LMS J. Comput. Math. 17 (Special issue A) (2014) 418–432 © 2014 Authors
doi:10.1112/S1461157014000151

On the quaternion ℓ-isogeny path problem

David Kohel, Kristin Lauter, Christophe Petit and Jean-Pierre Tignol

Abstract

Let $\mathcal{O}$ be a maximal order in a definite quaternion algebra over $\mathbb{Q}$ of prime discriminant p, and ℓ a small prime. We describe a probabilistic algorithm which, for a given left $\mathcal{O}$-ideal, computes a representative in its left ideal class of ℓ-power norm. In practice the algorithm is efficient and, subject to heuristics on expected distributions of primes, runs in expected polynomial time. This solves the underlying problem for a quaternion analog of the Charles–Goren–Lauter hash function, and has security implications for the original CGL construction in terms of supersingular elliptic curves.

1. *Introduction*

In this paper we provide a probabilistic algorithm to solve a quaternion ideal analog of the path problem in supersingular ℓ-isogeny graphs. The main result is an algorithm for the following. Let $B_{p,\infty}$ be a quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. Let ℓ be a 'small' prime, typically 2 or 3, or any small constant prime. Given a maximal quaternion order $\mathcal{O}$ in $B_{p,\infty}$ and a left $\mathcal{O}$-ideal I, compute an equivalent left $\mathcal{O}$-ideal $J = I\beta$ with norm ℓ^k for some k. This algorithm runs in practice in probabilistic polynomial time, and this effective runtime follows from heuristic assumptions on expected distributions of primes. With minimal adaptation, the algorithm can also be applied to output an ideal with smooth (or power-smooth) norm. The algorithm is described in terms of a special maximal order, but extends to any maximal order by passing through such a special order.

The motivation for this problem is an explicit equivalence of categories between left $\mathcal{O}$-ideals and supersingular elliptic curves (over $\bar{\mathbb{F}}_p$). The Deuring correspondence gives a bijection between such curves, up to Galois conjugacy, and isomorphism classes of maximal orders in $B_{p,\infty}$. This bijection can be turned into an equivalence of categories by the following construction. Let E_0/K be a fixed elliptic curve with endomorphism ring $\mathcal{O} = \mathrm{End}(E_0)$ a quaternion order in $B_{p,\infty} = \mathcal{O} \otimes \mathbb{Q}$ (we may take the base field $K = \mathbb{F}_{p^2}$ and E_0 such that $|E_0(K)| = (p+1)^2$). Associated to any pair (E_1, φ) where $\varphi : E_0 \to E_1$ is an isogeny, we obtain a left $\mathcal{O}$-ideal $I = \mathrm{Hom}(E_1, E_0)\varphi$ of norm $n = \deg(\varphi)$, and conversely every left $\mathcal{O}$-ideal arises in this way (see Kohel [8, § 5.3]). In particular, given any isogeny $\psi : E_0 \to E_1$ of degree m, the left $\mathcal{O}$-ideal $J = I\hat{\varphi}\psi/n$ is an equivalent ideal of norm m, where $\hat{\psi}$ is the dual of ψ.

The problem we address in this work is to solve the quaternion version of the supersingular ℓ-isogeny path problem: given E_0, E_1 and a small prime ℓ, find an ℓ-power isogeny from E_0 to E_1. Under this equivalence of categories, the analogous problem is the determination of an ℓ-power norm left $\mathcal{O}$-ideal in the class of a given left $\mathcal{O}$-ideal I. After introducing the necessary background on quaternion orders and ideals in § 2 and addressing some preliminary algorithmic problems in § 3, we solve the ℓ-power norm problem in § 4. Subject to reasonable heuristics

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 11RXX, 11YXX (primary), 11GXX, 11SXX (secondary).

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.

The third author is supported by an F.R.S.-FNRS postdoctoral research fellowship at Université catholique de Louvain, Louvain-la-Neuve.

on the probability of finding suitable primes, we obtain a probabilistic algorithm which solves this problem in expected polynomial time. The experimental runtime agrees with the most optimistic predictions for the distribution of primes.

The algorithm gives a clear distinction between the efficiency of the ℓ-isogeny problem in the equivalent category of quaternion ideals, whereas the analogous problem in the category of supersingular elliptic curves, on which the security of the Charles–Goren–Lauter hash function [4] is based, has to date resisted attack. This dichotomy poses several questions on the extent to which the information from the algebraic category can be transported to the geometric one. In particular, one expects an algorithm for computing the endomorphism ring of a given elliptic curve to provide an effective reduction to the algebraic setting, making the hardness of this problem critical to the underlying security.

2. *The quaternion ℓ-isogeny path problem*

In this section we first motivate and define the quaternion ℓ-isogeny path problem. We then recall basic facts on quaternion algebras. We introduce *p-extremal* maximal orders, which will play an important role in our solution of the quaternion ℓ-isogeny problem. We finally discuss properties of reduced norms and ideal morphisms.

2.1. *'Hard' isogeny problems*

The motivation for studying the quaternion ℓ-isogeny problem is based on the analogous (indeed categorically equivalent) problem for supersingular elliptic curves. The difficulty of this problem for elliptic curves underlies the security of the Charles–Goren–Lauter hash function [4].

As an example, finding a preimage (inverting the function) amounts to solving the following path problem in the supersingular ℓ-isogeny graph.

PROBLEM 1. Let p and ℓ be prime numbers, $p \neq \ell$. Let E_0 and E_1 be two supersingular elliptic curves over $\mathbb{F}_{p^2}$ with $|E_0(\mathbb{F}_{p^2})| = |E_1(\mathbb{F}_{p^2})| = (p+1)^2$. Find $k \in \mathbb{N}$ and an isogeny of degree ℓ^k from E_0 to E_1.

Similarly, finding collisions requires a solution to the following multiple path problem in the supersingular ℓ-isogeny graph.

PROBLEM 2. Let p and ℓ be prime numbers, $p \neq \ell$. Let E_0 be a supersingular elliptic curve over $\mathbb{F}_{p^2}$. Find $k_1, k_2 \in \mathbb{N}$, a supersingular elliptic curve E_1 and two distinct isogenies (i.e. with distinct kernels) of degrees respectively ℓ^{k_1} and ℓ^{k_2} from E_0 to E_1.

Setting $\mathcal{O} = \mathrm{End}(E_0)$, we have a category of left $\mathcal{O}$-ideals, with morphisms $I \to I\alpha \subseteq J$, for α in $B = \mathcal{O} \otimes \mathbb{Q}$, which is equivalent to the category of supersingular elliptic curves and isogenies. The analog of the path problem in supersingular ℓ-isogeny graphs is that of finding a representative ideal J for given I of norm ℓ^k. We call this problem the *quaternion ℓ-isogeny path problem*, and focus on its effective solution in this paper.

2.2. *Quaternion algebras*

In this work we consider the structure of left ideals of a maximal order in the quaternion algebra $B_{p,\infty}$ ramified only at p and ∞. Such an algebra is isomorphic to $\mathrm{End}(E) \otimes \mathbb{Q}$ for any supersingular elliptic curve $E/\mathbb{F}_{p^2}$. Here we denote $\mathrm{End}(E) = \mathrm{End}_{\bar{\mathbb{F}}_p}(E)$ and if we assume $\#E(\mathbb{F}_{p^2}) = (p+1)^2$, then the full endomorphism ring $\mathrm{End}(E)$ is defined over $\mathbb{F}_{p^2}$. Any definite

quaternion algebra over $\mathbb{Q}$ has a presentation of the form $\mathbb{Q}\langle i,j\rangle$, where $i^2 = a$, $j^2 = b$, $k = ij = -ji$ for negative integers a, b. The canonical involution on $B_{p,\infty}$ is given by

$$\alpha = x_0 + x_1 i + x_2 j + x_3 k \longmapsto \bar{\alpha} = x_0 - x_1 i - x_2 j - x_3 k$$

from which the reduced trace and norm take the form

$$\mathrm{Trd}(\alpha) = \alpha + \bar{\alpha} = 2x_0 \quad \text{and} \quad \mathrm{Nrd}(\alpha) = \alpha\bar{\alpha} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2.$$

The integral basis $\{1, i, j, k\}$ has the nice property of being an orthogonal basis with respect to the bilinear form $\langle x, y\rangle = \mathrm{Nrd}(x + y) - \mathrm{Nrd}(x) - \mathrm{Nrd}(y)$ associated to the reduced norm. Nevertheless, the order $\mathcal{O} = \mathbb{Z}\langle i, j\rangle$ is never maximal.

