Equidistribution on the modular surface and L-functions

Gergely Harcos

Alfréd Rényi Institute of Mathematics
http://www.renyi.hu/∼gharcos/

16 November 2011
University of Zagreb

Theorem (Fermat 1654, Euler 1772)

For an odd prime p we have:

$$p = x^2 + y^2 \iff p \equiv 1 \pmod 4$$
$$p = x^2 + 2y^2 \iff p \equiv 1, 3 \pmod 8$$

Proof (sketch).

Right hand side means that p is represented by some integral binary quadratic form $ax^2 + bxy + cy^2$ of discriminant $d = -4$ (resp. $d = -8$). Using the substitutions

$$(x, y) \overset{T}{\mapsto} (x - y, y) \qquad \text{and} \qquad (x, y) \overset{S}{\mapsto} (-y, x)$$

one can achieve that $|b| \leqslant |a| \leqslant |c|$, in which case $ax^2 + bxy + cy^2$ is the form on the left hand side. □

Representing primes by binary quadratic forms (2 of 6)

Definition (Lagrange 1773, Legendre 1798, Gauss 1801)

Two integral binary quadratic forms are (properly) equivalent if one can be brought to the other by an invertible linear substitution

$$(x, y) \mapsto (\alpha x + \beta y, \gamma x + \delta y), \qquad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Theorem

Equivalent forms have the same discriminant. The number of classes of a given nonsquare discriminant d is $\ll_\varepsilon |d|^{1/2+\varepsilon}$.

Proof (sketch).

Every class is represented by some $ax^2 + bxy + cy^2$ such that $|b| \leqslant |a| \leqslant |c|$ and $b^2 - 4ac = d$. Then $3b^2 \leqslant |d|$, and for each b there are $\ll_\varepsilon |d|^\varepsilon$ choices for a and c since $4ac = b^2 - d \neq 0$. □

Definition

Let d be a fundamental discriminant, i.e. a square-free integer $\equiv 1 \pmod 4$, or 4 times a square-free integer $\equiv 2, 3 \pmod 4$. For $d < 0$ we denote by $h(d)$ the number of classes of positive forms of discriminant d. For $d > 0$ we denote by $h(d)$ the number of classes of forms of discriminant d.

Example

The classes of positive forms of discriminant -56 are represented by $x^2 + 14y^2$, $2x^2 + 7y^2$, $3x^2 \pm 2xy + 5y^2$. Hence $h(-56) = 4$.

Theorem

Let n be a positive square-free integer $\equiv 1, 2 \pmod 4$, and let p be a prime not dividing $4n$. Then p is represented by some form of discriminant $-4n$ if and only if $(-n/p) = 1$. The latter condition depends only on $p \mod 4n$.

Representing primes by binary quadratic forms (4 of 6)

Example

Let $p \neq 2, 7$ be a prime. Then p is represented by one of $x^2 + 14y^2$, $2x^2 + 7y^2$, $3x^2 \pm 2xy + 5y^2$ if and only if $p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56}$.

Definition

Two classes of some fundamental discriminant d are in the same genus if they represent the same reduced residues modulo d.

Example

For $d = -56$ there are 2 genera, each consisting of 2 classes:

$$p = x^2 + 14y^2 \text{ or } p = 2x^2 + 7y^2$$
$$\iff p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$$
$$p = 3x^2 + 2xy + 5y^2 \text{ or } p = 3x^2 - 2xy + 5y^2$$
$$\iff p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}$$

Representing primes by binary quadratic forms (5 of 6)

- The classes of discriminant d considered above form a finite abelian group H_d under a natural group law called Gauss composition. We have seen that it is of size $h(d) \ll_\varepsilon |d|^{1/2+\varepsilon}$. In the case of a fundamental discriminant d the group is isomorphic to the narrow ideal class group of the number field $\mathbb{Q}(\sqrt{d})$, the multiplicative group of nonzero fractional ideals modulo totally positive principal fractional ideals.
- Each genus is a coset of H_d^2, hence the number of genera is a power of 2, namely the order of the elementary abelian group H_d/H_d^2. In other words, genera can be distinguished by quadratic characters of the class group H_d.
- One can distinguish classes within a genus by class field theory. For example, in the case of a fundamental discriminant d, one studies the maximal unramified extension of $\mathbb{Q}(\sqrt{d})$, a Galois extension with Galois group isomorphic to H_d.

