_G(s,C)$ has a meromorphic continuation to $\mathrm{Re}(s) > 1/2$ with simple poles. For any point $s_0 \in \mathbb{C}$ with $\mathrm{Re}(s_0) > 1/2$,

$$\sum_C \frac{|G|}{|C|}\left|\operatorname*{res}_{s=s_0} F_G(s,C)\right|^2 \le \left(\operatorname*{ord}_{s=s_0}\zeta_L(s)\right)^2 - \left(\operatorname*{ord}_{s=s_0}\zeta_K(s)\right)^2.$$

A refinement of Chebotarev's density theorem (2 of 2)

Corollary (Aramata 1931, Brauer 1947)

If L/K is a Galois extension, then $\zeta_L(s)/\zeta_K(s)$ is an entire function.

Corollary (Harcos–Soundararajan 2023)

For $\mathrm{Re}(s_0) > 1/2$, the following statements are equivalent:

1. *s_0 is a zero of $\zeta_L(s)/\zeta_K(s)$;*
2. *s_0 is a pole of $F_G(s, \{1\})$;*
3. *s_0 is a pole of $F_G(s, C)$ for some conjugacy class $C \subset G$.*

Corollary (Harcos–Soundararajan 2023)

For any conjugacy class $C \subset G$, consider the following hypothesis:

$$\sum_{\substack{N(\mathfrak{p}) \leq x \\ \mathrm{Frob}(\mathfrak{p}) = C}} \log N(\mathfrak{p}) = \frac{|C|}{|G|} \sum_{N(\mathfrak{p}) \leq x} \log N(\mathfrak{p}) + O_{C,\varepsilon}(x^{1/2+\varepsilon}).$$

If this holds for $C = \{1\}$, then it holds for the other C's as well.

A new zero-free region for Rankin–Selberg L-functions

Let $\mathfrak{F}_n$ be the set of unitary cuspidal automorphic representations of GL_n over $\mathbb{Q}$. Each $(\pi, \rho) \in \mathfrak{F}_n \times \mathfrak{F}_m$ gives rise to an L-function $L(s, \pi \times \rho)$ of degree nm, called the Rankin–Selberg L-function.

Theorem (Harcos–Thorner 2025)

Let $(\pi, \rho) \in \mathfrak{F}_n \times \mathfrak{F}_m$. For all $\varepsilon > 0$, there exists an ineffective constant $c_2 = c_2(\pi, \rho, \varepsilon) > 0$ such that if $\chi \in \mathfrak{F}_1$, then

$$|L(\sigma, \pi \times (\rho \otimes \chi))| \geqslant c_2 C(\chi)^{-\varepsilon}, \qquad \sigma \geqslant 1 - c_2 C(\chi)^{-\varepsilon}.$$

Theorem (Harcos–Thorner 2025, Jiang 2025+)

Let $(\pi, \rho) \in \mathfrak{F}_n \times \mathfrak{F}_m$. If $\rho = \widetilde{\pi} \otimes |\cdot|^{it}$ for some $t \in \mathbb{R}$, then put $\mathcal{M}_{\pi\times\rho}(x) = x^{1-it}/(1-it)$; otherwise, put $\mathcal{M}_{\pi\times\rho}(x) = 0$. Let $A > 0$. Let $q \leqslant (\log x)^A$ be coprime to the conductors of π, ρ, and let $a \pmod q$ be a reduced residue class modulo q. Then

$$\sum_{\substack{p \leqslant x \\ p \equiv a \pmod q}} \lambda_{\pi\times\rho}(p) \log p = \frac{\mathcal{M}_{\pi\times\rho}(x)}{\varphi(q)} + O_{\pi,\rho,A}\left(\frac{x}{(\log x)^A}\right).$$

Tatuzawa's theorem for Rankin–Selberg L-functions

Theorem (Harcos–Thorner 2025+)

Let $(\pi, \rho, \chi) \in \mathfrak{F}_n \times \mathfrak{F}_m \times \mathfrak{F}_1$ and $\varepsilon > 0$. There exist an effectively computable constant $c_3 = c_3(n, m, \varepsilon) > 0$ and a character $\psi = \psi_{\pi,\rho,\varepsilon} \in \mathfrak{F}_1$ such that if $L(s, \pi \times (\rho \otimes \chi))$ differs from $L(s, \pi \times (\rho \otimes \psi))$, then

$$L(\sigma, \pi \times (\rho \otimes \chi)) \neq 0, \qquad \sigma \geqslant 1 - c_3(C(\pi)C(\rho)C(\chi))^{-\varepsilon}.$$

Moreover, $L(s, \pi \times (\rho \otimes \psi))$ has at most one zero (necessarily simple) in the interval $\sigma \geqslant 1 - c_3(C(\pi)C(\rho)C(\psi))^{-\varepsilon}$.

Corollary

If $(\pi, \rho) \in \mathfrak{F}_n \times \mathfrak{F}_m$ and $\varepsilon > 0$, then $L(\sigma + it, \pi \times \rho)$ has at most one zero (necessarily simple) in the region

$$\sigma \geqslant 1 - c_3(C(\pi)C(\rho)(|t| + 3))^{-\varepsilon}.$$