Quadratic forms, elliptic curves, and modular forms

Jens Funke

University of Durham

January 9, 2009

Some very classical number theory

Number of ways a number N can be written as the sum of m squares:

$$r_m(N) = \#\left\{(x_1, x_2, \ldots, x_m) \in \mathbb{Z}^m : \sum_{i=1}^{m} x_i^2 = N\right\},$$

Classical problem: Find formulas for $r_m(N)$ (at least for small m).

$$r_4(N) = 8 \sum_{\substack{d>0, d|N \\ 4\nmid d}} d \quad = 8(p+1) \quad \text{if } N = p \text{ is prime}$$

(Similar formulas for $r_2(N)$, $r_6(N)$, $r_8(N)$).

Another problem: Find at least asymptotic formulas as $N \to \infty$.

Three quadratic forms(1)

$P(x,y,u,v)$

$$\begin{aligned} P(x,y,u,v) &= x^2+xy+3y^2+u^2+uv+3v^2 \\ &= (x+\tfrac{1}{2}y)^2+\tfrac{11}{4}y^2+(u+\tfrac{1}{4}v)^2+\tfrac{11}{4}v^2. \end{aligned}$$

$$2P(x,y,u,v) = (x,y,u,v)S\begin{pmatrix} x\\ y\\ u\\ v\end{pmatrix} \qquad \text{with} \qquad S = \begin{pmatrix} 2 & 1 & & \\ 1 & 6 & & \\ & & 2 & 1 \\ & & 1 & 6 \end{pmatrix}.$$

Note

$$\det S = 11^2.$$

Set

$$r_S(N) = \#\{(x,y,u,v)\in\mathbb{Z}^4 : P(x,y,u,v)=N\}.$$

Three quadratic forms(2)

$Q(x, y, u, v)$

$$Q(x, y, u, v) = 2(x^2 + y^2 + u^2 + v^2) + 2xu + xv + yu - 2yv$$

Note

$$2Q(x, y, u, v) = (x, y, u, v)T \begin{pmatrix} x \\ y \\ u \\ v \end{pmatrix} \qquad \text{with} \qquad T = \begin{pmatrix} 4 & & 2 & 1 \\ & 4 & 1 & -2 \\ 2 & 1 & 4 & \\ 1 & -2 & & 4 \end{pmatrix}$$

$$\det T = 11^2.$$

Set

$$r_T(N) = \#\{(x, y, u, v) \in \mathbb{Z}^4 : Q(x, y, u, v) = N\}.$$

Three quadratic forms(3)

$R(x, y, u, v)$

$$R(x, y, u, v) = x^2 + 4(y^2 + u^2 + v^2) + xu + 4yu + 3yv + 7uv$$

Note

$$2R(x, y, u, v) = (x, y, u, v)U \begin{pmatrix} x \\ y \\ u \\ v \end{pmatrix} \qquad \text{with} \qquad U = \begin{pmatrix} 2 & & 1 & \\ & 8 & 4 & 3 \\ 1 & 4 & 8 & 7 \\ & 3 & 7 & 8 \end{pmatrix}$$

$$\det U = 11^2.$$

Set

$$r_U(N) = \#\{(x, y, u, v) \in \mathbb{Z}^4 : R(x, y, u, v) = N\}.$$

A little theory

- P, Q, R (S, T, U) are positive definite integral integral (actually "even", i.e. with even diagonal) quaternary quadratic forms of determinant 11^2.
- Call two such quadratic forms *equivalent* if they differ by a change of basis for $\mathbb{Z}^4$. On the level of Gram matrices this is

$$S \sim T \qquad \text{if} \qquad ASA^t = T \qquad \text{with} \quad A \in GL_4(\mathbb{Z}).$$

Non trivial fact

There are 3 equivalence classes of such forms with determinant 11^2. These classes are represented by P, Q, R (resp. S, T, U).

Representation numbers:

$$P(x,y,u,v) = x^2 + xy + 3y^2 + u^2 + uv + 3v^2$$

$$Q(x,y,u,v) = 2(x^2 + y^2 + u^2 + v^2) + 2xu + xv + yu - 2yv$$

$$R(x,y,u,v) = x^2 + 4(y^2 + u^2 + v^2) + xu + 4yu + 3yv + 7uv$$

N	$r_S(N)$	$r_T(N)$	$r_U(N)$
1	4	0	6
2	4	12	0
3	8	12	6
4	20	12	24
5	16	12	18
6	32	24	36
7	16	24	12
8	36	36	36
11	4	0	6
13	40	24	48
17	40	48	36
19	48	48	48

Questions/Issues

- Find exact formulas for the representation numbers $r_S(N), r_T(N), r_U(N)$.
- Find asymptotic formulas for the representation numbers $r_S(N), r_T(N), r_U(N)$.
- Are there linear relations between the representation numbers $r_S(N), r_T(N), r_U(N)$?
- Study the difference between two of the representation numbers, say $r_S(N) - r_T(N)$.

