Lenstra-Hurwitz cliques and the class number one problem

D. D. LONG
MORWEN B. THISTLETHWAITE

A new sufficient condition is given for a number field to have class number one.

11R04; 20H10

1 Introduction

In his celebrated paper [Lenstra, 1977], Lenstra showed that given a number field k, if one could find in the ring of integers $\mathcal{O}_k$ a sufficiently large set $\{\tau_1, \tau_2, \ldots, \tau_M\}$ with the property that for every $i \neq j$, $\tau_i - \tau_j$ is a *unit* of $\mathcal{O}_k$, then the field k is Euclidean in the classical sense, *i.e.* with respect to the field norm.

A natural way to view this set is to form a graph whose vertices are elements of $\mathcal{O}_k$, with two vertices connected by an edge if the difference of the endpoints is a unit of $\mathcal{O}_k$. In these terms, Lenstra's theorem involves a condition on the size of a *clique* (i.e. a complete subgraph) in this graph. The cliques used by Lenstra we shall refer to as *unit cliques*.

The purpose of this paper is to show that a related but more flexible condition can be used to ensure that $\mathcal{O}_k$ is a principal ideal domain, *i.e.* that k has class number one. To describe the result, we begin with the following definition:

Definition Suppose that k is a number field and that $\Sigma = \{\alpha_1, \ldots, \alpha_M\}$ is a collection of integers of k.

Then we say that Σ is a *Lenstra-Hurwitz clique* if it has the following properties:

(i) Every difference $\delta\alpha_{ij} = \alpha_i - \alpha_j$ is either a unit or generates a prime ideal of $\mathcal{O}_k$.

(ii) In the cases that $\delta\alpha_{ij}$ is not a unit, we have a projection onto a finite field

$$\pi : \mathcal{O}_k \to \mathcal{O}_k / < \delta\alpha_{ij} >= \mathcal{F}$$

and we require that the natural map $\pi : \mathcal{O}_k^* \to \mathcal{F}^*$ be a surjection.

This is a clique in the graph whose vertices are elements of $\mathcal{O}_k$, with two vertices connected by an edge if their difference satisfies (i) and (ii) of Definition 1.

Then we show

Theorem 1.1 *Let $M(k)$ be one of the packing constants for the field k, coming from* [Lenstra, 1977] (1.9) *or* (1.12).

Suppose that k has a Lenstra-Hurwitz clique with more than $M(k)$ elements. Then k has class number one.

We begin with some general remarks. Following standard nomenclature, we say that k is *Euclidean* if $\mathcal{O}_k$ admits *some* Euclidean function, and that k is *norm-Euclidean* if the field norm of k is a Euclidean function on $\mathcal{O}_k$.

It is pointed out in [Lenstra, 1977] (see the remark following (2.3)) that since the length of a unit clique gives a lower bound on the norm of any ideal, classical considerations show that if the unit clique is large enough to prove the field is norm-Euclidean, then one already knows that the class number must be one. However, the added flexibility of Lenstra-Hurwitz cliques means that they can be much larger than the minimal ideal norm, in fact, up to around the square of that norm. We shall give examples in §3 and §3.1 to show that there are fields with a Lenstra-Hurwitz clique sufficiently large to deduce class number one, even though there is no unit clique of the type required by [Lenstra, 1977].

We also remark that condition (ii) has appeared in other places in the literature, *e.g.* [Motzkin, 1949], [Harper, 2004], in connexion with the search for conditions under which k being Euclidean is equivalent to k having class number one.

In the absence of standard notation, we refer to an element $\rho \in \mathcal{O}_k$ for which $\langle \rho \rangle$ is a prime ideal and $\mathcal{O}_k^* \to (\mathcal{O}_k/\langle \rho \rangle)^*$ is a surjection as a *Lenstra-Hurwitz prime.* We also call an ideal generated by such ρ a *Lenstra-Hurwitz prime ideal.*

In particular, one can apparently conjecture that $\mathcal{O}_k$ always contains infinitely many Lenstra-Hurwitz prime ideals [Murty & Petersen, 2013], and various authors have proved this under certain hypotheses. For example [Murty & Petersen, 2013] shows that (with certain conditions on the number field k), Lenstra-Hurwitz primes are plentiful in the sense that the number of Lenstra-Hurwitz prime ideals with norm $\leq x$ is $>> x/(log(x))^2$.

