PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 144, Number 11, November 2016, Pages 4583–4590
http://dx.doi.org/10.1090/proc/13126
Article electronically published on July 21, 2016

METACOMMUTATION AS A GROUP ACTION ON THE PROJECTIVE LINE OVER $\mathbb{F}_p$

ADAM FORSYTH, JACOB GUREV, AND SHAKTHI SHRIMA

(Communicated by Ken Ono)

Abstract. Cohn and Kumar showed the quadratic character of q modulo p gives the sign of the permutation of Hurwitz primes of norm p induced by the Hurwitz primes of norm q under metacommutation. We demonstrate that these permutations are equivalent to those induced by the right standard action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on $\mathbb{P}^1(\mathbb{F}_p)$. This equivalence provides simpler proofs of the results of Cohn and Kumar and characterizes the cycle structure of the aforementioned permutations. Our methods are general enough to extend to all orders over the quaternions with a division algorithm for primes of a given norm p.

1. Introduction

Consider the Hamilton quaternions $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$, where i, j, and k are uniquely defined by the relation

$$i^2 = j^2 = k^2 = ijk = -1.$$

In this paper, we study the subring of Hurwitz quaternions:

$$\mathcal{H} = \mathbb{Z}\left[i, j, \frac{1}{2}(1 + i + j + k)\right].$$

(In other words, this is the subring of quaternions whose components are either all elements of $\mathbb{Z}$ or all elements of $\mathbb{Z} + 1/2$.)

We begin by reviewing some fundamental definitions and results. For any quaternion

$$h = a + bi + cj + dk,$$

we call

$$\begin{aligned} h^\sigma &= a - bi - cj - dk, \\ N(h) &= a^2 + b^2 + c^2 + d^2, \\ \mathrm{tr}(h) &= h + h^\sigma = 2a \end{aligned}$$

its *conjugate*, *norm*, and *trace*, respectively. The reader can easily verify that the norm is multiplicative.

Because the ring of Hurwitz quaternions has left and right division algorithms, all of its ideals are principal. We call a Hurwitz integer P *prime* if it is irreducible. A Hurwitz integer is prime in $\mathcal{H}$ if and only if its norm is prime in $\mathbb{Z}$ (see [3] for details). In [3], Conway and Smith prove any factorization of a non-zero Hurwitz

Received by the editors March 18, 2015 and, in revised form, December 24, 2015.
2010 *Mathematics Subject Classification.* Primary 11R52; Secondary 11R27.

integer into Hurwitz primes is unique up to three phenomena, which we define below. ([1] provides another exposition of this theorem.)

The Euclidean algorithm in $\mathcal{H}$ lets us factor any non-zero $h \in \mathcal{H}$ with norm $N(h) = p_1 p_2 \cdots p_n$, where the p_i are prime, into a product of Hurwitz primes:

$$h = P_1 P_2 \cdots P_n, \quad \text{where } N(P_i) = p_i.$$

As in [2], we say this factorization of h is *modeled* on the factorization of $N(h) = p_1 p_2 \cdots p_n$. When $N(h)$ is square-free, we call such a factorization unique up to *unit migration*, because if the p_i are distinct, then every factorization of h modeled on

$$N(h) = \prod_{i=1}^{n} p_i$$

is of the form

$$h = (P_1 u_1)(u_1^{-1} P_2 u_2) \cdots (u_{n-1}^{-1} P_n),$$

where the u_i are units in $\mathcal{H}$. If a factorization of h contains both a prime P and P^σ in sequence, we can replace PP^σ by $P_1 P_1^\sigma$ where $N(P) = N(P_1)$. We call such a factorization unique up to *recombination*. As in [2], we say a left ideal $\mathcal{H}P$ for prime $P \in \mathcal{H}$ *lies over* a rational prime p if $N(P) = p$.

The next proposition, which [1] proves, establishes the main phenomenon we study in this paper.