2.3. *Extremal orders*

In this work we first place the focus on the *p-extremal* maximal orders $\mathcal{O}$ containing π such that $\pi^2 = -p$. For a general order there exists a unique maximal two-sided ideal $\mathfrak{P}$ over p, and this ideal is principal if and only if there exists such an element π. The maximal ideal $\mathfrak{P}$ is a generator of the two-sided class group, and p-extremal orders are precisely those of trivial two-sided class number. In the context of supersingular elliptic curves, these are the maximal orders which are endomorphism rings of elliptic curves defined over $\mathbb{F}_p$ with Frobenius endomorphism π.

Secondly, we focus on orders with distinguished quadratic subring R. For a maximal order $\mathcal{O}$ we define $d(\mathcal{O}) = \min\{\mathrm{disc}(R) : \mathbb{Z} \neq R \subsetneq \mathcal{O}\}$. Among all p-extremal maximal quaternion orders, we define a *special* p-extremal maximal order $\mathcal{O}$ to be a p-extremal maximal order such that $d(\mathcal{O})$ is minimal.

The following lemma establishes the main properties we need for such an order, after which Lemmas 2–4 provide for their existence by explicit construction.

LEMMA 1. *Let $\mathcal{O}$ be a maximal order in $B_{p,\infty}$ containing a subring $\mathbb{Z}\langle i, j\rangle$ with $i^2 = -q$, $j^2 = -p$, and $ij = -ji$, for q coprime to p. Set $R = \mathcal{O} \cap \mathbb{Q}[i]$ and let D be its discriminant. If R is the ring of integers of $\mathbb{Q}[i]$, then $R^\perp = Rj$ and $R + Rj$ is a suborder of index $|D|$ in $\mathcal{O}$. If ω is a generator of R, then*

$$\mathrm{Nrd}(x_1 + y_1\omega + (x_2 + y_2\omega)j) = f(x_1, y_1) + pf(x_2, y_2),$$

where $f(x, y)$ is a principal quadratic form of discriminant D.

Proof. The triviality of the trace of j and the anti-commuting relation $ij = -ji$ imply that $\mathbb{Q}(i)$ has orthogonal complement $\mathbb{Q}(i)j$ in $B_{p,\infty}$. Consequently $R^\perp \subset \mathcal{O}$ is a lattice in $\mathbb{Q}(i)j$ containing Rj, hence of the form $\mathfrak{a}j$ for a fractional ideal $\mathfrak{a}$ of R which contains R. The prime p is inert in R, since p is ramified in $B_{p,\infty}$ but not in R. Since the norm is integral on $\mathfrak{a}j$, and $\mathrm{Nrd}(j) = p$, it follows that $\mathfrak{a}$ is integral, hence equals R. The orthogonality of R and Rj implies that $j\beta = \bar{\beta}j$ for all β in R, so $jR = Rj$ and $R + Rj$ is closed under multiplication. The form of the norm follows from orthogonality and multiplicativity of the norm: $\mathrm{Nrd}(\beta_1 + \beta_2 j) = \mathrm{Nrd}(\beta_1) + p\mathrm{Nrd}(\beta_2)$. Consequently the discriminant of the norm form is D^2p^2, from which we conclude that $R + Rj$ has index $|D|$ in any maximal order. □

By convention, for our special p-extremal order $\mathcal{O}$, we fix $\mathbb{Z}[i] \subseteq R$ with $i^2 = -q$ and $D = \mathrm{disc}(R) = -d(\mathcal{O})$, and $j^2 = -p$ (i.e. $j = \pi$ above). Being of smallest discriminant, R is necessarily a maximal order whose discriminant is the first of the sequence

$$-3, -4, -7, -8, -q \quad \text{for prime } q \equiv 3 \bmod 4,$$

such that p is ramified or inert in R. The next three lemmas establish existence for $q = 1$, $q = 2$, and $q \equiv 3 \bmod 4$ prime. These lemmas incorporate and expand on Pizer [10, Propositions 5.1 and 5.2]. We recall that an order in a quaternion algebra is *Eichler* if it is the intersection of two maximal orders.

LEMMA 2. *Let $p \equiv 3 \bmod 4$ be a prime, and let $B = \mathbb{Q}\langle i, j\rangle$ be the quaternion algebra given by the presentation $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$, and set $R = \mathbb{Z}[i]$. Then B is ramified only at p and ∞, and $\mathbb{Z}\langle i, j\rangle$ is contained in exactly two maximal orders with index 4, described by the inclusion chains*

$$\mathbb{Z}\langle i, j\rangle \subsetneq \mathbb{Z}\left\langle i, \frac{1+i+j+k}{2}\right\rangle \subsetneq \begin{cases} \mathbb{Z}\left\langle i, \dfrac{1+j}{2}\right\rangle, \\ \mathbb{Z}\left\langle i, \dfrac{1+k}{2}\right\rangle. \end{cases}$$

In particular, $\mathbb{Z}\langle i, (1+i+j+k)/2\rangle$ is an Eichler order, but $\mathbb{Z}\langle i, j\rangle$ is not.

LEMMA 3. *Let $p \equiv 5 \bmod 8$ be a prime, and let $B = \mathbb{Q}\langle i, j\rangle$ be the quaternion algebra given by the presentation $i^2 = -2$, $j^2 = -p$, and $k = ij = -ji$, and set $R = \mathbb{Z}[i]$. Then B is ramified only at p and ∞, and $\mathbb{Z}\langle i, j\rangle$ is contained in exactly two maximal orders with index 8, described by the inclusion chains*

$$\mathbb{Z}\langle i, j\rangle \subsetneq \mathbb{Z}\left\langle i, j, \frac{i+k}{2}\right\rangle \subsetneq \mathbb{Z}\left\langle i, \frac{i+k}{2}, \frac{1+j+k}{2}\right\rangle \subsetneq \begin{cases} \mathbb{Z}\left\langle i, \dfrac{1+j+k}{2}, \dfrac{i+2j+k}{4}\right\rangle, \\ \mathbb{Z}\left\langle i, \dfrac{1+j+k}{2}, \dfrac{i+2j-k}{4}\right\rangle. \end{cases}$$

In particular, $\mathbb{Z}\langle i, j\rangle$ is not an Eichler order.

LEMMA 4. *Let p and q be primes, with $p \equiv 1 \bmod 4$, $q \equiv 3 \bmod 4$, and*

$$\left(\frac{-p}{q}\right) = 1.$$

Let $B = \mathbb{Q}\langle i, j\rangle$ be the quaternion algebra given by the relations $i^2 = -q$, $j^2 = -p$, and $k = ij = -ji$, and set $R = \mathbb{Z}[(1+i)/2]$. Then B is ramified only at p and ∞, and $\mathbb{Z}\langle (1+i)/2, j\rangle = R + Rj$ is contained in exactly two maximal orders with index q, described by the inclusion chains

$$\mathbb{Z}\langle (1+i)/2, j\rangle \subsetneq \begin{cases} \mathbb{Z}\left\langle \dfrac{1+i}{2}, j, \dfrac{ci+k}{q}\right\rangle, \\ \mathbb{Z}\left\langle \dfrac{1+i}{2}, j, \dfrac{ci-k}{q}\right\rangle, \end{cases}$$

where c is any root of $x^2 + p \bmod q$. In particular, $R + Rj$ is an Eichler order.

Under the generalized Riemann hypothesis, for $p \equiv 1 \bmod 4$, the smallest q satisfying the conditions of the last lemma is $O(\log(p)^2)$ by a result of Ankeny [1] (or explicitly $q < 2\log(p)^2$ by Bach [2]). In the remainder of this paper, we will assume that $B_{p,\infty}$, $\mathcal{O}$, and R are suitably constructed from these lemmas with $\operatorname{disc}(R)$ the minimal discriminant in which p is inert in the sequence -3, -4, -7, -8, or $-q$ for $q \equiv 3 \bmod 4$ prime.