Theorem 1.1 shows that sufficiently large geometric configurations of Lenstra-Hurwitz primes suffice to show that $\mathcal{O}_k$ *is* a PID. Perhaps surprisingly, computer

searches suggest such configurations are rather abundant. For example, there is a unique totally real sextic field with discriminant $5^3 \cdot 7^4 = 300125$, for which Lenstra's constant is around 8.45. The biggest known unit clique for this field has size 18, see 3.1; however, we found a Lenstra-Hurwitz clique of size 200. (Even so, this clique seems unlikely to be maximal.)

The method of proof of 1.1 is to exploit the well known criterion coming from the action of $SL(2,\mathcal{O}_k)$ on the k-points of $\mathbb{CP}^1$ by fractional linear transformations:

Proposition 1.2 *k has class number one if and only if for each $\xi \in k$ there is an $A \in \mathrm{SL}(2,\mathcal{O}_k)$ with $A \cdot \xi = \infty$.*

Our strategy is to show that the existence of a Lenstra-Hurwitz clique with at least $M(k)$ elements enables the construction of a subgroup G of $SL(2,\mathcal{O}_k)$ with the property that for each $\xi \in k$ there exists $A \in G$ with $A \cdot \xi = \infty$. Such a subgroup we call *totally cusped*. To the authors' knowledge, this is the first use of 1.2 to establish class number one for non-arithmetic examples. This strategy is implemented in §2, cumulating in Theorem 2.5.

In §3 we exhibit some examples of fields containing Lenstra-Hurwitz cliques sufficient to prove class number one. Further, we do some asymptotic analysis of our method which contrasts sharply with that of [Lenstra, 1977]; Lenstra shows that his method cannot be used to exhibit infinitely many Euclidean fields. However, our cliques are much larger and potentially there are infinitely many fields containing Lenstra-Hurwitz cliques sufficiently large to prove class number one.

Throughout this article, for a field element ξ, $N(\xi)$ will denote the *absolute value* of the field norm of ξ.

2 A Construction

At the heart of the proof of 1.1 lies a beautiful theorem (also used by Lenstra), due to Hurwitz:

Theorem 2.1 *Let K be a number field with norm $N(\,.\,)$ and let $\mathcal{O}$ be its ring of integers.*

Then there is a rational integer $M > 1$ with the property that for each $\xi \in K$, one can find a $\tau \in \mathcal{O}$ and a rational integer $0 < j < M$ for which

$$N(j\xi - \tau) < 1 \quad .$$

Proof The set of field elements with norm < 1 is relatively open (in the topology coming from embedding k into $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ in the canonical way), so we may choose an open neighbourhood of 0, U, say, so that all the elements of $U - U$ have norm less than 1. Using the volume form on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, let M be an integer larger than the ratio volume($\mathcal{P}$)/volume(U) (one can do a good deal better), where $\mathcal{P}$ is a fundamental parallelogram.

Given any element $\xi \in k$ and $0 < r < M$, consider the set $(r\xi + U)^*$, where the star operation $\mathcal{O}$-translates points outside $\mathcal{P}$ to the inside of $\mathcal{P}$. Notice that $(r\xi + U) \to (r\xi + U)^*$ is injective, since if two points ended at the same place, there would be integers τ_1 and τ_2 and $u_1, u_2 \in U$ for which $r\xi + \tau_1 + u_1 = r\xi + \tau_2 + u_2$, so that $\tau_1 - \tau_2 = u_2 - u_1$. The right hand side of this equality has norm < 1 and this can only happen for the integer 0, so $\tau_1 = \tau_2$ and $u_1 = u_2$. It follows volume($(r\xi + U)^*$) = volume(U), and therefore our choice of M implies that there must be values $0 < s < r < M$ so that $(r\xi + U)^* \cap (s\xi + U)^* \neq \emptyset$. This gives

$$r\xi + \tau_1 + u_1 = s\xi + \tau_2 + u_2$$

and therefore, taking $\tau = \tau_2 - \tau_1$, we see that $(r - s)\xi - \tau = u_2 - u_1$ has norm < 1 as required. □

Remark This idea is exploited by Lenstra, who notes that one may replace $\{1, \ldots, M\}$ in this argument by any set of integers $\{\alpha_1, \ldots, \alpha_M\}$. Then, provided the differences are all units, one can recover the condition the field be Euclidean using the fact

$$1 \;>\; N((\alpha_i - \alpha_j)\,\xi - \tau) \;=\; N(\xi - \tau(\alpha_i - \alpha_j)^{-1}) \;.$$

He also uses ideas from packing theory to improve the bound for M.