Proposition 1.1 (Conway and Smith)**.** *If P and Q are distinct primes in $\mathcal{H}$ that lie over rational primes p and q respectively, then PQ has a factorization $Q'P'$ modeled on qp that is unique up to unit migration.*

We call the process of "swapping" adjacent primes *metacommutation*. Given $Q \in \mathcal{H}$ with norm coprime to p, every P with norm p has an associated prime P' also of norm p, which satisfies

$$PQ = Q'P' \quad \text{for some } Q' \in \mathcal{H}.$$

The *metacommutation map* on primes of norm p sends every P to the corresponding P'. For each Q, this map induces a permutation of the Hurwitz primes of norm p. In [2], Cohn and Kumar prove that the sign of this permutation is $\left(\frac{q}{p}\right)$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol, and that this permutation has

$$1 + \left(\frac{\operatorname{tr}(Q)^2 - 4q}{p}\right)$$

fixed points. Although the current literature gives several properties of the permutation the metacommutation map induces, it does not directly describe this permutation.

In Sections 2 and 3 of this paper, we establish isomorphisms and bijections which simplify studying the metacommutation phenomenon; in Section 4, we show the metacommutation mapping is isomorphic to the right standard action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on the projective line over $\mathbb{F}_p$; in Section 5, we provide new, shorter proofs of the results of Cohn and Kumar, and characterize much of the cycle structure of the permutations.

2. Definitions and preliminaries

Let $\mathcal{H}/\mathcal{H}p = \overline{\mathcal{H}}$, where p is a fixed rational prime, and let $\overline{P}$ denote the reduction of any $P \in \mathcal{H}$ modulo p. Given a Hurwitz prime P of norm p, we can then define the left ideal $\overline{\mathcal{H}P} = \left\{h\overline{P} \mid h \in \overline{\mathcal{H}}\right\}$, which is the modulo p reduction of the ideal $\mathcal{H}P$. Note that two primes P and P' with norm p induce the same ideal in $\overline{\mathcal{H}}$ when they are left associates; this motivates us to consider uniqueness of the primes with norm p only up to left multiplication by units.

All such ideals have dimension two. Indeed, since conjugation is an automorphism of $\mathcal{H}$, $\overline{\mathcal{H}P}$ has the same dimension as $\overline{\mathcal{H}P^\sigma}$. Because the elements $h \in \overline{\mathcal{H}P^\sigma}$ are exactly those where hP equals 0 inside of $\overline{\mathcal{H}}$,

$$\dim(\overline{\mathcal{H}P}) + \dim(\overline{\mathcal{H}P^\sigma}) = \dim(\overline{\mathcal{H}}) = 4,$$

and $\dim(\overline{\mathcal{H}P}) = 2$ as desired.

[1] gives a one-to-one correspondence between primes in $\mathcal{H}$ and the two-dimen-,sional left ideals of $\overline{\mathcal{H}}$. This lets us count the number of Hurwitz primes of norm p through a bijective correspondence with points on the conic

$$C_p = \left\{(x, y, z) \in \mathbb{P}^2(\mathbb{F}_p) \mid x^2 + y^2 + z^2 = 0\right\}.$$

The following proposition establishes this correspondence. (The proof we give follows the argument in [2].)

Proposition 2.1. *There is a bijective correspondence between points on the conic C_p and Hurwitz primes P of norm p.*

Proof. The trace function on the ideal $\overline{\mathcal{H}P}$ is linear. Being a linear function from a two-dimensional vector space over $\mathbb{F}_p$ to a one-dimensional vector space, it therefore has a non-trivial kernel. It is easy to see that not every element of $\overline{\mathcal{H}P}$ can have trace 0. Indeed, if $q = a+bi+cj+dk$ is any non-zero element of $\overline{\mathcal{H}P}$, then one of a, b, c, and d is non-zero, and so one of q, iq, jq, and kq, which are all also in $\overline{\mathcal{H}P}$, will have non-zero trace. The kernel thus has dimension exactly one. It follows that up to scaling, there is a unique non-zero element

$$t_P = ai + bj + ck \in \overline{\mathcal{H}P}$$

with trace 0. But, all elements of $\overline{\mathcal{H}P}$ have norm 0, so $N(t_P) = 0$, implying

$$a^2 + b^2 + c^2 = 0.$$

Therefore, there is a corresponding point $c_P = (a, b, c) \in C_p$.