2.4. *Reduced norms and ideal morphisms*

Now suppose that $\mathcal{O}$ is any maximal order. We recall that the reduced norm on $B_{p,\infty}$ induces a reduced norm on left ideals defined by any of the equivalent conditions

$$\mathrm{Nrd}(I) := \sqrt{|\mathcal{O}/I|} = \gcd(\{\mathrm{Nrd}(\alpha) : \alpha \in I\}),$$

or by $I\bar{I} = \mathrm{Nrd}(I)\mathcal{O}$. It follows that the reduced norm on ideals is multiplicative and compatible with the reduced norm on elements $\mathrm{Nrd}(\alpha) = \mathrm{Nrd}(\alpha\mathcal{O}) = \mathrm{Nrd}(\mathcal{O}\alpha)$. If I and J are left $\mathcal{O}$-ideals, a homomorphism of I to J is a map given by $\alpha \mapsto \alpha\gamma$ for γ in $B_{p,\infty}^*$, which is an isomorphism if $J = I\gamma$. By the multiplicativity of the reduced norm, isomorphisms are similitudes of quadratic modules (with respect to the reduced norm). In particular, an isomorphism sends a reduced basis to a reduced basis. In fact the normalized norm map

$$q_I = \frac{\mathrm{Nrd}}{\mathrm{Nrd}(I)} : I \longrightarrow \mathbb{Z}$$

remains invariant under this isomorphism, in the sense that $q_I(\alpha) = q_J(\beta)$ for α in I and $\beta = \alpha\gamma$ in J. The normalized norm q_I is a positive-definite integral quadratic map, whose bilinear module given by $\langle x, y\rangle = q_I(x + y) - q_I(x) - q_I(y)$ has determinant p^2. This follows from the same property for any maximal order (see Pizer [**10**, Proposition 1.1]), since $|\mathcal{O}/I| = \mathrm{Nrd}(I)^2$, and the fact that any submodule of index m in a quadratic module L has determinant $m^2 \det(L)$.

The following lemma serves to replace an ideal I with an isomorphic one of different reduced norm.

LEMMA 5. *Let I be a left $\mathcal{O}$-ideal of reduced norm N and α an element of I. Then $I\gamma$, where $\gamma = \bar{\alpha}/N$, is a left $\mathcal{O}$-ideal of norm $q_I(\alpha)$.*

Proof. By the multiplicativity of the reduced norm, and $\mathrm{Nrd}(\alpha) = \mathrm{Nrd}(\bar{\alpha})$, we have

$$\mathrm{Nrd}(I\gamma) = \mathrm{Nrd}(I)\mathrm{Nrd}(\gamma) = N\frac{\mathrm{Nrd}(\alpha)}{N^2} = \frac{\mathrm{Nrd}(\alpha)}{N} = q_I(\alpha).$$

Clearly I is a fractional left $\mathcal{O}$-ideal, so it remains to show that $I\gamma \subseteq \mathcal{O}$. Since $\mathcal{O}\alpha \subseteq I$, we have $\bar{\alpha} \subseteq \bar{I}$, and hence $I\bar{\alpha} \subseteq I\bar{I} = N\mathcal{O}$, from which $I\gamma \subseteq \mathcal{O}$ follows. □

3. *Preliminary algorithmic results*

In this section we provide two algorithmic tools that will be used to solve the quaternion ℓ-isogeny path problem in § 4. The first algorithm computes prime norm representatives in ideal classes. The second computes representations of integers by the norm form of a p-extremal order.

3.1. *Computing prime norm representatives in ideal classes*

Given a maximal order $\mathcal{O}$ and a left $\mathcal{O}$-ideal I, we give a probabilistic algorithm that computes another left $\mathcal{O}$-ideal $J = I\gamma$ in the same class, but with prime norm. Using Lemma 5, this problem reduces to the problem of finding a prime represented by q_I.

Prime norm algorithm. Given a left $\mathcal{O}$-ideal I of norm N, with a Minkowski-reduced basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$. Generate random elements $\alpha = \sum_i x_i\alpha_i$ with (x_1, x_2, x_3, x_4) in a box $[-m, m]^4$ until finding an element α of I with $q_I(\alpha)$ prime, and return $I(\bar{\alpha}/N)$.

Assuming that numbers represented by q_I behave like random numbers, it remains to ensure that $q_I([-m,m]^4)$ contains sufficiently many primes to have a high probability of finding one. If $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$ is a Minkowski-reduced basis, the $q_I(\alpha_i)$ attain the successive minima, and we have the bounds

$$p^2 \leqslant 16 q_I(\alpha_1)q_I(\alpha_2)q_I(\alpha_3)q_I(\alpha_4) \leqslant 4p^2,$$

where $q_I(\alpha_i) \leqslant q_I(\alpha_{i+1})$. For a generic ideal I we expect $q_I(\alpha_4)$ to be in $\tilde{O}(\sqrt{p})$. In the worst case, $q_I(\alpha_4)$ is in $\tilde{O}(p)$ when I equals an order $\mathcal{O}$ containing a subring R with $|\mathrm{disc}(R)|$ in $O(\log(p)^n)$. Assuming I is generic, we expect to find α with $q_I(\alpha)$ in $\tilde{O}(m^2\sqrt{p})$. In practice, we find sufficiently many primes $q_I(\alpha)$ for m which grows polynomially in $\log(p)$. However to provably terminate, even under the Generalized Riemann Hypothesis, it may be necessary to allow m to exceed a function in $O(\sqrt[4]{p})$, in which case the output may exceed $O(p)$.

We implemented a prime norm algorithm in Magma [7]. We tested it on ideals of ℓ-power norms generated via a random walk from a given maximal order. All our computations with primes of up to 200 bits and random ideals took seconds on an Intel Xeon CPU X5500 processor with 24 GB RAM running at 2.67 GHz. The norms of the output ideals J were experimentally only slightly larger than $\sqrt{p}$. The experimental results are given in § A.1.

3.2. *Representing integers by special orders*

We also consider the problem of representing a sufficiently large positive integer M by the norm form of $\mathcal{O}$. Suppose that $\mathcal{O}$ is a p-extremal order, with suborder $R+Rj$, and let $D = \mathrm{disc}(R)$. We let $\Phi(x)$ be a monotone function such that a suitable interval $[x, x+\Phi(x)]$ contains sufficiently many primes, and we assume that $M \geqslant p\,\Phi(M)$. If ω is a reduced generator of R (of trace 0 or ± 1), then the norm form on $R+Rj$ is of the form

$$\mathrm{Nrd}(\alpha+\beta j) = f(x_1,y_1) + pf(x_2,y_2),$$

where $\alpha = x_1 + y_1\omega$ and $\beta = x_2 + y_2\omega$, and $f(x,y)$ is a principal form. For (x,y) in $[-m,m]^2$ with $m = \lfloor\sqrt{\Phi(M)/|D|}\rfloor$, we have $f(x,y) < \Phi(M)$ and $\mathrm{Nrd}(\beta j) < p\,\Phi(M) < M$. This gives the following algorithm on which we build our strong approximation algorithm.

Integer representation. Given an integer $M \geqslant p\,\Phi(M)$. Set $m = \lfloor\sqrt{\Phi(M)/|D|}\rfloor$, and choose (x_2,y_2) at random in $[-m,m]^2$ until finding a prime $r = M - pf(x_2,y_2)$ which is split in R and for which a prime $\mathfrak{r}$ over r is principal. Let $\alpha = x_1 + y_1\omega$ be a generator for $\mathfrak{r}$, set $\beta = x_2 + y_2\omega$, and return $\alpha + \beta j$.