Our variation of 2.1 is the following theorem:

Theorem 2.2 *In the notation of 1.1, suppose that k has a Lenstra-Hurwitz clique with more than $M(k)$ elements.*

Then there is finite set of $\mathcal{O}_k$-units $\{\omega_1, \ldots, \omega_T\}$ with the property:

Given any element $\xi \in k$, there is an integer $\tau' \in \mathcal{O}_k$ such that either

$$N(\xi - \tau') < 1$$

or

$$N(\delta\alpha_{ij}\,(\xi - \tau') - \omega_t) < 1$$

for some difference $\delta\alpha_{ij}$ and some $1 \leq t \leq T$.

Proof Given $\xi \in k$, exactly as in the Lenstra version of the Hurwitz argument, we can find a difference $\delta\alpha_{ij}$ and an integer τ so that $N(\delta\alpha_{ij}\,\xi - \tau) < 1$. If $\delta\alpha_{ij}$ is a unit, then this gives $N(\xi - \tau(\delta\alpha_{ij})^{-1}) < 1$, this is the first case of the conclusion.

If not, we have a map to a finite field $\pi : \mathcal{O}_k \to \mathcal{O}_k/\langle\delta\alpha_{ij}\rangle = \mathcal{F}$. There are now two cases. Firstly, suppose that $\pi(\tau)$ is 0, that is, $\tau = \delta\alpha_{ij}\,\tau'$ for some $\tau' \in \mathcal{O}_k$. Then we have

$$1 \;>\; N(\delta\alpha_{ij}\,\xi - \tau) \;=\; N(\delta\alpha_{ij}\,\xi - \delta\alpha_{ij}\,\tau') \;=\; N(\delta\alpha_{ij})N(\xi - \tau') \;.$$

Since $\delta\alpha_{ij}$ is a nonzero integer its norm is at least 1, so that

$$N(\xi - \tau') < 1$$

also as required by the first case.

Finally, if $\pi(\tau)$ is not 0, by condition (ii) we have that $\pi(\tau) = \pi(\omega)$ for some unit ω. It follows that $\tau = \omega + \delta\alpha_{ij}\,\tau'$ for some $\tau' \in \mathcal{O}_k$. We now rewrite:

$$1 \;>\; N(\delta\alpha_{ij}\,\xi - \tau) \;=\; N(\delta\alpha_{ij}\,(\xi - \tau') - (\tau - \delta\alpha_{ij}\,\tau')) \;=\; N(\delta\alpha_{ij}\,(\xi - \tau') - \omega) \;.$$

The finite list of units $\{\omega_1, \ldots, \omega_T\}$ is provided by choosing a transversal of units for each of the homomorphisms $\mathcal{O}_k \to \mathcal{O}_k/ < \delta\alpha_{ij} >$ and taking the union of this collection.

This completes the proof. □

Remark We note that there is a good deal of flexibility in the choice of the units $\{\omega_1, \ldots, \omega_T\}$ since they need satisfy only the weak restriction that they are a union of transversals for some prescribed finite collection of finite homomorphisms $\mathcal{O}_k^* \to \mathcal{F}^*$. In particular, with a view to applying Theorem 2.4 below, we can (and do) choose the units so that all the elements of the form $\delta\alpha_{ij}\,(\omega_k)^{-1}$ satisfy $|\delta\alpha_{ij}\,(\omega_k)^{-1} + 2| > 2$.

Our basic tool for showing that $\mathcal{O}_k$ has class number one is the following. For the readers' convenience, we include the elementary proof.

Proposition 2.3 *k has class number one if and only if for each $\xi \in k$ there is an $A \in \mathrm{SL}(2, \mathcal{O}_\mathrm{k})$ with $A \cdot \xi = \infty$.*

Proof Suppose that k has class number one, *i.e.* $\mathcal{O}_k$ is a principal ideal domain. Let $\xi \in k$ be written $\frac{\alpha}{\beta}$ with $\alpha, \beta \in \mathcal{O}_k$, and let $\gamma \in \mathcal{O}_k$ generate the ideal $\langle \alpha\,,\, \beta \rangle$. Then we have $\gamma = \lambda\alpha + \mu\beta$, $\alpha = \rho\gamma$, $\beta = \sigma\gamma$ for some $\lambda, \mu, \rho, \sigma \in \mathcal{O}_k$. Substituting the

last two equations into the first and cancelling γ, we obtain $\lambda\rho + \mu\sigma = 1$. Then the matrix $\begin{bmatrix} \lambda & \mu \\ -\sigma & \rho \end{bmatrix}$ lies in $\mathrm{SL}(2,\mathcal{O}_\mathrm{k})$ and throws $\frac{\alpha}{\beta}$ to ∞.

