Metacommutation of Hurwitz primes

Abhinav Kumar
MIT

Joint work with Henry Cohn

January 10, 2013

Quaternions and Hurwitz integers

Recall the skew-field of real quaternions $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$, with $i^2 = j^2 = -1$ and $ij = -ji = k$.

The reduced trace of $x = a + bi + cj + dk$ is $\mathrm{tr}(x) = 2a$ and the reduced norm is $\mathrm{N}(x) = a^2 + b^2 + c^2 + d^2$. The conjugate of x is $x^\sigma = a - bi - cj - dk$.

The ring $\mathcal{H}$ of Hurwitz integers consists of those quaternions with a, b, c, d all in $\mathbb{Z}$ or all in $\mathbb{Z} + 1/2$. It is a maximal order of $\mathcal{H} \otimes \mathbb{Q}$.

Primes and the Euclidean algorithm

With the reduced norm form, $\mathcal{H}$ is isometric to the D_4 lattice. There are 24 units in $\mathcal{H}$.

A prime P of $\mathcal{H}$ is an element which is not a product of two non-units. It lies over some rational prime $p = \mathrm{N}(P)$.

Primes and the Euclidean algorithm

With the reduced norm form, $\mathcal{H}$ is isometric to the D_4 lattice. There are 24 units in $\mathcal{H}$.

A prime P of $\mathcal{H}$ is an element which is not a product of two non-units. It lies over some rational prime $p = \mathrm{N}(P)$.

The ring $\mathcal{H}$ is Euclidean: i.e. it has the "division with small remainder" property. Therefore, any (left) ideal is principal: it has the form $\mathcal{H}x$ for some $x \in \mathcal{H}$.

This fact rapidly leads to a version of unique factorization into primes.

Factorization I

We may factor any nonzero $x \in \mathcal{H}$ as

$$x = P_1 P_2 \dots P_n$$

where P_i are Hurwitz primes of norms say p_i. We say this is a factorization of x *modeled on* a factorization $N(x) = p_1 \dots p_n$. (i.e. fixing the order of $p_1, \dots, p_n$).

Factorization I

We may factor any nonzero $x \in \mathcal{H}$ as

$$x = P_1 P_2 \dots P_n$$

where P_i are Hurwitz primes of norms say p_i. We say this is a factorization of x *modeled on* a factorization $N(x) = p_1 \dots p_n$. (i.e. fixing the order of $p_1, \dots, p_n$).

Theorem (Conway,Smith (?))

If x is primitive (not divisible) by a natural number larger than 1, then there is a factorization of x modeled on any factorization of its norm. It is unique up to unit-migration, i.e. replacing

$$x = P_1 \dots P_n$$

by

$$x = (P_1 u_1)(u_1^{-1} P_2 u_2) \dots (u_{n-1}^{-1} P_n).$$

Factorization II

In particular, if P and Q are primes of distinct prime norms p and q, then $PQ = Q'P'$ for some Q' and P' of norms q and p respectively. This "operation" is called metacommutation.

Factorization II

In particular, if P and Q are primes of distinct prime norms p and q, then $PQ = Q'P'$ for some Q' and P' of norms q and p respectively. This "operation" is called metacommutation.

Theorem (Conway, Smith)

The prime factorization of a Hurwitz quaternion is unique up to (repeated applications of) unit-migration, metacommutation and recombination.

Recombination is the process of replacing PP^σ by $P'P'^\sigma$.

Metacommutation problem

From Conway and Smith, “On Quaternions and Octonions”:

```
However, this does not completely justify the term "unique
factorization" for Hurwitzians. To do so would require
solving a problem we call the metacommutation problem:
How does a prime factorization PQ modelled on pq determine
a corresponding factorization Q'P' modelled on qp?
This difficult problem does not seem to have been
addressed in the literature.
```

Permutation action

Note that if we start with P, Q and produce Q', P' satisfying $PQ = Q'P'$, the prime P' is unique up to left multiplication by units (since $Q'P'$ is unique up to unit-migration). Also, left multiplying P by a unit does not affect P'.

So we can consider the action of Q on the set of primes of norm p up to left multiplication. This is a permutation, since right multiplication by Q^σ provides an inverse.

Points on a conic

Proposition

For p odd (i.e. unramified in $\mathcal{H}_{\mathbb{Q}}$), there are exactly $p+1$ primes of norm p, up to left multiplication by units.