Representing primes by binary quadratic forms (6 of 6)

Theorem (taken from Cox's wonderful book)

Let n be a positive square-free integer $\equiv 1, 2 \pmod 4$. There is an irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ such that for a prime dividing neither n nor the discriminant of $f_n(x)$,

$$p = x^2 + ny^2 \iff (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \pmod p \text{ has an integer solution.}$$

Example

For a prime $p \neq 2, 7$ we have:

$$p = x^2 + 14y^2 \iff$$
$$p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56} \text{ and}$$
$$x^4 + 2x^2 - 7 \equiv 0 \pmod p \text{ has an integer solution.}$$

Geometric picture (1 of 2)

Consider the upper half-plane $\mathcal{H}$ together with its boundary $\mathbb{R} \cup \{\infty\}$. The group $\mathsf{SL}_2(\mathbb{R})$ acts on this object by fractional linear transformations

$$z \overset{g}{\longmapsto} \frac{\alpha z + \beta}{\gamma z + \delta}, \qquad g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathsf{SL}_2(\mathbb{R}).$$

Equip $\mathcal{H}$ with the $\mathsf{SL}_2(\mathbb{R})$-invariant line element and corresponding area element

$$d^2 s(z) := \frac{dx^2 + dy^2}{y^2} \quad \text{and} \quad d\mu(z) := \frac{3}{\pi}\, \frac{dxdy}{y^2}.$$

Then the geodesics in $\mathcal{H}$ are the half-lines and semi-circles orthogonal to $\mathbb{R}$: they obey the axioms of hyperbolic geometry.

Geometric picture (2 of 2)

Decompose each form of some fundamental discriminant d as

$$ax^2 + bxy + cy^2 = a(x - uy)(x - wy),$$

$$u := \frac{-b - \sqrt{d}}{2a}, \qquad w := \frac{-b + \sqrt{d}}{2a}.$$

For $d < 0$ consider the unique root in $\mathcal{H}$, while for $d > 0$ join the two roots by a semi-circle in $\mathcal{H}$. The actions of $\mathrm{SL}_2(\mathbb{Z})$ on forms and on $\mathcal{H} \cup \mathbb{R} \cup \{\infty\}$ are compatible, hence by projection to the modular surface $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$, we obtain $h(d)$ special points or geodesics depending on the sign of d. For $d > 0$ the projected geodesics are closed of length $2\ln(\lambda_d)$, where $\lambda_d > 1$ generates the group of positive units in $\mathbb{Q}(\sqrt{d})$.

Question (Linnik 1968)

Let $d \to -\infty$ (resp. $d \to \infty$) run through fundamental discriminants. How are the $h(d)$ special points (resp. closed geodesics) of discriminant d distributed in $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$?

Dirichlet's class number formula and Siegel's theorem

- Λ_d: the set of special points or closed geodesics on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ representing the $h(d)$ classes of forms of discriminant d
- w_d: the number of roots of unity in $\mathbb{Q}(\sqrt{d})$

Theorem (Dirichlet 1839)

Let d be a fundamental discriminant. Then we have

$$h(d) = \frac{w_d}{2\pi}\,|d|^{\frac{1}{2}}\,L(1,(\tfrac{d}{\cdot})), \qquad d<0,$$
$$h(d)\ln(\lambda_d) = \frac{w_d}{2}\,|d|^{\frac{1}{2}}\,L(1,(\tfrac{d}{\cdot})), \qquad d>0.$$

Theorem (Siegel 1934)

Let d be a fundamental discriminant. Then we have

$$|d|^{-\varepsilon} \ll_\varepsilon L(1,(\tfrac{d}{\cdot})) \ll_\varepsilon |d|^{\varepsilon}.$$

Equidistribution and L-functions (1 of 4)

- H_d: the narrow ideal class group of $\mathbb{Q}(\sqrt{d})$ acting on Λ_d

Theorem (Zhang 2001, Du–Fr–Iw 2002, Popa 2006, Ha–Mi 2006)

Let d be a fundamental discriminant, and $H \leqslant H_d$ be a subgroup. Let $g : \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \to \mathbb{C}$ be a smooth function of compact support.