Conversely, suppose that for each $\xi \in k$ there exists $A \in \mathrm{SL}(2,\mathcal{O}_\mathrm{k}))$ with $A\cdot\xi = \infty$. Let $\mathcal{I}$ be a non-zero ideal of $\mathcal{O}_k$. Since $\mathcal{O}_k$ is a Dedekind domain, $\mathcal{I}$ may be generated by two elements, say α, β [Fröhlich and Taylor, 1993]. From the hypothesis there exists $A \in \mathrm{SL}(2,\mathcal{O}_\mathrm{k})$ sending $(\alpha\,,\,\beta)$ to $(\gamma\,,\,0)$ for some (non-zero) $\gamma \in \mathcal{O}_k$, and from the mechanics of the matrix product γ is an $\mathcal{O}_k$–linear combination of α, β. But A^{-1} sending $(\gamma\,,\,0)$ to $(\alpha\,,\,\beta)$ shows that each of α, β is an $\mathcal{O}_k$– multiple of γ. Therefore $\mathcal{I} = \langle\alpha\,,\,\beta\rangle = \langle\gamma\rangle$, i.e. every ideal is principal. □

We construct a totally cusped subgroup of $\mathrm{SL}(2,\mathcal{O}_\mathrm{k})$ from the existence of a sufficiently large Lenstra-Hurwicz clique; there are two steps, the first being to construct a certain Schottky group. The proof of 2.4 involves slightly fewer words if we assume the field k is real, and henceforth we assume this. No new ideas are involved in the non-real case.

Theorem 2.4 *Suppose that $\beta_1, \ldots, \beta_r$ is a a collection of integers of k for which $|\beta_j + 2| > 2$ $(1 \le j \le r)$. Then there exist elements $\gamma_1, \ldots \gamma_r$ of a Schottky group $\Gamma \subset \mathrm{SL}(2,\mathcal{O}_\mathrm{k})$ and rational integers $t_1, \ldots t_r$, such that*

$$\gamma_j \cdot (t_j + 1/\beta_j) \;=\; \infty \quad (1 \le j \le r)\ .$$

Remark The proof of Theorem 1.1 does not depend on the group Γ in the statement of Theorem 2.4 being a Schottky group; however, this condition on Γ can be achieved with very little effort, and it seems desirable to remain in the realm of discrete subgroups of $\mathrm{SL}(2,\mathcal{O}_\mathrm{k})$ as long as possible.

Proof The fractional linear transformation defined by the matrix

$$\eta_j \;=\; \begin{bmatrix} -(\beta_j + 1) & 1 \\ \beta_j & -1 \end{bmatrix}$$

lies in $\mathrm{SL}(2,\mathcal{O}_\mathrm{k})$ and carries $1/\beta_j$ to ∞. It is a hyperbolic element, since it has trace equal to $-(\beta_j + 2)$, presumed larger than 2 in absolute value. Furthermore, neither endpoint of its axis is ∞. Since conjugation of η_j by a parabolic $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ has the effect of translating the axis of η_j horizontally through Euclidean distance a in the upper-half plane, we may choose $t_j \in \mathbb{Z}$ so that the axes of the hyperbolics

$$\gamma_j \;=\; \begin{bmatrix} 1 & t_j \\ 0 & 1 \end{bmatrix} \cdot \eta_j \cdot \begin{bmatrix} 1 & -t_j \\ 0 & 1 \end{bmatrix}$$

are distant from one another, thus guaranteeing the Schottky behaviour; note also that $\gamma_j \cdot (t_j + 1/\beta_j) = \infty$, as required. □

The group we ultimately construct will begin with a Schottky group of the type just constructed, with the β_j's carefully chosen with guidance from the given clique. The key will be showing that this group, augmented by the translational subgroup, is totally cusped. We now explain how this is achieved.