Because $t_P \neq 0$, $\dim(\overline{\mathcal{H}}t_P) = 2$ by the same argument as above, $\overline{\mathcal{H}}t_P = \overline{\mathcal{H}P}$. Therefore, t_P is a left associate of P, and the map $P \mapsto c_P$ is a bijection. □

This bijection lets us reduce the study of metacommutation to an action on C_p.

The following proposition describes the conjugation action on the conic.

Proposition 2.2. *For a prime $P \in \mathcal{H}$ with norm p, let Q be a Hurwitz integer with norm coprime to p. If $PQ = Q'P'$, then $\overline{Q^{-1}}t_P\overline{Q} = t_{P'}$.*

Proof. Because Q and Q' are invertible in $\overline{\mathcal{H}}$,

$$\overline{Q^{-1}\mathcal{H}PQ} = \overline{\mathcal{H}PQ} = \overline{\mathcal{H}Q'P'} = \overline{\mathcal{H}P'}.$$

As $t_P \in \overline{\mathcal{H}P}$, we can deduce that

$$\overline{Q^{-1}} t_P \overline{Q} \in \overline{\mathcal{H}P'}.$$

$\overline{Q^{-1}} t_P \overline{Q}$ is non-zero and has trace 0, so $\overline{Q^{-1}} t_P \overline{Q} = t_{P'}$. □

Proposition 2.2 gives a simpler way of thinking about the metacommutation action: as a group action by conjugation of the quaternions with non-zero norm in $\overline{\mathcal{H}}$ on the points on our projective conic.

3. An isomorphism

While the characterization of the metacommutation mapping as a group action on C_p, as [2] gives, is simple, $\overline{\mathcal{H}}$ is still not as intuitive as we want. So in the spirit of simplifying our study of metacommutation, we recall the following proposition.

Proposition 3.1. *$\overline{\mathcal{H}}$ is isomorphic to $\mathcal{M}_2(\mathbb{F}_p)$.*

Proof. The isomorphism follows from the fact that $\overline{\mathcal{H}}$ is a split four-dimensional algebra over $\mathbb{F}_p$; for the sake of clarity we will construct an explicit isomorphism $\varphi : \overline{\mathcal{H}} \to \mathcal{M}_2(\mathbb{F}_p)$. If $\gamma \in \overline{\mathcal{H}}$ and

$$\gamma = \gamma_1 + \gamma_2 i + \gamma_3 j + \gamma_4 k,$$

then

$$\varphi(\gamma) = \begin{pmatrix} \gamma_1 + \gamma_2 a + \gamma_4 b & \gamma_3 + \gamma_4 a - \gamma_2 b \\ -\gamma_3 + \gamma_4 a - \gamma_2 b & \gamma_1 - \gamma_2 a - \gamma_4 b \end{pmatrix},$$

where $a^2 + b^2 \equiv -1 \bmod p$. (A pigeonhole argument proves such a and b always exist; see [4].) Note that under φ, we have

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; i \mapsto \begin{pmatrix} a & -b \\ -b & -a \end{pmatrix},$$

$$j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; k \mapsto \begin{pmatrix} b & a \\ a & -b \end{pmatrix}.$$

Explicit calculation then shows

$$\varphi(\gamma\delta) = \varphi(\gamma)\varphi(\delta) \quad \text{and} \quad \varphi(\gamma + \delta) = \varphi(\gamma) + \varphi(\delta).$$

(Also, note that

$$\varphi(i)^2 = \varphi(j)^2 = \varphi(k)^2 = \varphi(i)\varphi(j)\varphi(k) = \varphi(-1),$$

as desired.) Thus, φ is a ring homomorphism, and, since it is bijective, an isomorphism. □

Corollary 3.1. *$N(\gamma) = \det(\varphi(\gamma))$ and $\operatorname{tr}(\gamma) = \operatorname{tr}(\varphi(\gamma))$, where $\operatorname{tr}(\varphi(\gamma))$ is the standard matrix trace.*

4. An action on the projective line over $\mathbb{F}_p$

Now we characterize the metacommutation action as a group action.