Clearly the output has norm M. We assume that primes have density $1/\log(M)$ in the arithmetic progression $M - p\,[0,\Phi(M)]$. Moreover, we assume that such primes are equidistributed among primes which are non-split and split in R and, in the latter case, among each of the $h(R)$ ideal classes of R. Finally, we must assume that elements $\beta = x_2 + y_2\omega$ give rise to integers $r = M - p\,\mathrm{Nrd}(\beta)$ with the same primality probabilities as random integers in the range $M - p\,[0,\Phi(M)]$. Under such heuristic assumptions, the expected number of random β to be tested is $2h(R)\log(M)$. Detecting a prime r, solving for a representative prime $\mathfrak{r}$ over r, and determination of a principal generator can be done in expected polynomial time by Cornaccia's algorithm [5].

Under the heuristic assumptions made above, we can appeal to average distributions among all arithmetic progressions $a - p\,[0,\Phi(M)]$, for representatives a of $(\mathbb{Z}/p\mathbb{Z})^*$. In the application that follows, M will be of the form ℓ^e or $N\ell^e$, and we can adapt to failure to find primes in a particular arithmetic progression sparsely populated with primes by changing e.

4. *Main algorithm*

In this section we provide an algorithm to solve the quaternion ℓ-isogeny path problem. We also sketch a generalization of our approach to build ideal class representatives with powersmooth norms.

4.1. *Overview of the algorithm*

We reduce the quaternion ℓ-isogeny problem to a restricted version of the same problem, where we assume that $\mathcal{O}$ is a special p-extremal maximal order with suborder $R + Rj$ as defined in § 2.2. We also assume that I is a left $\mathcal{O}$-ideal with reduced norm N, where N is a (large) prime coprime to ℓ, $|\mathrm{disc}(R)|$ and p. A reduction from generic left $\mathcal{O}$-ideals to left $\mathcal{O}$-ideals with the required norms can be effectively performed with the algorithm of § 3.1. A reduction from general maximal orders to special p-extremal orders will be provided in § 4.6.

Using Lemma 5, the quaternion ℓ-isogeny path problem is also reduced to an effective strong approximation theorem in § 4.2. In particular, if the ideal is given by a pair of generators $I = \mathcal{O}(N, \alpha)$, the quaternion ℓ-isogeny path problem is reduced to finding $\lambda \in \mathbb{Z}$ coprime to N and

$$\beta \equiv \lambda\alpha \bmod N\mathcal{O}$$

with $\mathrm{Nrd}(\beta) = N\ell^e$ for some positive integer e.

Sections 4.3–4.5 describe the core of our approach to solve this problem. Since the index of $R + Rj$ in $\mathcal{O}$ is coprime to N, we have an isomorphism

$$\frac{R + Rj}{N(R + Rj)} \cong \frac{\mathcal{O}}{N\mathcal{O}}.$$

We can therefore choose representative elements in $R + Rj$ as convenient to simplify the algorithm. Since the index $[\mathcal{O} : R + Rj] = |\mathrm{disc}(R)|$ is assumed to be small (in $O(\log(p)^2)$ under the Generalized Riemann Hypothesis), the size of the output might be slightly larger, but the distinction is asymptotically insignificant. A direct approach to the strong approximation problem to solve for β seems daunting, so instead we reduce to the following steps:

(1) solve for a random $\gamma \in \mathcal{O}$ of reduced norm $N\ell^{e_0}$;
(2) solve for $[\mu]$ in $(\mathcal{O}/N\mathcal{O})^*$ such that $(\mathcal{O}\gamma/N\mathcal{O})[\mu] = I/N\mathcal{O}$;
(3) solve for the strong approximation of $[\mu]$ (modulo N) by μ in $\mathcal{O}$ of reduced norm ℓ^{e_1}.

Here we denote the element $\mu + N\mathcal{O}$ of $\mathcal{O}/N\mathcal{O}$ by $[\mu]$ to distinguish it from the conjugate $\bar{\mu}$ of μ. The output $\beta = \gamma\mu$ is then an element of I with reduced norm $N\ell^e$ where $e = e_0 + e_1$. The element γ can be constructed with the algorithm of § 3.2. We solve for $[\mu]$ by linear algebra in § 4.3, showing that we can take $[\mu]$ in $(R/NR)^*[j] \subseteq (\mathcal{O}/N\mathcal{O})^*$. The core of the algorithm is the final specialized strong approximation algorithm of § 4.4, taking $[\mu]$ in $(R/NR)^*[j]$ and constructing the lifting μ of norm ℓ^e. The whole algorithm for p-extremal orders is analyzed in § 4.5.

As mentioned above, we finally remove the p-extremal condition in § 4.6 by providing a reduction from the general case to the case of p-extremal orders, and we generalize our approach to compute ideal representatives of smooth or powersmooth norms in § 4.7.

4.2. *Effective strong approximation*

Let $B := B_{p,\infty}$ be the quaternion algebra ramified at p and ∞. Let $\mathbb{A}_{\mathbb{Q}}$ be the rational adèle ring, defined as the restricted product of $\mathbb{Q}_v$ with respect to $\mathbb{Z}_v$, let $\ell \neq p$ be a 'small' prime, and let $\mathbb{A}_{\mathbb{Q},\ell}$ be the restricted product over all $v \neq \ell$. Let $\mathbb{A}_B = B \otimes_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q}}$ be the adèle ring of B, and $\mathbb{A}_{B,\ell} = B \otimes \mathbb{A}_{\mathbb{Q},\ell}$. Then B embeds diagonally in $\mathbb{A}_B$ and is discrete in $\mathbb{A}_B$ (see [**3**, § 14]). The strong approximation theorem (see [**3**, § 15]) asserts that B is dense in $\mathbb{A}_{B,\ell}$ (see also Vignéras [**11**, Théorème Fondamental 1.4, p. 61]).

The strong approximation theorem can be viewed as a strong version of the Chinese remainder theorem. We apply this to find an element of a left $\mathcal{O}$-ideal I which generates I almost everywhere. Each such ideal is known to be generated by two elements N and α, where we may take $N = \mathrm{Nrd}(I)$ for the first generator. This follows since locally $\mathcal{O}_v = \mathcal{O} \otimes \mathbb{Z}_v$ is a left principal ideal ring, hence so is the quotient $\mathcal{O}/N\mathcal{O}$.

If $I = \mathcal{O}(N, \alpha) := \mathcal{O}N + \mathcal{O}\alpha$, the approximation theorem implies that we can find β in I such that

$$\beta \equiv \alpha \bmod N\mathcal{O}$$

and $\mathrm{Nrd}(\beta) = N\ell^e$ for some positive integer e, from which $I = \mathcal{O}(N, \alpha) = \mathcal{O}(N, \beta)$. By Lemma 5, an effective version of this strong approximation theorem is sufficient to solve the quaternion ℓ-isogeny path problem. In particular, since β is in I, the ideal $I\bar{\beta}/N$ is an isomorphic ideal of norm ℓ^e.

Similarly, solving for

$$\beta \equiv \lambda\alpha \bmod N\mathcal{O},$$

with $\lambda \in \mathbb{Z}$ coprime to N such that we still have $I = \mathcal{O}(N, \beta)$, is also sufficient to solve the quaternion ℓ-isogeny path problem. We will focus on this relaxed effective strong approximation theorem in the next subsections.

4.3. *Isomorphism of $\mathcal{O}/N\mathcal{O}$-ideals*

In this section let I be a left $\mathcal{O}$-ideal of prime norm $N \neq p$, and let γ be an arbitrary element of $\mathcal{O}$ of norm NM, where $\gcd(N, M) = 1$. Since N is large, we can assume that it does not divide the index $[\mathcal{O} : R + Rj]$, hence we have equalities of rings

$$\mathcal{O}/N\mathcal{O} = (R + Rj)/N(R + Rj) \cong \mathbb{M}_2(\mathbb{Z}/N\mathbb{Z}).$$

We denote by $[\alpha]$ the class of an element α in $\mathcal{O}/N\mathcal{O}$ (as distinct from its conjugate $\bar{\alpha}$).

We note that $\mathcal{O}\gamma/N\mathcal{O}$ and $I/N\mathcal{O}$ are proper non-zero left $\mathcal{O}/N\mathcal{O}$-ideals. The following explicit classification of such ideals, in $\mathbb{M}_2(\mathbb{Z}/N\mathbb{Z})$, will let us construct an explicit isomorphism between these ideals.