2.1 A reduction procedure.

For the present discussion, we assume that α, β are fixed integers of k, that P, Q are variable integers of k, and that $A = \begin{bmatrix} a & b \\ r & s \end{bmatrix}$ is a matrix in $\mathrm{SL}(2, \mathcal{O}_k)$.

Recall that A acts as a fractional linear transformation on a fraction p/q by the rule

$$A \cdot \frac{p}{q} = \frac{ap + bq}{rp + sq} ,$$

and that ∞ is represented by any fraction p/q with $p \neq 0$, $q = 0$.

Let us suppose that A throws the field element α/β to infinity; then, together with the determinant condition on A, we have

$$\begin{aligned} r\alpha + s\beta &= 0 \\ as - br &= 1 \end{aligned}$$

We then have the identities

$$\begin{aligned} r(a\alpha + b\beta) &= -as\beta + br\beta = -\beta \\ s(a\alpha + b\beta) &= as\alpha - br\alpha = \alpha \end{aligned}$$

Therefore, if we multiply numerator and denominator of the formal expression

$$\frac{aP + bQ}{rP + sQ}$$

by the integer $-(a\alpha + b\beta)$, and recalling that P and Q are integers, we obtain an expression for $A \cdot (P/Q)$ as the quotient of two integers where the denominator is $\beta P - \alpha Q$.

We exploit this as follows. Suppose that we are given $x = p/q$, and that there happen to be integers α, β (for example, as given by the Hurwitz-type arguments) satisfying

$$N(\beta x - \alpha) = N(\beta(p/q) - \alpha) < 1 ,$$

or equivalently

$$N(\beta p - \alpha q) \ < \ N(q) \ .$$

Suppose further that we are given a matrix $A \in \mathrm{SL}(2, \mathcal{O}_k)$ for which $A \cdot (\alpha/\beta) = \infty$. Applying the above computation, we see that $A \cdot (p/q)$ has an expression as the quotient of two integers where the denominator has norm $N(p\beta - q\alpha)$, strictly less than the norm of the denominator q of x (in fact there might be cancellations making this norm smaller, but this is the worst it could be). This is the reduction procedure that we sought.

Definition Fix some field k, equipped with a Lenstra-Hurwitz clique Σ.

We say that a subgroup G of $\mathrm{SL}(2, \mathcal{O}_k)$ *satisfies the Lenstra-Hurwitz condition for* Σ if for each of the elements $\omega_t/\delta\alpha_{ij}$ coming from the clique, there is an integer $\tau_{i,j,t} \in \mathcal{O}_k$ and an element $\gamma_{i,j,t} \in G$ so that

$$\gamma_{i,j,t} \cdot (\omega_t/\delta\alpha_{ij} + \tau_{i,j,t}) \ = \ \infty \ .$$

Definition Let G be a subgroup of $\mathrm{SL}(2, \mathcal{O}_k)$. The *augmented group* G^A is the group generated by G together with (i) all translations coming from $\mathcal{O}_k$, *i.e.* all elements of the form $\begin{bmatrix} 1 & \tau \\ 0 & 1 \end{bmatrix}$ for $\tau \in \mathcal{O}_k$, and (ii) the element $\eta = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

Notice that even if G is discrete, its augmented group almost never is. We claim:

Theorem 2.5 *Suppose that k has a Lenstra-Hurwitz clique with at least $M(k)$ elements. Then:*

(i) There is a Schottky group $G < \mathrm{SL}(2, \mathcal{O}_k)$ satisfying the Lenstra-Hurwitz condition.

(ii) The augmented group G^A is a totally cusped subgroup of $\mathrm{SL}(2, \mathcal{O}_k)$.

(iii) The field k has class number one.

Proof (iii) follows from (ii) immediately, from the classical criterion of Proposition 2.3.

By hypothesis, we have a sufficiently large Lenstra-Hurwitz clique that we may apply Theorem 2.2. Using the elements provided by that result, we may construct a Schottky group G from Theorem 2.4 with the integers $\beta_{i,j,t} = (\delta\alpha_{ij} \ . \ \omega_t^{-1})$. (As in the remark following Theorem 2.4, all of these integers satisfy $|\beta_{i,j,t} + 2| > 2$.)

The Schottky group G maps all elements $1/\beta_{i,j,t} + \tau_{i,j,t}$ to ∞, so G satisfies the Lenstra-Hurwitz condition for the given clique. This proves (i).

