Divisibilities of Hurwitz class numbers

Martin Raum

Wednesday, July 10, 2020

Chalmers tekniska högskola
Gothenburg, Sweden

Hurwitz class numbers

Definition

Given a negative discriminant D, the Hurwitz class number is twice the number of automorphism-weighted positive definite, integral, binary quadratic forms of discriminant D.

$$H(D) := 2\#\{aX^2 + bXY + cY^2 : a, b, c \in \mathbb{Z}, b^2 - 4ac = D\} /\!/ \mathrm{SL}_2(\mathbb{Z}).$$

If $D \equiv 3 \pmod 4$ or $D \equiv 2 \pmod 4$, then $H(D) = 0$.

Undefined values of H are set to 0, for convenience.

Denominators divisors of 6: $H(D) \in \frac{1}{6}\mathbb{Z}$.

Class numbers of imaginary quadratic fields

For negative fundamental discriminants D, $H(D)$ is the class number $h(D)$ of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$. It should behave mostly erratic; we expect it to exhibit almost no patterns.

Example values

$$H(0) := \frac{-1}{12},\ H(-3) = \frac{1}{3}, H(-4) = \frac{1}{2}, H(-12) = \frac{4}{3},$$
$$H(-7) = H(-8) = H(-11) = 1.$$

For large values of n, $H(n)$ grows sub-polynomially

$$H(995) = 8, H(996) = 12, H(999) = 32,$$
$$H(9\,999) = 110, H(99\,999) = 336, H(999\,999) = 1\,216.$$

Modular generating series

The generating series for Hurwitz class numbers is the holomorphic part of a real-analytic Eisenstein series.

$$E_{\frac{3}{2}}(\tau) := \sum_D H(D) e(-D\tau) + \frac{1}{8\pi} y^{-\frac{1}{2}} + \frac{1}{8\sqrt{\pi}} \sum_{n \in \mathbb{Z}\setminus\{0\}} |n| \Gamma\left(-\tfrac{1}{2}, 4\pi n^2 y\right) e(-n^2\tau),$$

where $\tau = x + iy \in \mathbb{H}$, the upper half plane, $e(\tau) := \exp(2\pi i \tau)$, and Γ is the upper incomplete Gamma function.

Divisibility on arithmetic progressions

Among all regular patterns arithmetic progressions are one of the simplest.

For which prime numbers ℓ and integers $a > 0$ and b do we have

$$\forall n \in \mathbb{Z} \colon H(an - b) \equiv 0 \pmod{\ell}?$$

Torsion in class groups

Classical question: What is the factorization of $h(D) = H(D)$ for fundamental discriminants D?

Divisibility by ℓ: One factor of $h(D)$, and thus ℓ-torsion elements in the class group of $\mathbb{Q}(\sqrt{-D})$.

Divisibility statistics

Factorization of $h(D)$ *statistically* predicted by the Cohen–Lehnstra heuristics.

Recently refined by Holmin–Jones–Kurlberg–McLeman–Petersen.

Except for $\ell = 2$ (Gauß), nothing is known about divisibility *patterns* of $h(D)$, and no such patterns are expected. This is different for $H(D)$.

Ramanujan-type congruences for modular forms

When does the holomorphic part of $E_{\frac{3}{2}}$ have Ramanujan-type congruences modulo ℓ on arithmetic progressions $an+b$?

For the partition function, we have $\ell \mid a$ (Radu, Ahlgren-Ono Conjecture).

For mock theta series, in all known cases, we must have $c^-(an+b)=0$ for all n (Andersen).

Exploring congruences

Computer implementation

Available implementations of Hurwitz class numbers were not fast enough to serve sufficient data quickly: Results comprise some terabytes.

Based on Eichler-Hurwitz recursions, I provided a new implementation. The key point is to respect hardware architecture: cache hierarchy and vector instructions.

Congruences found

Some congruences found:

$$H(2^6(4n-1)) \equiv H(3^8(3n-1)) \equiv H(5^2(5n-2)) \equiv H(5^2(5n-3))$$
$$\equiv H(7^2(7n-3)) \equiv H(7^2(7n-5)) \equiv H(7^2(7n-6)) \equiv 0 \pmod{7}.$$

$$H(2^6(8n-3)) \equiv H(3^9(3n-1)) \equiv H(3^9(3n-2))$$
$$\equiv H(5^6(5n-2)) \equiv H(5^6(5n-3)) \equiv H(11^2(11n-2)) \equiv H(11^2(11n-6))$$
$$\equiv H(11^2(11n-7)) \equiv H(11^2(11n-8)) \equiv H(11^2(11n-10)) \equiv 0 \pmod{11}.$$

Observations

We focus on congruences modulo $\ell \geq 5$, and maximal arithmetic progressions $a\mathbb{Z} - b$ with respect to inclusion of sets.