Points on a conic

Proposition

For p odd (i.e. unramified in $\mathcal{H}_{\mathbb{Q}}$), there are exactly $p+1$ primes of norm p, up to left multiplication by units.

Proof.

Let $\overline{\mathcal{H}}$ be the reduction of $\mathcal{H}$ mod p. The reduction Π of $\mathcal{H}P$ is a 2-dimensional vector space over $\mathbb{F}_p$. There is a unique element $t_P = (x, y, z)$ of trace zero in Π. It gives a point on the conic $x^2 + y^2 + z^2 = 0$ in $\mathbb{P}^2(\mathbb{F}_p)$. One proves that this association is bijective, and there are $p+1$ points on the smooth conic. $\square$

(More abstractly, conic is a Severi-Brauer variety)

Points on a conic

Proposition

For p odd (i.e. unramified in $\mathcal{H}_{\mathbb{Q}}$), there are exactly $p+1$ primes of norm p, up to left multiplication by units.

Proof.

Let $\overline{\mathcal{H}}$ be the reduction of $\mathcal{H}$ mod p. The reduction Π of $\mathcal{H}P$ is a 2-dimensional vector space over $\mathbb{F}_p$. There is a unique element $t_P = (x, y, z)$ of trace zero in Π. It gives a point on the conic $x^2 + y^2 + z^2 = 0$ in $\mathbb{P}^2(\mathbb{F}_p)$. One proves that this association is bijective, and there are $p+1$ points on the smooth conic. $\square$

(More abstractly, conic is a Severi-Brauer variety)

We can analyze the cycle structure of the metacommutation permutation by Q on the $p+1$ primes of norm P, for all primes Q of norm q.

Data on cycle structure

Example

$p = 13$, $q = 11$.

```
gp > allcyclestructs(11,13)
% 2 = [[[2, 2, 2, 2, 2, 2, 2], 24], [[1, 1, 12], 96], [[14], 72],
[[1, 1, 4, 4, 4], 96]]
```

Data on cycle structure

Example

$p = 13$, $q = 11$.

```
gp > allcyclestructs(11,13)
% 2 = [[[2, 2, 2, 2, 2, 2, 2], 24], [[1, 1, 12], 96], [[14], 72],
[[1, 1, 4, 4, 4], 96]]
```

So there are

- 24 primes Q for which the permutation consists of seven transpositions
- 96 primes Q for which the permutation has two fixed points and a cycle of length 12
- 72 primes Q for which the permutation is a cycle of length 14
- and 96 primes Q for which the permutation has two fixed points and three cycles of length 4.

Total number of primes Q is $288 = 24(11 + 1)$.

Observations and Questions

- When are there fixed points? How many?
- The rest of the permutation seems to break up into cycles of equal length.
- What is the sign of the permutation?
- How do these depend on the particular prime Q chosen?

Theorem (Cohn-K)

Let p and q be distinct rational primes, let Q be a Hurwitz prime of norm q, and consider the Hurwitz primes of norm p modulo left multiplication by units.

Main results

Theorem (Cohn-K)

Let p and q be distinct rational primes, let Q be a Hurwitz prime of norm q, and consider the Hurwitz primes of norm p modulo left multiplication by units.

1. *Metacommutation by Q permutes these primes, and the sign of the permutation is the quadratic character $\left(\frac{q}{p}\right)$ of q modulo p.*

Main results

Theorem (Cohn-K)

Let p and q be distinct rational primes, let Q be a Hurwitz prime of norm q, and consider the Hurwitz primes of norm p modulo left multiplication by units.

1. *Metacommutation by Q permutes these primes, and the sign of the permutation is the quadratic character $\left(\frac{q}{p}\right)$ of q modulo p.*
2. *If $p = 2$, or if Q is congruent to a rational integer modulo p, then metacommutation by Q is the identity permutation.*
   Otherwise it has $1 + \left(\frac{\mathrm{tr}(Q)^2 - q}{p}\right)$ fixed points.

Main results

Theorem (Cohn-K)

Let p and q be distinct rational primes, let Q be a Hurwitz prime of norm q, and consider the Hurwitz primes of norm p modulo left multiplication by units.