The strategy for proving (ii) is to show that given any field element, we can use a translation in the augmented group together with the Lenstra-Hurwitz condition to reduce the norm of its denominator. (This isn't quite well defined, but we can begin with any representation of the given field element as a quotient of integers α/β, and apply a sequence of moves which reduces denominator norms. For example, we may reduce $\min\{N(\beta)\}$ over all such expressions α/β for the field element.) This shows any element of the field can be moved to an integer. In G^A, all integers are all equivalent to 0, and hence by application of η, to ∞. This will show that G^A is totally cusped. The details now follow:

Fix any element $\xi \in k$. By Theorem 2.2, the clique gives an integer τ' so that either

$$N(\xi - \tau') \ < \ 1$$

or

$$N(\delta\alpha_{ij}(\xi - \tau') - \omega_t) \ < \ 1 \ .$$

Notice that ξ and $\xi - \tau'$ differ by integral translation, so that one is a cusp of G^A if and only if the other one is, and moreover they have the same denominator; therefore it suffices to work with $\xi' = \xi - \tau'$.

Elements ξ' of the first type have their denominators reduced by application of η.

For elements ξ' of the second type we argue as follows. By (i), the group G contains sufficient elements to throw any of the finite collection of elements $\omega_t/\delta\alpha_{ij} + \tau_{i,j,t}$ to ∞; hence G^A contains elements throwing any $\omega_t/\delta\alpha_{ij}$ to ∞. Noting that $G \leq SL(2, \mathcal{O}_k)$ implies that G^A also is, the computation of §2.1 applies and shows that this group element reduces the denominator of $\xi - \tau'$. Repeating this procedure eventually reduces the denominator to an integer of norm 1. When this is achieved, we have shown that the original ξ is G^A-equivalent to an integer. All such are equivalent to ∞ in G^A, so that ξ is a cusp, as required. □

3 Examples & estimates for cliques.

We collect some facts about Lenstra-Hurwitz cliques and prime cliques, (i.e. those satisfying only condition (i) of Definition 1) and give some examples.

The definition of clique is translationally invariant, so we may assume the clique contains 0. Cliques encode some subtle questions about primes: for example, one sees

easily that a prime clique in $\mathbb{Z}$ contains at most four integers, and that there are up to translation precisely three cliques of size four. Any clique that does not contain 2 has size at most three, but unsolved nature of the twin primes conjecture means that it is currently unknown whether there are infinitely many distinct such cliques.

It is easily seen that the size of a unit clique is bounded above by the smallest norm of an ideal of $\mathcal{O}_k$. This fails for prime cliques, as evidenced by the clique below of length 7 in $k = \mathbb{Q}(\sqrt{173})$; every quadratic field has a prime ideal of norm at most 4, as either 2 is a prime (it is in this case) and has norm 4, or if not the prime factors of 2 will each have norm 2.

However, one can provide an upper bound on the size of a prime clique.

Theorem 3.1 *Suppose that $\mathcal{O}_k$ has largest unit clique with U elements and that the minimal norm of a principal ideal of $\mathcal{O}_k$ is L.*

Then a prime clique Σ of $\mathcal{O}_k$ contains at most $U.L$ elements.

Proof Let $\langle q \rangle$ be a principal ideal of R of smallest norm L, and let $\pi : R \to \mathcal{F} = R/\langle q \rangle$ be the natural map onto the quotient field. We shall show that for each $x \in \mathcal{F}$, $|\pi^{-1}(x) \cap \Sigma| \leq U$.

Let $x \in \mathcal{F}$, and let the non-zero elements of $\pi^{-1}(x) \cap \Sigma$ be σ_1 , σ_2 , $\ldots$. Then for each $i \neq j$ we have $\sigma_i - \sigma_j = q.\xi_{ij}$ for some $\xi_{ij} \in R$. Since a multiple of the prime q cannot be a unit, $\sigma_i - \sigma_j$ must be prime, and it follows that ξ_{ij} is a unit. Furthermore, if i , j , k are pairwise distinct, we have $(\sigma_i - \sigma_j) - (\sigma_i - \sigma_k) = \sigma_k - \sigma_j$, from which it follows that $\xi_{ij} - \xi_{ik} = \xi_{kj}$. Therefore all differences of pairs of elements of $\{0\,, \xi_{12}\,, \xi_{13}\,, \xi_{14}\,, \ldots\}$ are units, and we see that this set is a unit clique, by hypothesis of size at most U.