Representation numbers:

N	$r_S(N)$	$r_T(N)$	$r_U(N)$
1	4	0	6
2	4	12	0
3	8	12	6
5	16	12	18
7	16	24	12
11	4	0	6
13	40	24	48
17	40	48	36
19	48	48	48

Theorem (Hecke)

$$\tfrac{1}{4} r_S(N) + \tfrac{1}{6} r_T(N) = \tfrac{1}{4} r_T(N) + \tfrac{1}{6} r_U(N)$$

$$\boxed{\frac{3}{2} r_S(N) - \frac{1}{2} r_T(N) = r_U(N)}$$

Representation numbers (2)

$$P(x,y,u,v) = x^2 + xy + 3y^2 + u^2 + uv + 3v^2$$

$$Q(x,y,u,v) = 2(x^2 + y^2 + u^2 + v^2) + 2xu + xv + yu - 2yv$$

p	$r_S(p)$	$r_T(p)$	$\frac{1}{4}(r_S(p) - r_T(p))$
2	4	12	-2
3	8	12	-1
5	16	12	1
7	16	24	-2
13	40	24	4
17	40	48	-2
19	48	48	0
23	56	60	-1
29	72	72	0
31	88	60	7
37	96	84	3
41	88	120	-8
43	96	120	-6
47	128	96	8

A particular elliptic curve

$$E : G(x,y) = y^2 + y - x^3 + x^2 = 0$$
$$f(y) := y^2 + y = x^3 - x^2 =: g(x)$$

- Looking at the curve in projective space, one obtains an additional point ∞.
- *Important feature*: For K an arbitrary field $E(K)$ as the structure of an abelian group.
- Testing ground for far reaching conjectures in number theory/algebraic geometry.
- TODAY: Reduce mod (p) for p prime and count the number of solutions:

$$\#E(\mathbb{F}_p).$$

$p = 5$: $y^2 + y = x^3 - x^2$

- $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ has 5 elements:

n	$y^2 + y$	$x^3 - x^2$
0	0	0
1	2	0
2	1	4
3	2	3
4	0	3

Get points

$$(0,0) \quad (1,0) \quad (0,4) \quad (1,4) \quad \infty$$

p	$\#E(\mathbb{F}_p) : y^2 + y - x^3 + x^2 = 0$
2	5
3	5
5	5
7	10
13	10
17	16
19	20
23	23
29	30
31	25
37	35
41	50
43	50
47	40
53	60

Heuristical argument: $E(\mathbb{F}_p)$ should have $p+1$ points. WHY?

- Roughly half of numbers $\pmod p$ are squares. So $f(y) = y^2 + y$ takes roughly half of the values $\pmod p$.
- $g(x) = x^3 - x^2$ takes random values. So for a given x, the probability of $g(x)$ hitting a square is roughly $1/2$. If we do, we get (typically) *two* points on the affine part of the curve.
- Have p possibilities for x. So the expected value of the affine points on E is $\frac{1}{2} \cdot 2 \cdot p = p$.
- "∞"$\longrightarrow p+1$ points.

Theorem (Hasse):

$$|p + 1 - E(\mathbb{F}_p)| \leq 2\sqrt{p}.$$

p	$\#E(\mathbb{F}_p)$	$a_p := p + 1 - E(\mathbb{F}_p)$
2	5	-2
3	5	-1
5	5	1
7	10	-2
13	10	4
17	16	2
19	20	0
23	23	1
29	30	0
31	25	7
37	35	3
41	50	-8
43	50	-6
47	40	8
53	60	-6

p	$r_S(p)$	$r_T(p)$	$\frac{1}{4}(r_S(p) - r_T(p))$	a_p
2	4	12	-2	-2
3	8	12	-1	-1
5	16	12	1	1
7	16	24	-2	-2
13	40	24	4	4
17	40	48	-2	-2
19	48	48	0	0
23	56	60	-1	-1
29	72	72	0	0
31	88	60	7	7
37	96	84	3	3
41	88	120	-8	-8
43	96	120	-6	-6
47	128	96	8	8
53	120	144	-6	-6

Madness

Quadratic Forms

$$P(x, y, u, v) = x^2 + xy + 3y^2 + u^2 + uv + 3v^2$$
$$Q(x, y, u, v) = 2(x^2 + y^2 + u^2 + v^2) + 2xu + xv + yu - 2yv$$

Elliptic Curve

$$E : G(x, y) = y^2 + y - x^3 + x^2 = 0$$

Theorem (Eichler?)