1. *Metacommutation by Q permutes these primes, and the sign of the permutation is the quadratic character $\left(\frac{q}{p}\right)$ of q modulo p.*
2. *If $p = 2$, or if Q is congruent to a rational integer modulo p, then metacommutation by Q is the identity permutation.*
   Otherwise it has $1 + \left(\frac{\mathrm{tr}(Q)^2 - q}{p}\right)$ fixed points.
3. *The rest of the permutation consists of cycles of length equal to the multiplicative order of the roots of the polynomial $(x+1)^2 - (4a^2/q)x$.*

Idea of proof I

$p = 2$ is easy to analyze, so we may assume p odd.

Write the reduction of Q mod p as $\overline{Q} = a + bi + cj + dk$.

We prove the **key lemma**: metacommutation by Q acts as conjugation on the points of the conic associated to p. That is, $t_P = \overline{Q}^{-1} t_p \overline{Q}$ up to scaling.

Idea of proof I

$p = 2$ is easy to analyze, so we may assume p odd.

Write the reduction of Q mod p as $\overline{Q} = a + bi + cj + dk$.

We prove the **key lemma**: metacommutation by Q acts as conjugation on the points of the conic associated to p. That is, $t_P = \overline{Q}^{-1} t_p \overline{Q}$ up to scaling.

Therefore, we may represent the metacommutation operation by an element ϕ of $SO_3(\mathbb{F}_p)$.

Idea of proof I

$p = 2$ is easy to analyze, so we may assume p odd.

Write the reduction of Q mod p as $\overline{Q} = a + bi + cj + dk$.

We prove the **key lemma**: metacommutation by Q acts as conjugation on the points of the conic associated to p. That is, $t_P = \overline{Q}^{-1} t_p \overline{Q}$ up to scaling.

Therefore, we may represent the metacommutation operation by an element ϕ of $SO_3(\mathbb{F}_p)$.

Its characteristic polynomial is

$$(x-1)\left(x^2 + 2\left(1 - \frac{a^2}{q}\right)x + 1\right)$$

Idea of proof II

We are interested in points $v = (x, y, z)$ with $x^2 + y^2 + z^2 = 0$ up to scaling: these correspond to the primes above p.

Idea of proof II

We are interested in points $v = (x, y, z)$ with $x^2 + y^2 + z^2 = 0$ up to scaling: these correspond to the primes above p.

Let $v_0 = (b, c, d)$; it is fixed under conjugation by $\overline{Q}$.

Idea of proof II

We are interested in points $v = (x, y, z)$ with $x^2 + y^2 + z^2 = 0$ up to scaling: these correspond to the primes above p.

Let $v_0 = (b, c, d)$; it is fixed under conjugation by $\overline{Q}$.

If $v_0 = (0, 0, 0)$ then the permutation is obviously the identity.

Idea of proof II

We are interested in points $v = (x, y, z)$ with $x^2 + y^2 + z^2 = 0$ up to scaling: these correspond to the primes above p.

Let $v_0 = (b, c, d)$; it is fixed under conjugation by $\overline{Q}$.

If $v_0 = (0, 0, 0)$ then the permutation is obviously the identity.

Otherwise the number of fixed points is the number of eigenvectors v (up to scaling) with $\langle v, v\rangle = 0$ and $\langle v, v_0\rangle = 0$.

Analyzing the char poly shows that we get 0 or 2 points, depending on the quadratic character of $a^2 - q$.

Idea of proof III

Now if $\langle v_0, v_0 \rangle \neq 0$, then we project any v **not orthogonal** to v_0 orthogonally to the vector v_0 and thereby transfer the metacommutation action to $SO(2\text{-dim quad form})$, which is cyclic and easy to analyze. (Consider action of $SO(q_2)$ on a conic, which is simply transitive).

This is the "generic" case.

Idea of proof III

Now if $\langle v_0, v_0 \rangle \neq 0$, then we project any v **not orthogonal** to v_0 orthogonally to the vector v_0 and thereby transfer the metacommutation action to $SO(2\text{-dim quad form})$, which is cyclic and easy to analyze. (Consider action of $SO(q_2)$ on a conic, which is simply transitive).

This is the "generic" case.

The last case is when $\langle v_0, v_0 \rangle = 0$ but $v_0 \neq 0$. Then the matrix corresponding to Q is unipotent, and the rest of the permutation is a p-cycle.

Reference: "Metacommutation of Hurwitz primes",
Henry Cohn and Abhinav Kumar,
available at `http://web.mit.edu/abhinavk/www/papers.html`

Thank you!