Theorem 4.1. *The metacommutation action on C_p is isomorphic to the right standard action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on $\mathbb{P}^1(\mathbb{F}_p)$, which we use in the form*

$$\langle x, y\rangle * \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \langle a_1 x + a_3 y, a_2 x + a_4 y\rangle.$$

Proof. Let $\mathcal{U}$ denote the elements of $\overline{\mathcal{H}}$ with non-zero norm. Under the isomorphism φ, $\mathcal{U} \mapsto \mathrm{GL}_2(\mathbb{F}_p)$, when we projectivize $\mathrm{GL}_2(\mathbb{F}_p)$ to obtain $\mathrm{PGL}_2(\mathbb{F}_p)$, we have an isomorphism

$$\Theta : \mathcal{U}/\mathbb{F}_p^* \to \mathrm{PGL}_2(\mathbb{F}_p),$$

since $\mathrm{PGL}_2(\mathbb{F}_p)$ is the quotient of $\mathrm{GL}_2(\mathbb{F}_p)$ by the scalar matrices $\mathrm{Z}(\mathbb{F}_p)$.

Recall that elements of the conic C_p are, by definition, those elements with norm and trace equal to zero. Hence, C_p maps to D under φ, where D denotes the elements in $\mathcal{M}_2(\mathbb{F}_p)$ modulo scalars of the form

$$\begin{pmatrix} -a_1 & a_2 \\ a_3 & a_1 \end{pmatrix}, \quad \text{where } a_1^2 = -a_2 a_3.$$

We can characterize the $p+1$ elements of D as follows. If $a_3 = 0$, then $a_1 = 0$, and therefore only one element of C_p maps to such a matrix: $\left(\begin{smallmatrix} 0 & a_2 \\ 0 & 0 \end{smallmatrix}\right)$, which is equivalent to $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$.

Otherwise, by scaling, we can assume $a_3 = 1$; under Θ, the p remaining points of C_p then map to the elements of D of the form

$$\begin{pmatrix} -a_1 & -a_1^2 \\ 1 & a_1 \end{pmatrix}.$$

Associate each matrix $M \in D$ to the left kernel $v(M)$ of its action on the projective line; $M = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ has $v(M) = \langle 0, 1\rangle$, and $M = \left(\begin{smallmatrix} -a_1 & -a_1^2 \\ 1 & a_1 \end{smallmatrix}\right)$ has $v(M) = \langle 1, a_1\rangle$. Then for any $A \in \mathrm{PGL}_2(\mathbb{F}_p)$ and $c \in \mathbb{P}^1(\mathbb{F}_p)$, $c = v(M)$ implies $cM = 0$. It follows that $(cA)(A^{-1}MA) = 0$, and hence $v(A^{-1}MA) = v(M)A$.

We have proven the metacommutation action on C_p is isomorphic to the action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on D by conjugation, and that the action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on D by conjugation is isomorphic to the right standard action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on $\mathbb{P}^1(\mathbb{F}_p)$. Therefore the metacommutation action on C_p is isomorphic to the right standard action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on $\mathbb{P}^1(\mathbb{F}_p)$. □

5. Main results

We now present new, shorter proofs of some previously known results about the metacommutation map, as well as new information our isomorphism provides. In the following calculations, p is an odd prime, and $Q \in \mathcal{H}$ has prime norm $q \neq p$.

Theorem 5.1 (Cohn and Kumar, 2013)**.** *The sign of the metacommutation map of a Hurwitz prime of norm q on the Hurwitz primes of norm p is $\left(\frac{q}{p}\right)$.*

Proof. Recall three facts:

(1) The determinant of a matrix equals the norm of its associated quaternion.
(2) Due to the equivalence of group actions, the sign of a metacommutation map is the sign of the induced permutation of $\mathbb{P}^1(\mathbb{F}_p)$.