LEMMA 6. *Let N be a prime and $A = \mathbb{M}_2(\mathbb{Z}/N\mathbb{Z})$. There exists a bijection*

$$S : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \times \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \longrightarrow \frac{\{\gamma \in A \backslash \{0\} : \det(\gamma) = 0\}}{(\mathbb{Z}/N\mathbb{Z})^*},$$

given by

$$S((u : v), (x : y)) = \begin{pmatrix} ux & uy \\ vx & vy \end{pmatrix}.$$

Under this correspondence, the set of proper non-trivial left A-ideals is in bijection with the set

$$\{\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \times (x : y) : (x : y) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})\},$$

and the right action of $A^*/(\mathbb{Z}/N\mathbb{Z})^* = \mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$ on left A-ideals is transitive and induced by the natural (transpose) action on $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.

Proof. The non-zero matrices of determinant zero, modulo $(\mathbb{Z}/N\mathbb{Z})^*$, determine a hypersurface $ad = bc$, which is the image of $\mathbb{P}^1 \times \mathbb{P}^1$ by the Segre embedding in $\mathbb{P}^3$ $(= (A\backslash\{0\})/(\mathbb{Z}/N\mathbb{Z})^*)$. It is easily verified that left and right multiplication induce the standard and transpose multiplication on the first and second factors of $\mathbb{P}^1 \times \mathbb{P}^1$, respectively, under this isomorphism, from which the result follows. □

Using an explicit isomorphism $\mathcal{O}/N\mathcal{O} \cong \mathbb{M}_2(\mathbb{Z}/N\mathbb{Z})$, by this lemma we can find $[\mu]$ in $(\mathcal{O}/N\mathcal{O})^*$ such that $(\mathcal{O}\gamma/N\mathcal{O})[\mu] = I/N\mathcal{O}$, using linear algebra over $\mathbb{Z}/N\mathbb{Z}$.

In § 4.4 we require an input $[\mu]$ which is a unit in $Rj/N\mathcal{O}$. Observing that $[j]$ is a unit, we see that such units form a coset of $(R/NR)^*$:

$$(\mathcal{O}/N\mathcal{O})^* \cap Rj/N\mathcal{O} = (R/NR)^*[j].$$

We note that $(R/NR)^*$ acts on the $N+1$ proper non-trivial left $\mathcal{O}$-ideals, with kernel $(\mathbb{Z}/N\mathbb{Z})^*$. By hypothesis, R is a subring of small discriminant in which N is not ramified. If N is inert in R, then the $N+1$ ideals form one orbit. Otherwise, if N is split, there is one orbit of size $N-1$ and two fixed points $\mathcal{O}\mathfrak{p}_1/N\mathcal{O}$ and $\mathcal{O}\mathfrak{p}_2/N\mathcal{O}$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are the prime ideals of R over N. With overwhelming probability, $I/N\mathcal{O}$ and $\mathcal{O}\gamma/N\mathcal{O}$ will not be such fixed points, and so we can solve for $[\mu]$ in $(R/NR)^*[j]$. In the event of failure, we can select a new γ or N.

4.4. *Approximating elements of $(R/NR)^*[j]$ by ℓ-power norm representatives*

In this section we assume that ℓ is a quadratic non-residue modulo N. Let also ω be a generator of R of minimal norm, either 1, 2, or $(1+q)/4$, for q a prime congruent to 3 modulo 4. We now motivate the restriction to elements of $(R/NR)^*[j]$ in the previous section.

We suppose that we are given as input a lift $\mu_0 = x_0 + y_0\omega + (z_0 + w_0\omega)j$ of an arbitrary element of $\mathcal{O}/N\mathcal{O}$ to $R + Rj$. The relaxed approximation problem is to search for λ in $\mathbb{Z}$ and $\mu_1 = x_1 + y_1\omega + (z_1 + w_1\omega)j$ such that $\mu = \lambda\mu_0 + N\mu_1$ satisfies the norm equation

$$\mathrm{Nrd}(\mu) = f(\lambda x_0 + Nx_1, \lambda y_0 + Ny_1) + p\, f(\lambda z_0 + Nz_1, \lambda w_0 + Nw_1) = \ell^e,$$

for some $e \in \mathbb{N}$, where $f(x,y) = \mathrm{Nrd}(x + y\omega)$ is a principal binary quadratic form of discriminant D as in Lemma 1. The key idea to solve this norm equation, as used in [9] to cryptanalyze the other hash function of Charles, Goren and Lauter, is that it simplifies considerably when $x_0 = y_0 = 0$:

$$\mathrm{Nrd}(\mu) = N^2 f(x_1, y_1) + p\, f(\lambda z_0 + Nz_1, \lambda w_0 + Nw_1) = \ell^e. \tag{4.1}$$

The simple algorithm we now describe to solve this equation justifies the choice of $[\mu] \in (R/NR)^*[j]$ in § 4.3.

To construct μ, given $[\mu] \in (R/NR)^*[j]$, we consider a first lift $\mu_0 = (z_0 + w_0\omega)j$ to Rj as above, and find λ in $\mathbb{Z}$ and $\mu_1 = (x_1 + y_1\omega) + (z_1 + w_1\omega)j$ in $R + Rj$ satisfying the simplified equation (4.1). This equation modulo N gives $\lambda^2 p\, f(z_0, w_0) = \ell^e \bmod N$, and, since ℓ is a quadratic non-residue modulo N, we choose the parity of e depending on whether $p\, f(z_0, w_0)$ is a quadratic residue modulo N or not, and solve for a square root modulo N to find λ, in $0 < \lambda < N$.

Now for fixed z_0, w_0, and λ, equation (4.1) implies a linear equation in z_1 and w_1:

$$2\lambda p L((z_0, w_0), (z_1, w_1)) = \frac{\ell^e - \lambda^2 p f(z_0, w_0)}{N} \bmod N, \tag{4.2}$$

where L is the bilinear polynomial

$$L((z_0, w_0), (z_1, w_1)) = \langle z_0 + w_0\omega, z_1 + w_1\omega \rangle = 2z_0z_1 + \mathrm{Trd}(\omega)(z_0w_1 + w_0z_1) + 2\mathrm{Nrd}(\omega)w_0w_1.$$

Since N is a large prime, such that $\gcd(x_0w_0|D|p, N) = 1$, there are exactly N solutions (z_1, w_1) to the linear equation (4.2). We choose a random solution satisfying

$$|\lambda z_0 + Nz_1| < N^2 \quad \text{and} \quad |\lambda w_0 + Nw_1| < N^2,$$

and equation (4.1) now leads to a problem of representation of an integer by a binary quadratic form:

$$f(x_1, y_1) = r := \frac{\ell^e - p f(\lambda z_0 + Nz_1, \lambda w_0 + Nw_1)}{N^2}. \tag{4.3}$$

We assume that e was chosen sufficiently large so that r is positive. If r (or rq), modulo a smooth square integer factor, is prime, splits and is a norm in R, Cornaccia's algorithm [5] can efficiently solve this equation, or determine that no solution exists. In the latter case, we repeat with a new value of (z_1, w_1). Assuming the values of r behave as random values around $N^4|D|p$, we expect to choose $\log(N^4|D|p)h(D)$ values before finding a solution.

In practice, we begin with e the minimal possible value having the correct parity, then we progressively increase it if no solution has been found. For N in the range $\tilde{O}(\sqrt{p})$, we expect the size of e to satisfy $e \sim \log_\ell(N^4|D|p) \sim 3\log_\ell(p)$.

4.5. *Algorithm analysis and experimental results*

We summarize our algorithm to compute an ℓ-power norm representative of a left $\mathcal{O}$-ideal, where $\mathcal{O}$ is a special p-extremal maximal order.