For all $p \neq 11$ prime, we have

$$\boxed{p + 1 - \#E(\mathbb{F}_p) = \frac{1}{4}(r_S(p) - r_T(p)).}$$

Langlands

- This example is from a unpublished manuscript by Langlands from 1973.
- Langlands writes: "I have been unable to convince myself that the theorems are *trivial*.
- "As I said in a letter to Weil almost six years ago, one can hope that the theory of automorphic forms on reductive groups will eventually lead to general theorems of the same sort."

Modular Forms

A modular form (for the purposes of this talk):

- A holomorphic function f on the upper half plane
$$\mathbb{H} = \{z = x + iy : y > 0\}.$$
- $$f\left(\tfrac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$
for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $N \mid c$. ("level N", "weight k")
- In particular, applying $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ we obtain $f(z+1) = f(z)$.
- The Fourier expansion of f starts at $n = 0$:
$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$$

If $a_0 = 0$, then we call f a cusp form.

Theta Series

For the quadratic forms P, Q, R (resp. S, T, U), set

$$\theta(z, S) = \sum_{\mathbf{x}\in\mathbb{Z}^4} e^{2\pi i P(\mathbf{x})z} = \sum_{\mathbf{x}\in\mathbb{Z}^4} e^{\pi i\, {}^t\mathbf{x}S\mathbf{x}z}$$
$$= \sum_{n\geq 0} r_S(n) e^{2\pi i n z}$$

Generating series for the representation numbers $r_S(n)$.
(Same for T and U)

Theorem (classical, harmonic analysis)

$\theta(z, S)$ is a modular form of weight 2 and level 11. (Same for T and U).

So have three modular forms of weight 2 and level 11:

$$\theta(z,S) \qquad \theta(z,T) \qquad \theta(z,U)$$

But the space of modular forms of weight 2 and level 11 is only two-dimensional. Moreover, there is one "easy" modular form, the level 11 Eisenstein series of weight 2

$$E_2(z) = \sum_{n=0}^{\infty} b_n e^{2\pi i n z} \qquad \text{with} \qquad b_p = p+1 \qquad (p \neq 11 \text{prime})$$

Staring again at $r_S(n), r_T(n), r_U(n)$, we directly obtain a proof for

Linear Relation

$$\frac{1}{4}\theta(z,S) + \frac{1}{6}\theta(z,T) = \frac{1}{4}\theta(z,T) + \frac{1}{6}\theta(z,U) = E_2(z)$$

$$\frac{1}{4}r_S(n) + \frac{1}{6}r_T(n) = \frac{1}{4}r_T(n) + \frac{1}{6}r_U(n) \qquad = n+1 \quad (\text{if } n \text{ prime})$$

Elliptic Curves vs. Modular Forms

Eichler-Shimura (50-60's):

Given a modular cusp form $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ of weight 2 and level N, can construct an elliptic curve E of so called conductor N such that

$$p + 1 - E(\mathbb{F}_p) = a_p \qquad (p \nmid N)$$

Taniyama-Shimura Conjecture, Theorem of Wiles et al.:

Can go the other way around. That is, every integral elliptic curve is modular.

$$\frac{1}{4}(\theta(z,S) - \theta(z,T)) \longleftrightarrow E : y^2 + y = x^3 - x^2$$

- There are more sophisticated (geometric) versions/interpretations of this correspondence.

Service of Modular Forms for Elliptic Curves

Fermat's Last Theorem

Given $\alpha^\ell + \beta^\ell = \gamma^\ell$ with α, β, γ coprime integers and $\ell \geq 5$ a prime, construct an elliptic curve

$$E : y^2 = x(x - \alpha^\ell)(x + \beta^\ell)$$

By T-S-Wiles get a modular form f with certain properties.
(Hard) work of Frey-Ribet-Serre then shows that such an f cannot exist.