(3) The sign of an element A of $\mathrm{GL}_2(\mathbb{F}_p)$ is defined as the quadratic character of its determinant modulo p; that is, the Legendre symbol

$$\left(\frac{\det(A)}{p}\right).$$

Sign does not vary with multiplication by a scalar matrix, because the determinant of a scalar 2 by 2 matrix is a square, and the determinant is multiplicative; thus, the sign of a matrix in $\mathrm{PGL}_2(\mathbb{F}_p)$ is well defined. The sign of the permutation induced by an element of $\mathrm{PGL}_2(\mathbb{F}_p)$ on $\mathbb{P}^1(\mathbb{F}_p)$ is equal to the sign of the matrix of the element, as the kernels of both of these maps are normal subgroups of $\mathrm{PGL}_2(\mathbb{F}_p)$ of index 2, and so their intersection is a normal subgroup of $\mathrm{PSL}_2(\mathbb{F}_p)$ of index 1 or 2. But $\mathrm{PSL}_2(\mathbb{F}_p)$ is simple for $p > 3$, and when $p = 3$ is isomorphic to A_4, which has no subgroups of order 6. Thus the two kernels coincide, and so the sign of the metacommutation action of Q is the sign of $\Theta(Q)$, which is

$$\left(\frac{\det(\Theta(Q))}{p}\right) = \left(\frac{\det(\varphi(Q))}{p}\right) = \left(\frac{q}{p}\right).$$

□

Theorem 5.2 (Cohn and Kumar, 2013)**.** *The number of fixed points of the metacommutation map on p is*

$$1 + \left(\frac{\mathrm{tr}(Q)^2 - 4q}{p}\right),$$

unless $\overline{Q} \in \mathbb{F}_p$, in which case every point is a fixed point.

Proof. Let

$$M_Q = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$$

be the element of $\mathrm{PGL}_2(\mathbb{F}_p)$ associated to $\overline{Q}$. The characteristic polynomial of M_Q is

$$(a_1 - x)(a_4 - x) - a_2 a_3 = x^2 - \mathrm{tr}(Q)x + q.$$

The number of distinct roots in $\mathbb{F}_p$ of this polynomial is

$$1 + \left(\frac{\mathrm{tr}(Q)^2 - 4q}{p}\right).$$

This number of eigenvalues is the same as the number of fixed points of the projectivized map, with the exception of when there is an eigenvalue with geometric multiplicity of 2, in which case all points will be fixed points. This occurs when M_Q is diagonal and so $\overline{Q}$ is in $\mathbb{F}_p$. □

We can also study the cycle structure of the metacommutation maps using $\mathrm{PGL}_2(\mathbb{F}_p)$, thanks to Theorem 4.1.

Theorem 5.3. *All of the cycles which are not fixed points in a metacommutation map have the same length.*

Proof. We proceed by contradiction. Suppose a permutation $M_Q \in \mathrm{PGL}_2(\mathbb{F}_p)$ of the points of $\mathbb{P}^1(\mathbb{F}_p)$ had cycles with lengths m and n where $m > n > 1$. Then $(M_Q)^n$ would have at least n fixed points, but would not be the identity permutation. Thus $n = 2$, because (by Theorem 5.2) permutations with more than two fixed points fix all $p+1$ points of $\mathbb{P}^1(\mathbb{F}_p)$. We now show that if such an M_Q contains

a cycle of length 2, then M_Q itself must have order 2, and all cycles of M_Q have length 1 or 2.

Suppose for some transformation

$$M_Q = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_p)$$

that $\langle x, y\rangle \in \mathbb{P}^1(\mathbb{F}_p)$ has order 2, so that

$$\langle x, y\rangle \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}^2 = \langle x, y\rangle.$$

Then,

$$\begin{aligned} \langle x, y\rangle \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}^2 &= \langle a_1x + a_3y, a_2x + a_4y\rangle \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \\ &= \big\langle (a_1^2 + a_2a_3)x + (a_1a_3 + a_3a_4)y, \\ &\qquad (a_2a_1 + a_2a_4)x + (a_4^2 + a_2a_3)y\big\rangle. \end{aligned} \tag{5.1}$$

Hence, for some non-zero $\lambda \in \mathbb{F}_p$,

$$\begin{aligned} \lambda x &= (a_1^2 + a_2a_3)x + a_3(a_1 + a_4)y, \\ \lambda y &= a_2(a_1 + a_4)x + (a_4^2 + a_2a_3)y. \end{aligned}$$