THEOREM 7. *Let $\mathcal{O}$ be a maximal order in a quaternion algebra $B_{p,\infty}$ and let ℓ be a small prime. There exists a probabilistic algorithm, which takes as input a left $\mathcal{O}$-ideal and outputs an isomorphic left $\mathcal{O}$-ideal of ℓ-power reduced norm.*

Under the most optimistic heuristic assumptions on randomness of representations of integers by quadratic forms and uniform distributions of primes, this algorithm is expected to run in polynomial time and to produce ideals of norm ℓ^e, where

$$e \sim \log_\ell(Np\Phi(p)|D|) + \log_\ell(N^4|D|p) - \log_\ell N^2,$$

where the three terms respectively account for the norms of γ, μ and N^{-1}. Assuming that $\log_\ell(N) \sim \frac{1}{2}\log_\ell(p)$ and that in practice $\Phi(p) \sim \log(p)^n$ suffices, this leads to

$$e \sim \tfrac{7}{2}\log_\ell(p).$$

We implemented the algorithms of this paper in Magma [7]. We first tested the algorithm of § 3.2 to compute N times ℓ-power norm elements in $\mathcal{O}$ with $\ell \in \{2, 3\}$, for random primes p of sizes up to 200 bits and for N values obtained after applying the algorithm of § 3.1 on an ideal generated via a random walk from $\mathcal{O}$. The norm of the outputs was close to the expected values.

We then tested the algorithm of § 4.4 for $\ell \in \{2, 3\}$, for random p values of sizes up to 200 bits, for N values obtained after applying the algorithm of § 3.1 on an ideal generated via a random walk from $\mathcal{O}$, and for $\mu_0 = (z_0 + w_0\omega)j$ with randomly chosen $z_0, w_0 \in \mathbb{Z}/N\mathbb{Z}$ not both equal to zero. The exponents of the norms of the quaternions computed were close to the expected value $3\log_\ell p$.

We finally tested the overall algorithm of § 4 for $\ell \in \{2, 3\}$, for random p values of sizes up to 200 bits, and for ideals I generated via a random walk from $\mathcal{O}$. The ℓ-valuation of the norm of the ideals computed was close to the expected value $\frac{7}{2}\log_\ell p$.

All computations were carried out on an Intel Xeon CPU X5500 processor with 24 GB RAM running at 2.67 GHz. The algorithm of § 4.4 succeeded in less than 100 s for all 200 bit primes, and the overall algorithm of § 4 terminated in less than 250 s for primes in this range. Additional experimental results are provided in the Appendix.

4.6. *Generalization to arbitrary orders*

We now describe how to remove the condition that $\mathcal{O}$ is one of the special orders defined in § 2.2. First we encode the relation between two maximal orders embedded in $B_{p,\infty}$ in terms of an associated ideal.

LEMMA 8. *Suppose that $\mathcal{O}_1$ and $\mathcal{O}_2$ are given maximal orders in $B_{p,\infty}$. Then the Eichler order $\mathcal{O}_1 \cap \mathcal{O}_2$ has the same index in each of $\mathcal{O}_1$ and $\mathcal{O}_2$, which we denote M, and the set*

$$I(\mathcal{O}_1, \mathcal{O}_2) = \{\alpha \in B_{p,\infty} \mid \alpha\mathcal{O}_2\bar{\alpha} \subseteq M\mathcal{O}_1\}$$

is a left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal of reduced norm M. Conversely, if I is a left $\mathcal{O}_1$-ideal with right order $\mathcal{O}_2$, such that $I \not\subseteq n\mathcal{O}_1$ for any $n > 1$, then $I = I(\mathcal{O}_1, \mathcal{O}_2)$.

Proof. The determinant of the norm form of any maximal order $\mathcal{O}$ is p^2, and for any sublattice $L \subset \mathcal{O}$ of index M, the reduced norm form on L has determinant $M^2 \det(\mathcal{O})$. This establishes the well-known result that the index of an Eichler order in any maximal order is an invariant, called its level.

It is clear by construction that $I(\mathcal{O}_1, \mathcal{O}_2)$ is a left $\mathcal{O}_1$-module and a right $\mathcal{O}_2$-module. Locally at any prime q, we may assume $\mathcal{O}_1$ and $\mathcal{O}_2$ are $\mathbb{Z}_q$-orders such that $\mathcal{O}_2 = \alpha^{-1}\mathcal{O}_1\alpha$, for some α in $\mathcal{O}_1$ hence also in $\mathcal{O}_2$. It follows that we have an inclusion $\alpha\mathcal{O}_2 = \mathcal{O}_1\alpha \subseteq I(\mathcal{O}_1, \mathcal{O}_2)$. However, removing any integer factors (in the center), the reduced norm of a minimal α must equal the level $M\mathbb{Z}_q$, which implies equality. The global result follows from the local–global principle.

Conversely, since any left $\mathcal{O}_1$-ideal I is locally principal at each prime q, one can find locally α such that $I = \mathcal{O}_1\alpha$; the right order of I is then $\mathcal{O}_2 = \alpha^{-1}\mathcal{O}_1\alpha$. By hypothesis α is not divisible by any integer and we conclude that the Eichler order has level $\mathrm{Nrd}(\alpha) = \mathrm{Nrd}(I) = M\mathbb{Z}_q$. From the above construction in terms of a local generator, we conclude $I = I(\mathcal{O}_1, \mathcal{O}_2)$. □

THEOREM 9. *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be maximal orders in a quaternion algebra $B_{p,\infty}$ and let ℓ be a small prime. Given an algorithm which takes as input a left $\mathcal{O}_1$-ideal and outputs an equivalent left $\mathcal{O}_1$-ideal of ℓ-power reduced norm, there exists an algorithm with the same complexity, up to a constant of size polynomial in the input size of $\mathcal{O}_1$ and $\mathcal{O}_2$, which takes as input a left $\mathcal{O}_2$-ideal and outputs an equivalent left $\mathcal{O}_2$-ideal of ℓ-power reduced norm.*

Proof. Assume we are given two orders $\mathcal{O}_1$, $\mathcal{O}_2$ and a left $\mathcal{O}_2$-ideal J, and set $I = I(\mathcal{O}_1, \mathcal{O}_2)$ as in Lemma 8. The ideal I may be of arbitrarily large norm, but is bounded by something polynomial in the specification of $\mathcal{O}_1$ and $\mathcal{O}_2$ in terms of a basis for $B_{p,\infty}$.

Supposing that we have an algorithm for $\mathcal{O}_1$, we find representative left $\mathcal{O}_1$-ideals for I and IJ such that $I_1 = I\bar{\gamma}_1/\mathrm{Nrd}(I)$ with γ_1 in I, and $I_2 = IJ\bar{\gamma}_2/\mathrm{Nrd}(IJ)$ with γ_2 in IJ, where

$$\mathrm{Nrd}(\gamma_1) = \mathrm{Nrd}(I)\ell^{e_1} \quad \text{and} \quad \mathrm{Nrd}(\gamma_2) = \mathrm{Nrd}(IJ)\ell^{e_2}.$$

It follows that $\gamma = \bar{\gamma}_1\gamma_2/\mathrm{Nrd}(I)$ is an element of J with reduced norm $\mathrm{Nrd}(\gamma) = \mathrm{Nrd}(J)\ell^{e_1+e_2}$, and hence $J\bar{\gamma}/\mathrm{Nrd}(J)$ is of reduced norm $\ell^{e_1+e_2}$. □

This provides a reduction of the general case to the case of special p-extremal orders, at the cost of two applications of the algorithm of § 4, and a larger power of ℓ.

4.7. *Generalization to powersmooth norms*

We recall that a number $s = \prod \ell_i^{e_i}$ is S-powersmooth if $\ell_i^{e_i} < S$. Our algorithms can be easily modified to construct ideal representatives of powersmooth norms. Using the approximations as before, the norm should be of size close to $p^{7/2}$. Since the product of all maximal powers of a prime lower than S can be approximated by $S^{S/\log S}$, an adaptation of our algorithms will allow us to compute S-powersmooth representatives of left ideal classes of $\mathcal{O}$, with $S \approx \frac{7}{2}\log p$.

5. *Conclusion and future work*

In this paper we have provided a probabilistic algorithm to solve a quaternion ideal analog of the path problem in supersingular ℓ-isogeny graphs. The algorithm runs in expected

polynomial time subject to heuristics on expected distributions of primes, and it is efficient in practice.