L-functions

- For $f = \sum_{n=0}^{\infty} a_n e^{2\pi inz}$ a modular (cusp) form of weight 2 (k is also ok), form its L- series

$$L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s} \qquad\qquad Re(s) \gg 0$$

- This (should) encodes interesting information about f and its Fourier coefficients.
- From the transformation properties of f it follows (rather easily) that $L(f,s)$ has an analytic continuation to $\mathbb{C}$ and

$$L(f, 2-s) \leftrightarrow L(f,s)$$

- These are generalizations of the Riemann ζ-function

$$\zeta(s) = \sum_{N=1}^{\infty} n^{-s}.$$

Hasse-Weil L-function

For E an integral elliptic curve, set $a_p = p + 1 - |E(\mathbb{F}_p)|$ and define

$$L(E,s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \qquad Re(s) > 3/2$$

- $L(E,s)$ should encode very important information about E.
- Expect: Analytic continuation and functional equation etc.
- Problem: Impossible by itself.
- Solution: Wiles: $L(E,s) = L(f,s)$ for some modular form f
- Mordell-Weil: $E(\mathbb{Q})$ is a finitely generated abelian group:

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times \text{finite}.$$

Birch-Swinnerton-Dyer conjecture (weak form):

$$(\text{order of vanishing of } L(E,s) \text{ at } s=1) = \text{rank of } E(\mathbb{Q}) = r$$

Service of Elliptic Curves for Modular Forms

Two kinds of modular forms:

- Eisenstein series such as E_2
- Cusp Forms such as $\frac{1}{4}(\theta(z,S) - \theta(z,T))$

- Fourier coeff. of Eisenstein series are easy: $\sigma(p) = p + 1$
- Fourier coeff. of cusp forms are mysterious: a_p
- Have $|a_p| \leq 2\sqrt{p}$ by the connection to elliptic curves and Hasse's theorem. The theory of modular forms cannot obtain this bound by itself. It needs the connection to algebraic geometry.
- (Generalization of this bound to modular forms of arbitrary weight k: Deligne as a consequence of his proof of the Weil conjectures)

Bounds for representation numbers

$$\boxed{\theta(z,S) = \frac{12}{5}\cdot E_2(z) \quad + \quad \frac{8}{5}\cdot[\tfrac{1}{4}(\theta(z,S)-\theta(z,T))]}.$$

So

$$\boxed{r_S(p) = \frac{12}{5}(p+1) + \frac{8}{5}a_p}$$

Thus

$$\boxed{|r_S(p) - \frac{12}{5}(p+1)| \leq \frac{16}{5}\sqrt{p}}$$

So for my favorite prime $p = 1,000,003$, have

$r_S(p) \sim 2,400,007$ up to an error of at most 3200

A Glimpse at the Langlands Program

- Modular forms are examples of an automorphic form/representation for the group GL_2 (or SL_2), the invertible 2×2 matrices.

  $SL_2(\mathbb{R})$ acts on the upper half plane $\mathbb{H}$ by Möbius transformations: $\mathbb{H} \simeq SL_2(\mathbb{R})/SO(2)$.
- Can define automorphic forms associated to other algebraic groups as well, such as GL_n or orthogonal groups. Furthermore, can attach L-functions to these forms.
- For GL_1, important examples of automorphic forms are Dirichlet characters:

  $$\text{Homomorphisms: } (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$$

  L-function: Dirichlet L-series:

  $$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) n^{-s}.$$

Aspect I: Functoriality

- Langlands functoriality predicts that one can transfer automorphic forms from one group to another (in certain situations depending on some data). This transfer behaves "nice" with respect to L-functions etc..
- Each case of functoriality is hard, deep and has (is expected to have) substantial arithmetic consequences.
- TODAY: The quaternary quadratic forms can be interpreted associated to a definite quaternion algebra D over $\mathbb{Q}$. The theta series are the transfer/lift from the "trivial" (automorphic) representation associated to D to GL_2.

  The theta series are classical, but in terms of automorphic forms this is the so-called Jacquet-Langlands correspondence.

Aspect II: Non-abelian class field theory

- HOLY GRAIL: Understand the Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.
- For $K/\mathbb{Q}$ a finite Galois extension, its Galois group $Gal(K/\mathbb{Q})$ captures its arithmetic.
- Example: $K = \mathbb{Q}(i)$, $Gal(K/\mathbb{Q}) \simeq \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$.

  Question: Which rational prime numbers p stay prime in $\mathbb{Z}[i]$?