If $x \neq 0$, then all elements of $\pi^{-1}(x)$ are non-zero, and the argument of the previous paragraph shows directly that $|\pi^{-1}(x) \cap \Sigma| \leq U$.

For the case $x = 0$, we also have to consider that $\pi^{-1}(x)$ contains 0. However, for each i we now have $\sigma_i = q.\eta_i$ for some $\eta_i \in R$, and from the fact that $\sigma_i \neq 0$ we deduce that σ_i is prime and therefore that η_i is a unit. Moreover, $\eta_i - \eta_j = \xi_{ij}$, so we see that $\{0\,, \eta_1\,, \eta_2\,, \ldots\}$ is a unit clique. Therefore there are at most $U - 1$ elements σ_i, and we arrive at the conclusion $|\pi^{-1}(x) \cap \Sigma| \leq U$ as before. □

Corollary 3.1.1 *With the exception of $d = 5$, in a real quadratic field $\mathbf{Q}(\sqrt{d})$, a prime clique has at most 8 elements (in the case that 2 is prime) and at most 4 elements (in the case that 2 splits).*

Example 1. Using Lenstra's estimate (1.9) [Lenstra, 1977] for the field $k = \mathbb{Q}(\sqrt{173})$, one sees that exhibiting a clique with more than $M(k) = \frac{1}{2}\sqrt{173} \cong 6.58$ suffices to prove class number one. A computer search reveals the Lenstra-Hurwitz clique

$$\Sigma = \left\{0\,,\ \tfrac{1}{2}(-77+3\sqrt{173})\,,\ -25+2\sqrt{173}\,,\ -12+\sqrt{173}\,,\ 13-\sqrt{173}\,,\ \tfrac{1}{2}(27+\sqrt{173})\,,\ \tfrac{1}{2}(53-\sqrt{173})\right\}$$

of length 7. Thus $\mathbb{Q}(\sqrt{173})$ has class number equal to one. Notice that it is known that this field is not norm-Euclidean, so it is impossible for Lenstra's technique to work in this case. Indeed, the paucity of exceptional units in quadratic fields severely limits the possible size of their cliques.

In fact, $\mathbb{Q}(\sqrt{173})$ contains a prime clique of size 8, but it is unknown whether there is a Lenstra-Hurwitz clique of this size.

The field $\mathbb{Q}(\sqrt{5})$ does have exceptional units and the corollary does not apply. In fact one can check that this field has a Lenstra-Hurwitz clique of size 16:

$$\left\{0\,,\ 1\,,\ -1\,,\ -2\,,\ 1-\sqrt{5}\,,\ -1-\sqrt{5}\,,\ 2+\sqrt{5}\,,\ -2-\sqrt{5}\,,\ \tfrac{1}{2}(-1-\sqrt{5})\,,\ \tfrac{1}{2}(-3-\sqrt{5})\,,\right.$$
$$\left.\tfrac{1}{2}(3+\sqrt{5})\,,\ \tfrac{1}{2}(-3-3\sqrt{5})\,,\ \tfrac{1}{2}(-5-3\sqrt{5})\,,\ \tfrac{1}{2}(-5-\sqrt{5})\,,\ \tfrac{1}{2}(-7-3\sqrt{5})\,,\ \tfrac{1}{2}(-11-5\sqrt{5})\right\}$$

There is a unit clique of size 4, and 2 is prime, so this Lenstra-Hurwitz clique is in fact maximal.

Example 2. (Lenstra's "near miss"). In [Lenstra, 1977] (3.5), Lenstra does some analysis of the sextic field K of discriminant $5^3 \cdot 7^4 = 300125$. He computes the packing constant M in this case to be approximately 8.454, so for his method to apply he needs a unit clique with at least 9 elements.

He exhibits a unit clique with 8 elements, and observes that there is one further element that one could add which almost provides a unit clique of size 9: there is one difference which fails to be a unit. One can compute that this one failure is a prime γ of norm 29, and that the unit group of $\mathcal{O}_K$ does indeed surject the finite field $\mathcal{O}_K/ < \gamma >$. It follows there is a Lenstra-Hurwitz clique of length 9, and so the field has class number one. (In fact Lenstra subsequently uses a multiple packing constant argument to show the field is norm-Euclidean.) A computer search reveals that there is in fact a unit clique of size 18 for this field, large enough to establish that the field is norm-Euclidean. Furthermore, it transpires that there is a much larger Lenstra-Hurwitz clique, of length 200.