Following Deuring [6], there is a one-to-one correspondence between supersingular elliptic curves modulo p, up to Galois conjugacy, and isomorphism classes of maximal orders in the quaternion algebra $B_{p,\infty}$. By identifying isogeny kernels with powersmooth ideals in the quaternion algebra graphs, we expect our techniques to lead to both partial attacks on Charles, Goren and Lauter's isogeny based hash function (when the initial curve has extremal endomorphism ring), and to security reductions to the problem of computing the endomorphism ring of a supersingular elliptic curve. Similarly, we expect our results to lead to a constructive version of Deuring's correspondence from maximal orders in $B_{p,\infty}$ to their corresponding elements in the category of supersingular elliptic curves.

Appendix. *Experimental results*

In our experiments, the value of m and the function Φ appearing in the specification of our algorithms were fixed to *a priori* minimal values based on probabilistic arguments on the distribution of primes, then increased when needed.

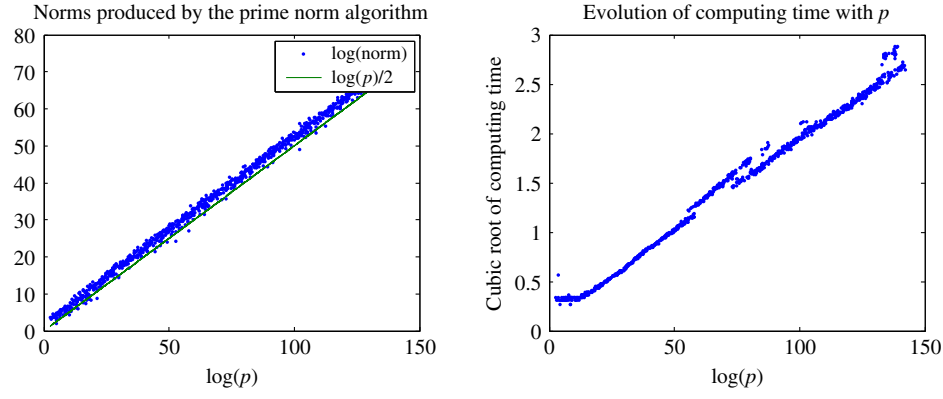

FIGURE A.1. *Experimental results for the algorithm of* § 3.1 *(with m of the expected size): logarithm of the output norm $q_I(\alpha)$ and cubic root of running time with respect to* $\log p$.

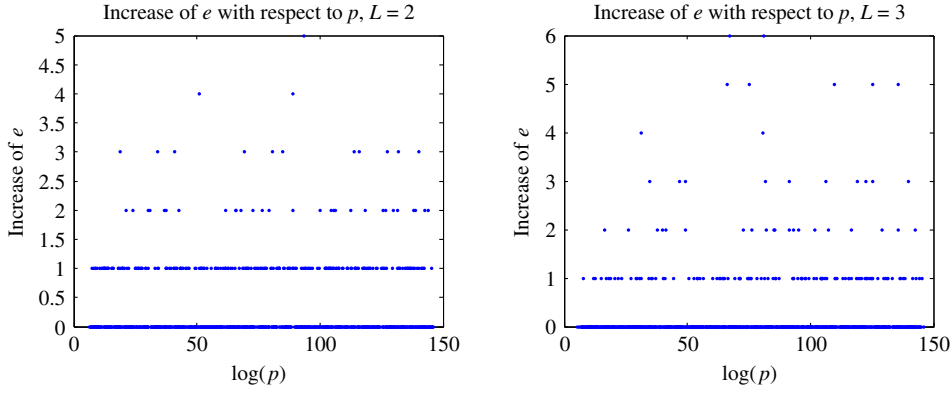

FIGURE A.2. *Experimental results for computing elements of norms $N\mathfrak{l}^e$ with the algorithm of* § 3.2, *for various p values with $\ell = 2$ (left) and $\ell = 3$ (right): difference between the minimal exponent e needed and a prediction based on probabilistic arguments.*

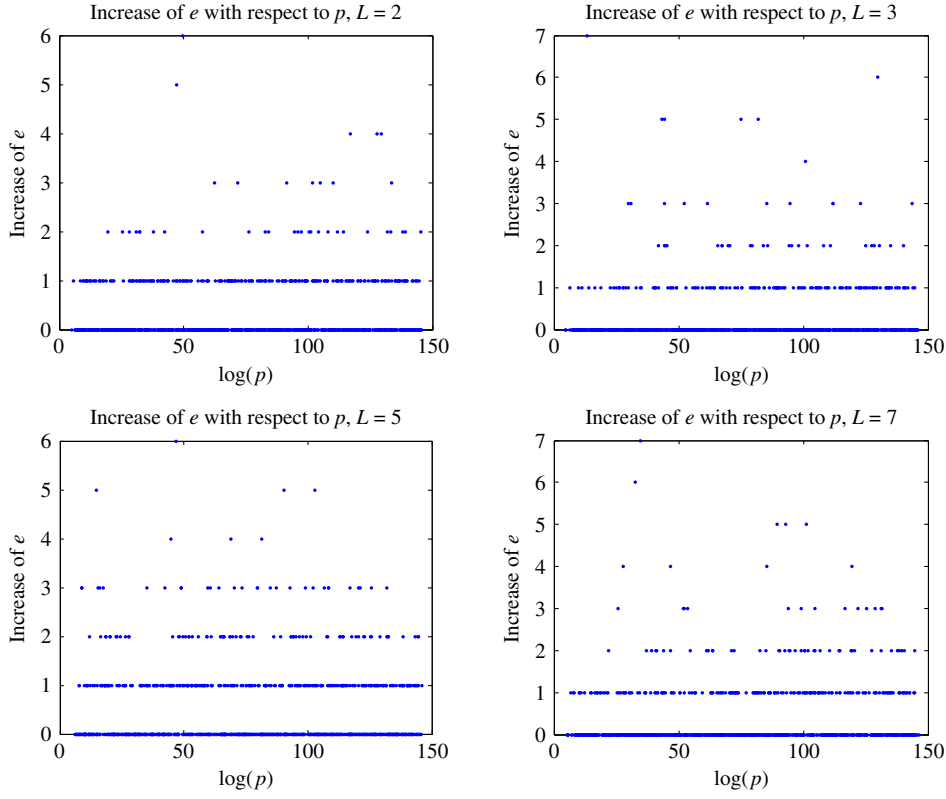

FIGURE A.3. *Experimental results for computing elements of norms ℓ^e with the algorithm of § 3.2, for $\ell \in \{2, 3, 5, 7\}$ and various p values: difference between the minimal exponent e needed and a prediction based on probabilistic arguments.*

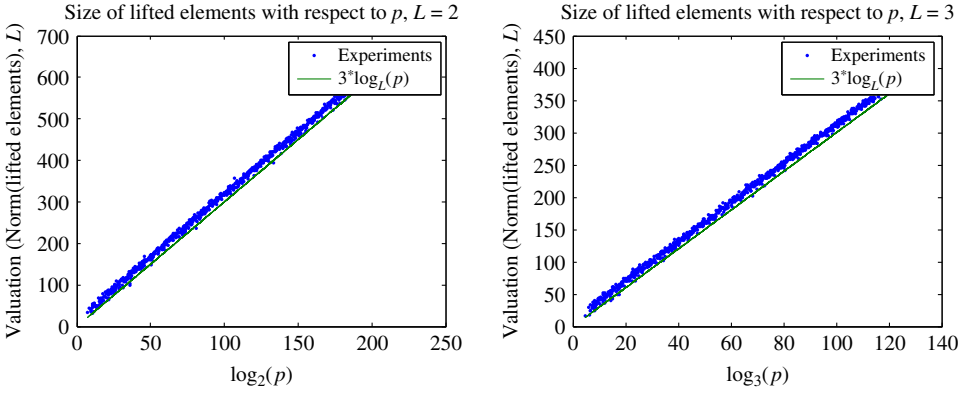

FIGURE A.4. *Size of ℓ-power norm quaternions obtained with the algorithm of § 4.4 for various p values with $\ell = 2$ (left) and $\ell = 3$ (right). The green line corresponds to the approximated values $3 \log_\ell p$.*

A.1. *Prime norm ideals*

We show experimental results on the prime norm algorithm of § 3.1 in Figure A.1. The norms of the ideals constructed seem to be slightly larger than $p^{1/2}$ and the computation time cubic in $\log(p)$.