Then a is a prime power say of p, b exhausts square classes in $\mathbb{Z}/a\mathbb{Z}$, and $p = \ell$ if and only if $-b$ is a square modulo a.

The later is equivalent to having a non-holomorphic modular completion of the generating function

$$\sum_n H(-(an+b))e((an+b)\tau).$$

Comparison to other congruences

For the partition function a is usually not a prime power. This is connected to the singularities at cusps of $1/\eta(\tau)$.

For the partition function (Radu) and in fact all weakly holomorphic modular forms (R.) b exhausts square classes. The argument extends to Hurwitz class numbers if $-b$ is not a square modulo a.

The "non-holomorphic" congruences have no analogue in the literature. The fact that $\ell \mid a$ for the partition function (Radu, Ahlgren-Ono conjecture) has different reasons.

Hurwitz class number formula

The fact that $E_{\frac{3}{2}}$ is an eigenform with Shimura lifts multiples of E_2 is captured by

$$H(Df^2) = H(D)\frac{w(Df^2)}{w(D)}\sum_{d\,|\,f} d\prod_{p\,|\,d}\left(1-\frac{1}{p}\left(\frac{D}{p}\right)\right),$$

where the product runs over primes p dividing d and $w(D)|6$ is the number of roots of unity in the quadratic order of discriminant D.

Congruences implied by the Hurwitz class number formula

Evaluating the sum over $d \mid f$ (which is multiplicative), we see for instance that for $a = \ell^e$, $b = \ell^c u$, $\gcd(\ell, u) = 1$, $c' = \lfloor c/2 \rfloor$, $e > c$, we have congruences implied by the class number formula if and only if

$$2 \mid c \text{ and } -u \in (\mathbb{Z}/\ell\mathbb{Z})^{\times 2}, \quad \text{i.e. } -b \in (\mathbb{Z}/a\mathbb{Z})^2.$$

All observed congruences of $H(D)$ can be explained by the Hurwitz class numbers formula, and our observations can all be proved for such congruences.

Interestingly, all congruences for the partition and other modular forms I am aware of can be explained by Hecke operators.

Hurwitz Congruence Conjecture

Fix a prime $\ell \geq 5$. Given integers $a > 0$ and b with the property that

$$\forall n \in \mathbb{Z} : H(an - b) \equiv 0 \pmod{\ell}.$$

Then for every n, writing $an - b = Df^2$ with a fundamental discriminant D, we have

$$\sum_{d \mid f} d \prod_{p \mid d} \left(1 - \frac{1}{p}\left(\frac{D}{p}\right)\right) \equiv 0 \pmod{\ell}.$$

Hurwitz Congruence Conjecture

The conjecture does not seem accessible with current technology.

The most elusive congruences are the non-holomorphic ones: Tools to study congruences usually rely on the modular curve over $\mathbb{F}_\ell$ and Galois representations.

Results

Non-holomorphic Hurwitz congruences

Theorem (Beckwith, R., Richter): Fix a prime $\ell \geq 5$. Given integers $a > 0$ and b with the property that

$$\forall n \in \mathbb{Z} : H(an - b) \equiv 0 \pmod{\ell} \quad \text{and} \quad -b \in (\mathbb{Z}/a\mathbb{Z})^2.$$

Then we have $\ell \mid a$.

This not only heavily restricts non-holomorphic congruences, but more importantly enables the use of some tools used to study holomorphic modular forms.

Hurwitz congruences in square classes

Theorem (R.): Fix a prime $\ell \geq 5$. Given integers $a > 0$ and b with the property that

$$\forall n \in \mathbb{Z} : H(an - b) \equiv 0 \pmod{\ell}.$$

Then we have congruences

$$\forall n \in \mathbb{Z} : H(an - b') \equiv 0 \pmod{\ell}$$

for all $b' \in b(\mathbb{Z}/a\mathbb{Z})^{\times 2}$.

The case of "holomorphic" congruences follows from previous work in 2019, but the non-holomorphic case relies on the previous theorem.

Hurwitz congruences in square classes

Corollary: Fix a prime $\ell \geq 5$. Given integers $a > 0$ and b such that $a\mathbb{Z} + b$ is maximal with the property that

$$\forall n \in \mathbb{Z} : H(an - b) \equiv 0 \pmod{\ell}.$$

Then $a/\gcd(a, b)$ is square free away from 2.