  - If $p \equiv 1 \pmod 4$, then p splits:
    $p = (a+ib)(a-ib) = a^2 + b^2$, $13 = (3+2i)(3-2i) = 9+4$.
  - If $p \equiv 3 \pmod 4$, then p is inert, ie., stays prime.
  - Splitting behavior is determined by $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$.
  - Splitting behavior is determined by the (unique) Dirichlet character $\chi : (\mathbb{Z}/4\mathbb{Z})^\times \to \{\pm 1\}$:

$$\chi(1) = +1 \qquad \chi(3) = -1.$$

Aspect II: Non-abelian class field theory

- In general: If $K/\mathbb{Q}$ has abelian Galois group, then the splitting behavior is determined by congruences $(\mathbb{Z}/N\mathbb{Z})^\times$, ie, by Dirichlet characters $\pmod{N}$, ie, by automorphic forms for GL_1.
- If $K = \mathbb{Q}(\zeta_N)$, the N-th cyclotomic field, then a rational prime p splits completely if and only if $p \equiv 1 \pmod{N}$.
- If $Gal(K/\mathbb{Q})$ is non-abelian, then for a complex representation $\rho : Gal(K/\mathbb{Q}) \to GL_n(\mathbb{C})$ can study its Artin L-function $L(\rho, s)$ (generalizations of the Dirichlet L-series.)
- Artin-Langlands conjecture: $L(\rho, s)$ comes from the L-function of an automorphic representation of GL_n. In fact, there should be a correspondence between n-dimensional complex representations ρ of the Galois group $Gal(K/\mathbb{Q})$ and automorphic representations of GL_n.

Aspect II: Non-abelian class field theory

- Arithmetic consequences. Example: $K = \mathbb{Q}(\theta)$ with $\theta^3 - \theta - 1 = 0$. For $p \neq 23$, the following can happen
  - (I) p splits into the product of three different prime (ideals)
  - (II) p splits into the product of two different prime (ideals)
  - (III) p stays prime.
- Consider the modular form f of weight 1 and level 23:

$$f(z) = e^{2\pi iz} \prod_{n=1}^{\infty}(1 - e^{2\pi inz})(1 - e^{46\pi inz}) = \sum_{n=1}^{\infty} b_n e^{2\pi inz}$$

  - (I) $b(p) = +2$
  - (II) $b(p) = 0$
  - (III) $b(p) = -1$
- Not much is known beyond certain cases for GL_2.

Aspect III: ℓ-adic representations

- Associated to an elliptic curve one can construct an ℓ-adic representation:

  $$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{Q}}_\ell),$$

  whose L-function is the L-function $L(E, s)$ from before.
- Wiles showed that this representation is modular.

Indefinite quadratic forms

- Study analogous questions associated to forms such as

$$x^2 + y^2 - z^2 \qquad 4ac - b^2 \qquad x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots x_{p+q}^2$$

- The naive theta series and generating series for the representation numbers no longer make sense (convergence collapses, representation numbers become infinite).
- Can associate to an indefinite quadratic form a **geometric** object: Its symmetric space (and also locally symmetric spaces). Study certain "nice" submanifolds (and the (co)homology class they define) and analogous generating series for these cycles.
- For $4ac - b^2$, the symmetric space is $\mathbb{H}$ on which $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ acts by Moebius transformations. For $\mathbf{x} = (a, b, c) \in \mathbb{Z}^3 = L$ with $4ac - b^2 = N > 0$, associate the root $C_{\mathbf{x}}$ of $az^2 + bz + c = 0$ in $\mathbb{H}$ (cycle). Get a composite cycle

$$C_N = \sum_{\mathbf{x}=(a,b,c)\in\mathbb{Z}^3,\, 4ac-b^2=N, \quad \bmod \ \mathrm{SL}_2(\mathbb{Z})} C_{\mathbf{x}}.$$

- Applications in number theory, representation theory and (arithmetic) geometry.
- (Gauss-Kronecker):

$$r_3(D) = 12\left(H(4D) - 2H(D)\right),$$

where $H(D)$ is the class number of integral binary positive definite quadratic forms $\left(\begin{smallmatrix} 2a & b \\ b & 2c \end{smallmatrix}\right)$ of given discriminant $-D = b^2 - 4ac$.

(The generating series $\sum_D (\#C_D)\, e^{2\pi i D\tau}$ is almost a modular form).

Propaganda

- Modular/automorphic forms play a (the?) central role in modern number theory
- Y. Petridis (UCL) will say more about modular/automorphic forms - analytic aspects.
- Durham has a great group in algebra and number theory (yes, we do modular forms!).
- Other places are Bristol, Cambridge, Imperial, Nottingham, Sheffield, UCL, Warwick (list surely incomplete)