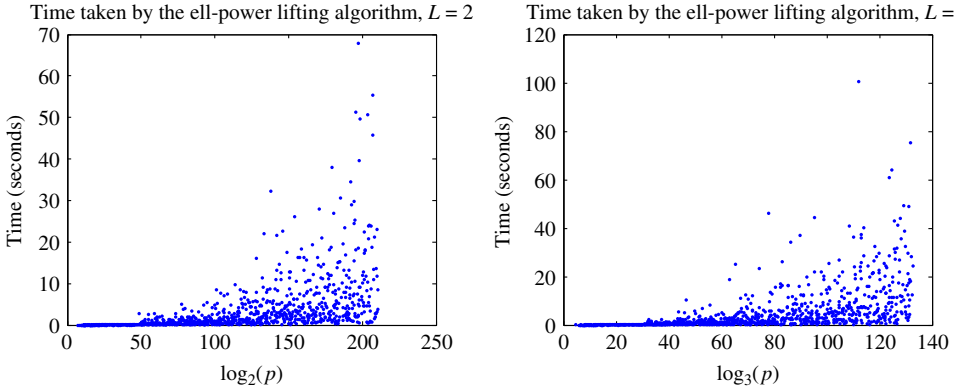

FIGURE A.5. *Time taken by the algorithm of § 4.4 for various p values, with $\ell = 2$ (left) and $\ell = 3$ (right).*

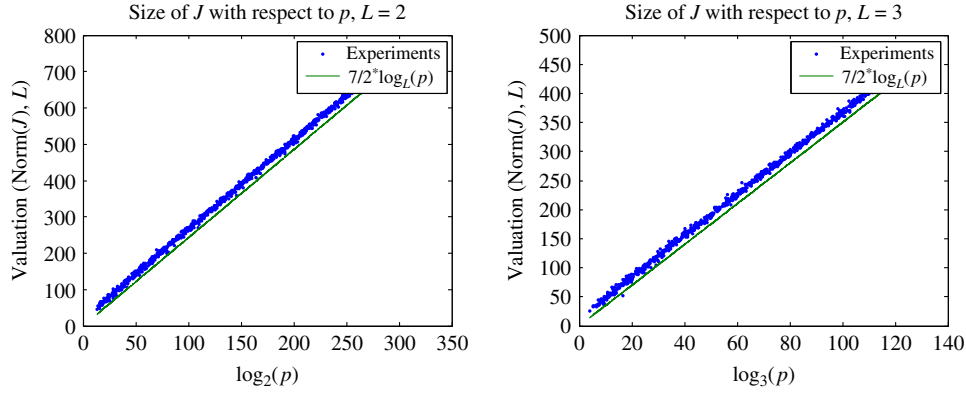

FIGURE A.6. *Size of ℓ-power norm ideals returned by the algorithm of § 4 for various p values with $\ell = 2$ (left) and $\ell = 3$ (right). The green line shows a priori approximative values $\frac{7}{2}\log_\ell p$.*

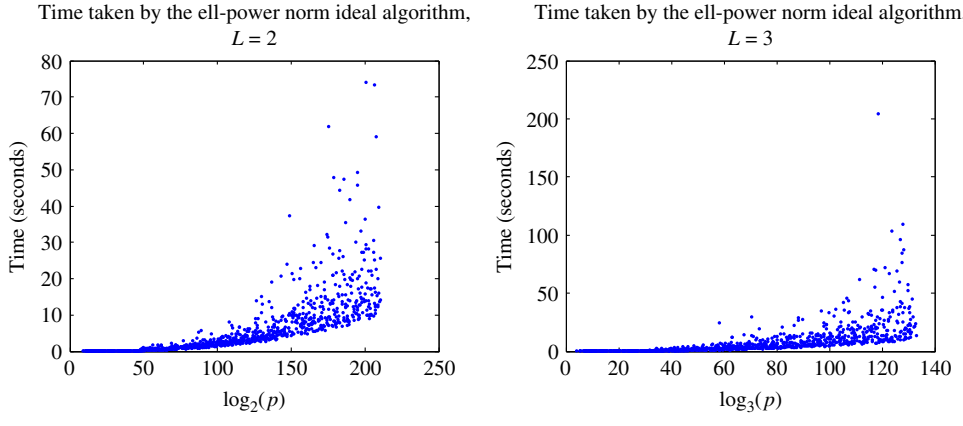

FIGURE A.7. *Time taken by the algorithm of § 4 for various p values with $\ell = 2$ (left) and $\ell = 3$ (right).*

A.2. *Quaternion elements with particular norms*

Experimental results on the algorithm of § 3.2 are shown in Figures A.2 and A.3, for computing elements of norms $N\ell^e$ or ℓ^e respectively, for some e. The results show the difference between the minimal exponent e needed and a prediction based on probabilistic arguments. All computations took less than 1 second.

A.3. *Ideals with ℓ-power norms*

Experimental results on the algorithms of § 4 are shown in Figures A.4–A.7.

Acknowledgements. The research leading to these results has received funding from the Fonds National de la Recherche — FNRS and from the European Research Council through the European ISEC action HOME/2010/ISEC/AG/INT-011 B-CCENTRE project.

References

1. N. C. Ankeny, 'The least quadratic non residue', *Ann. of Math.* (2) 55 (1952) no. 1, 65–72.
2. E. Bach, 'Explicit bounds for primality testing and related problems', *Math. Comp.* 55 (1990) no. 191, 355–380.
3. J. W. S. Cassels, 'Global fields', *Algebraic number theory* (eds J. W. S. Cassels and A. Frohlich; Academic Press, 1967) 42–84.
4. D. X. Charles, K. E. Lauter and E. Z. Goren, 'Cryptographic hash functions from expander graphs', *J. Cryptology* 22 (2009) no. 1, 93–113.
5. G. Cornacchia, 'Su di un metodo per la risoluzione in numeri interi dell'equazione $\sum_{h=0}^{n} c_h x^{n-h} y^h = p$', *Giornale di Matematiche di Battaglini* 46 (1903) 33–90.
6. M. Deuring, 'Die Typen der Multiplikatorenringe elliptischer Funktionenkörper', *Abh. Math. Semin. Univ. Hamb.* 14 (1941) 197–272.
7. W. Bosma, J. J. Cannon, C. Fieker and A. Steel (eds), *Handbook of Magma functions*, version 2.20 (2013) http://magma.maths.usyd.edu.au/magma/.
8. D. Kohel, (1996) 'Endomorphism rings of elliptic curves over finite fields', PhD Thesis, University of California, Berkeley.
9. C. Petit, K. Lauter and J.-J. Quisquater, 'Full cryptanalysis of LPS and Morgenstern hash functions', *Security and cryptography for networks*, Lecture Notes in Computer Science 5229 (eds R. Ostrovsky, R. De Prisco and I. Visconti; Springer, Berlin, 2008) 263–277.
10. A. Pizer, 'An algorithm for computing modular forms on $\Gamma_0(N)^*$', *J. Algebra* 64 (1980) 340–390.
11. M.-F. Vignéras, *Arithmétique des algèbres de quaternions* (Springer, 1980).

David Kohel
Institut de Mathématiques de Marseille
Université d'Aix-Marseille
163, avenue de Luminy, Case 907
13288 Marseille Cedex 9
France
David.Kohel@univ-amu.fr

Kristin Lauter
Microsoft Research
One Microsoft Way
Redmond, WA 98052
USA
klauter@microsoft.com

Christophe Petit
UCL Crypto Group
Université catholique de Louvain
Place du Levant 3
B1348 Louvain-la-Neuve
Belgium
christophe.petit@uclouvain.be

Jean-Pierre Tignol
UCL – ICTEAM/INMA
Université catholique de Louvain
Avenue G. Lemaitre 4, box L4.05.01
B1348 Louvain-la-Neuve
Belgium
Jean-Pierre.Tignol@uclouvain.be