Techniques

The generating function

When working with half-integral weight modular forms, we implicitly use the theta multiplier.

$$E_{\frac{3}{2}}(\tau) := \sum_D H(D)e(-D\tau) + \frac{1}{16\pi}\theta^*(\tau) \in \mathbb{M}_{\frac{3}{2}}(\Gamma_0(4)),$$

where θ^* is a non-holomorphic Eichler integral of

$$\theta := \theta_{1,0} \in \mathrm{M}_{\frac{1}{2}}(\Gamma_0(4)) \text{ with}$$

$$\theta_{a,b}(\tau) := \sum_{\substack{n\in\mathbb{Z} \\ n\equiv b \pmod a}} e\left(\tfrac{n^2\tau}{a}\right) \in \mathrm{M}_{\frac{1}{2}}(\Gamma(4a)), \quad a \in \mathbb{Z}_{\geq 1}, b \in \mathbb{Z}.$$

Congruences in terms of a modular form

To encode congruences on arithmetic progressions as a modular form we use

$$\mathrm{U}_{a,b} \sum_{n\in\mathbb{Z}} c(f;n;y)e(n\tau) := \sum_{\substack{n\in\mathbb{Z} \\ n\equiv b \pmod a}} c\big(f;\tfrac{n}{a};\tfrac{y}{a}\big)e\big(\tfrac{n\tau}{a}\big).$$

We have

$$\mathrm{U}_{a,b}\, E_{\frac{3}{2}} \in \mathrm{M}_{\frac{3}{2}}\big(\Gamma(4a)\big).$$

$$\mathrm{U}_{a,b}\,\theta = \sum_{\beta^2\equiv b \pmod a} \theta_{a,\beta} \quad \text{and} \quad \mathrm{U}_{a,b}\,\theta^* = \sum_{\beta^2\equiv -b \pmod a} \sqrt{a}\,\theta^*_{a,\beta}.$$

Producing a holomorphic modular form...

Since congruences cannot be extracted from real-analytic modular forms, we apply holomorphic projection:

$$\pi_2^{\mathrm{hol}}\big((\mathrm{U}_{a,b}\, E_{\frac{3}{2}}) \cdot (\theta_{a,\beta} + \theta_{a,-\beta})\big) =: \sum_{n=0}^{\infty} c(n) e(n\tau),$$

where β is a fixed square root of b modulo a.

The idea that products with theta series preserve sufficient information after holomorphic projection was applied to mock theta series in a paper by İmamoğlu, R., Richter.

...and analyzing its coefficients

If we have $H(an-b) \equiv 0$ for all n but $\ell \nmid a$, then

$$c(n_a pq) \equiv -2(1+q) \pmod{\ell} \quad \text{and}$$
$$c(n_a p^2 q) \equiv -2(1+p+q) \pmod{\ell}$$

for any primes $p, q \equiv 1 \pmod{\ell}$ such that

$$p^2 > (an_a)q > (an_a)^2 p > (an_a)^3.$$

Here n_a is a certain auxiliary integer, that is co-prime to both p and q.

A theorem by Serre

To deduce a contradiction we use a theorem by Serre.

There are infinitely many primes $p \equiv 1 \pmod{a\ell}$ such that

$$c(f; np^r) \equiv (r+1)c(f; n) \pmod{\ell}$$

for all $n \in \mathbb{Z}$ co-prime to p, $r \in \mathbb{Z}_{\geq 0}$, and $f \in \mathrm{M}_2(\Gamma_1(4a))$.

Can be extended to quasi-modular forms.

This theorem was previously used by Ono, Ahlgren-Ono, Treneer to produce congruences from Hecke eigenvalues.

And finally a contradiction

On one hand we have

$$c(n_a pq) \equiv -2(1+q) \pmod{\ell} \quad \text{and}$$
$$c(n_a p^2 q) \equiv -2(1+p+q) \pmod{\ell},$$

one the other hand,

$$c(f; np^r) \equiv (r+1)c(f; n) \pmod{\ell}.$$

Hence we have

$$1+q \equiv 0 \pmod{\ell} \quad \text{or} \quad 3(1+q) \equiv 2(1+q+p) \pmod{\ell},$$

contradicting $q \equiv 1 \pmod{\ell}$.