Suppose $a_1 + a_4 = 0$. Then, $\lambda x = (a_1^2 + a_2a_3)x$ and

$$\lambda y = (a_4^2 + a_2a_3)y = (a_1^2 + a_2a_3)y.$$

Note that x and y cannot both be zero, so $a_1^2 + a_2a_3 = \lambda$. Hence, all points of $\mathbb{P}^1(\mathbb{F}_p)$ are fixed points under M_Q^2 and all cycles will have length 1 or 2. Otherwise,

$$(a_1^2 + a_2a_3)xy + a_3(a_1 + a_4)y^2 = (a_4^2 + a_2a_3)xy + a_2(a_1 + a_4)x^2. \tag{5.2}$$

Dividing (5.2) by $a_1 + a_4$ yields

$$(a_1 - a_4)(xy) = a_2x^2 - a_3y^2.$$

This implies

$$x(a_2x + a_4y) = y(a_1x + a_3y),$$

and thus

$$\langle x, y\rangle \sim \langle a_1x + a_3y, a_2x + a_4y\rangle, \tag{5.3}$$

so

$$\langle x, y\rangle \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \langle x, y\rangle,$$

which means $\langle x, y\rangle$ has order 1, a contradiction. Hence, all cycles have orders 1 and 2. This proves all the cycles of an element of $\mathrm{PGL}_2(\mathbb{F}_p)$ have the same length. □

Theorem 5.3 immediately implies the cycle length divides $p + 1$, p, or $p - 1$ depending on whether the permutation has respectively 0, 1, or 2 fixed points. In fact, the number of permutations (and thus the number of distinct metacommutation maps) with order $k > 1$ is well known to equal

$$\begin{cases} \varphi(k)p(p-1)/2 & \text{if } k \mid (p+1), \\ \varphi(k)p(p+1)/2 & \text{if } k \mid (p-1), \\ p^2 - 1 & \text{if } k = p. \end{cases}$$

6. A generalization

The results in Section 5 are stated in terms of the ring of Hurwitz quaternions. However, the only specific properties needed of an order $\mathcal{O}$ over the quaternions for these results to extend are a division algorithm for primes of norm p and an isomorphism of $\mathcal{O}/p\mathcal{O}$ with $M_2(\mathbb{F}_p)$. This latter property is equivalent to $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{F}_p$ being trivial. In particular, the Lipschitz quaternions

$$\mathcal{L} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\},$$

do not generally have a division algorithm, which is why results about metacommutation were first stated in terms of the Hurwitz integers. But in the Lipschitz integers, we can divide Q by P as long the norm of P is an odd rational prime, and so our results on metacommutation still hold.

Acknowledgements

The authors thank Henry Cohn for suggesting this area of research and for providing thoughtful comments; likewise, we thank Raffael Singer for his invaluable guidance during the period when this research was conducted. We also thank the Clay Mathematics Institute for funding the CMI/PROMYS research labs, as well as Erick Knight, Glenn Stevens, and the PROMYS program for making this research possible. Lastly we would like to thank Tara Smith and Daniel Allcock for helpful comments, and Edward Sanger for his support.

References

[1] Boyd Coan and Cherng-tiao Perng, *Factorization of Hurwitz quaternions*, Int. Math. Forum **7** (2012), no. 41-44, 2143–2156. MR2967414

[2] H. Cohn and A. Kumar, *Metacommutation of Hurwitz primes*, Proceedings of the American Mathematical Society (2013), to appear, available at `arxiv.org/abs/1307.0443`.

[3] John H. Conway and Derek A. Smith, *On quaternions and octonions: their geometry, arithmetic, and symmetry*, A K Peters, Ltd., Natick, MA, 2003. MR1957212

[4] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716

[5] E. F. Robertson and P. D. Williams, *A presentation of* $\mathrm{PGL}(2, p)$ *with three defining relations*, Proc. Edinburgh Math. Soc. (2) **27** (1984), no. 2, 145–149. MR760609

Department of Mathematics, Stanford University, Stanford, California 94305
E-mail address: `adamforsyth@stanford.edu`

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139
E-mail address: `gurev@mit.edu`

Department of Mathematics, Princeton University, Princeton, New Jersey 08540
E-mail address: `sshrima@princeton.edu`