- *If $d < 0$ and $z_0 \in \Lambda_d$ is a Heegner point, then*

$$\frac{\sum_{\sigma\in H} g(z_0^\sigma)}{\sum_{\sigma\in H} 1} = \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} g(z)\,d\mu(z) + O_g\left([H_d : H]|d|^{-\frac{1}{2827}}\right).$$

- *If $d > 0$ and $G_0 \in \Lambda_d$ is a closed geodesic, then*

$$\frac{\sum_{\sigma\in H} \int_{G_0^\sigma} g(z)\,ds(z)}{\sum_{\sigma\in H} \int_{G_0^\sigma} 1\,ds(z)} = \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} g(z)\,d\mu(z) + O_g\left([H_d : H]|d|^{-\frac{1}{2827}}\right).$$

Equidistribution and L-functions (2 of 4)

By applying harmonic analysis on the finite abelian group H_d and on the modular surface $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$, one can reduce the above equidistribution result to cancelation in certain Weyl-sums. It suffices to establish

$$\sum_{\sigma\in H_d}\overline{\psi(\sigma)}g(z_0^\sigma) \ll (1+|t|)^A\,|d|^{\frac{1}{2}-\frac{1}{2826}}, \qquad d<0,$$

$$\sum_{\sigma\in H_d}\overline{\psi(\sigma)}\int_{G_0^\sigma} g(z)\,ds(z) \ll (1+|t|)^A\,|d|^{\frac{1}{2}-\frac{1}{2826}}, \qquad d>0,$$

with an absolute constant $A>0$, where $\psi : H_d\to\mathbb{C}^\times$ is a character, and g is an L^2-normalized Hecke–Maass cusp form or a standard Eisenstein series $E(\cdot,\frac{1}{2}+it)$ of Laplacian eigenvalue $\frac{1}{4}+t^2$ for the modular group $\mathrm{SL}_2(\mathbb{Z})$.

By formulae of Zhang (2001) for $d < 0$ and Popa (2006) for $d > 0$, which are based on the deep work of Waldspurger (1981), the left hand side is related to central values of Rankin–Selberg L-functions:

$$\left| \sum_{\sigma \in H_d} \overline{\psi(\sigma)} \ldots \right|^2 = c_d \, |d|^{\frac{1}{2}} \, |\rho_g(1)|^2 \, \Lambda\left(f_\psi \otimes g, \tfrac{1}{2}\right).$$

Here c_d is positive and takes only finitely many different values, $\rho_g(1)$ is the first Fourier coefficient of g, $\Lambda(\pi, s)$ denotes the completed L-function, and f_ψ is the automorphic induction of ψ from GL_1 over $\mathbb{Q}(\sqrt{d})$ to GL_2 over $\mathbb{Q}$ such that $\Lambda(f_\psi, s) = \Lambda(\psi, s)$. The modular form f_ψ was discovered by Hecke (1937) and Maass (1949) in this special case, it is of level $|d|$ and nebentypus $\left(\frac{d}{\cdot}\right)$.

Equidistribution and L-functions (4 of 4)

Using standard bounds for $\rho_g(1)$ and the gamma factors included in $L_\infty\left(f_\psi \otimes g, \frac{1}{2}\right)$, one can further reduce equidistribution to the following subconvex bound for the finite Rankin–Selberg L-function (with a different $A > 0$):

$$L\left(f_\psi \otimes g, \tfrac{1}{2}\right) \ll (1 + |t|)^A \, |d|^{\frac{1}{2} - \frac{1}{1413}}.$$

If ψ is not quadratic and g is cuspidal, then the above L-value is a genuine $\mathrm{GL}_2 \times \mathrm{GL}_2$ L-value. In this case the subconvex bound was proved by Harcos–Michel (2006). Otherwise we are dealing with a product of two GL_2 L-values, or two $\mathrm{GL}_2 \times \mathrm{GL}_1$ L-values, or four GL_1 L-values. In this case the subconvex bound was proved by Duke–Friedlander–Iwaniec (2002) and Blomer–Harcos–Michel (2007), Conrey–Iwaniec (2000), and Burgess (1963).