The action of $\mathrm{Mp}_1(\mathbb{Z})$ on congruences

Abstract spaces of modular forms

An abstract space of modular forms is a finite dimensional $\mathrm{Mp}_1(\mathbb{Z})$ right-representation on a space V together with a homomorphism ϕ into a space of modular forms $\mathrm{M}_k(\Gamma)$.

The point of this construction is to later avoid intricate calculations with multiplier systems, but use Kubota's theory of metaplectic covers. The merit is also that it extends to all algebraic groups.

Induction to full level

Given a modular form $f \in \mathrm{M}_k(\Gamma)$, replace it by

$$V := \mathbb{C}f \otimes_{\mathbb{C}[\Gamma]} \mathbb{C}\big[\mathrm{Mp}_1(\mathbb{Z})\big], \quad \phi : f \otimes \gamma \mapsto f\big|_k \gamma$$

to always work with $\mathrm{Mp}_1(\mathbb{Z})$.

This is an induced representation.

Vector-valued Hecke operators

We have a map

$$\mathrm{GMp}_1(R) \twoheadrightarrow \{(\gamma, s) \in \mathrm{Mat}_2(R) \times R : \gamma\gamma^{\#} = \left(\begin{smallmatrix} s & 0 \\ 0 & s \end{smallmatrix}\right)\},$$

and from this a $\mathrm{Mp}_1(\mathbb{Z})$-biset $\mathrm{GMp}_1^{(M)}$, the fiber of M under the projection to s.

The Hecke operator $\mathrm{T}_M(V, \phi)$ is defined by

$$\mathrm{T}_M V \otimes_{\mathbb{C}[\mathrm{Mp}_1(\mathbb{Z})]} \mathbb{C}[\mathrm{GMp}_1^{(M)}(\mathbb{Z})], \quad \mathrm{T}_M \phi : f \otimes \gamma \mapsto f\big|_k \gamma.$$

This can be shown to be isomorphic to a direct sum of restriction-inductions (as opposed to induction-restriction).

Ramanujan-type congruences and Hecke operators

The operator $\mathrm{U}_{a,b}$ selecting coefficients on $a\mathbb{Z}+b$ can be expressed by elements in $K[\mathrm{GMp}_1^{(a)}(\mathbb{Z})]$, where $K=\mathbb{C}$ (or later $K=\mathbb{Q}_\ell^{\mathrm{un}}$).

$$a^{\frac{k}{2}-1}\sum_{h\,(\mathrm{mod}\,a)} e(-hb/a)\left(\begin{smallmatrix}1 & h\\ 0 & a\end{smallmatrix}\right).$$

We can describe the structure of Ramanujan-type congruences through vector-valued Hecke operators. For many results, this and the ℓ-integral structure is all that is needed.

ℓ-kernels are subrepresentations

We obtain a map from the space of modular forms

$$\mathrm{FE} : \mathrm{M}_k(\Gamma) \longrightarrow \mathbb{C}[\![q^{1/\infty}]\!] = \varinjlim \mathbb{C}[\![q^{1/N}]\!], \quad f \longmapsto \sum_{n \in \mathbb{Q}} c(n) e(n\tau).$$

Hence an ℓ-kernel of abstract spaces of modular forms:

$$\ker_\ell(V, \phi) = \{v \in V : \mathrm{FE}(\phi(v)) \in \ell \mathbb{Z}_\ell^{\mathrm{un}}[\![q^{1/\infty}]\!]\}.$$

By Deligne-Rapoport (plus some extra work) this is a subrepresentation for some $\Gamma_0(\gcd(\ell^\infty, \mathrm{lvl}(V, \phi)))$.

Congruences on square classes

Congruences on arithmetic progressions deliver vectors in $\ker_\ell(V,\phi)$. We examine which subrepresentation they generate.

The fact that for congruences on arithmetic progressions $H(an-b)\equiv 0 \pmod{\ell}$ exist for whole square classes of b follows from examining the action of the usual Cartan in $\mathrm{Mp}_1(\mathbb{Z}/a\mathbb{Z})$ on

$$\pi_2^{\mathrm{hol}}\Big(\big(\mathrm{T}_a\,\mathbb{C}E_{\frac{3}{2}}\big)\otimes\mathbb{C}\{\theta_{a,\beta}:\beta \pmod{a}\}\Big).$$

Local components of automorphism representations

For newforms and assuming that $\gcd(\ell, a) = 1$, ℓ-kernels effectively cut out a representation for a maximal compact open K_ℓ from the local component ϖ_ℓ of an automorphism representation $\varpi \cong \bigotimes' \varpi_p$.