We can go further and do some asymptotic analysis in the spirit of [Lenstra, 1977]. As observed in §2 of *loc. cit* , in a number field of degree n, a unit clique has at most 2^n elements, the reason being that either 2 is prime and has norm 2^n, or else the prime

factors of 2 have smaller norm. Therefore, by Theorem 3.1, a prime clique has at most 2^{2n} elements.

It is a classical result that there are only finitely many number fields of given discriminant, and Lenstra's constants $M(k)$ tend to ∞ for fixed n and as $\Delta \to \infty$, and thus Theorem 1.1 will only apply finitely often for any given n.

However, it is interesting to observe a divergence between Lenstra's more subtle observations in §2 and the prime clique estimate at this point. Since for $n >> 0$, (1.12) of [Lenstra, 1977] is sharper than (1.9), the relevant constant here is

$$M(k) \;=\; \sigma_n \cdot \frac{\Gamma(1+n/2)}{\pi^{n/2}} \cdot \left(\frac{4}{n}\right)^{n/2} \cdot |\Delta|^{1/2} \;\;,$$

and to have any hope we need at least $2^{2n} > M(k)$, yielding

$$|\Delta| \;<\; \frac{\pi^n n^n 4^n}{\Gamma(1+n/2)^2 \sigma_n^2} \;\;,$$

giving the estimate (see §2 of [Lenstra, 1977])

$$|\Delta|^{1/n} \;<\; 16\pi e + o(1) \;\;.$$

This is to be contrasted with the constant $4\pi e$ given in [Lenstra, 1977]. In particular, Serre's estimate using GRH gives that $|\Delta|^{1/n} > 8\pi e^{\gamma} + o(1)$ (here γ is Euler's constant), and since $4\pi e < 8\pi e^{\gamma}$, Lenstra deduces that his method fails uniformly for sufficiently large n. However, prime cliques are potentially better behaved since $16\pi e > 8\pi e^{\gamma}$.

Incorporating the Lenstra-Hurwitz condition (*ii*) into the analysis seems a good deal more delicate; the question of whether a given prime is Lenstra-Hurwitz or not is bound up with deep issues related (at least in part) to the Artin Conjecture. However, one can show some primes do *not* satisfy this condition:

Theorem 3.2 *Let p be a rational prime, not 2 or 3, which remains inert in K.*

Then p is not a Lenstra-Hurwitz prime in $\mathcal{O}_K$.

Proof. Suppose K has degree n over $\mathbb{Q}$, so that $\mathcal{O}_K/\langle p\rangle$ is a finite field with p^n elements. In order for p to be Lenstra-Hurwitz, we must exhibit a unit with order $p^n - 1$. We claim no such unit exists.

Take a unit u in $\mathcal{O}_K^*$. Let $f(X)$ be the minimal polynomial of u over $\mathbb{Q}$. There are two cases:

(a) Suppose that $f(X)$ factorizes modulo p, say into two factors, one of degree a and one of degree b, where $a+b=n$. Then by the Cayley-Hamilton theorem, the order of u modulo p is at most $LCM(p^a-1, p^b-1)$ which in turn is at most $(p^a-1)(p^b-1)/(p-1)$ since the factor $(p-1)$ occurs in both terms. This has order around $p^{a+b-1} = p^{n-1}$ and is less than p^n for $p \geq 3$.

(b) Suppose that $f(X)$ is irreducible modulo p. In this case it defines a degree n extension L over $\mathbb{Z}/p$. Now there is a norm map $N : L \to \mathbb{Z}/p$, which in this setting is the constant term of $f(X)$ up to sign. The fact that u is a unit means that $N(u)$ is ± 1 and thus u^2 is in the kernel of the map $N^* : L^* \to \mathbb{Z}/p^*$.

We claim that $ker(N^*)$ has size $(p^n-1)/(p-1)$. The reason is this: The extension L over $\mathbb{Z}/p$ is cyclic, so by Hilbert Satz 90, if σ generates the Galois group, then all the elements of norm 1 (i.e. $ker(N^*)$) have the form $a/\sigma(a)$. There is a map

$$L^* \to ker(N^*)$$

given by $a \to a/\sigma(a)$ which Hilbert's result implies is onto. The kernel of this map is the fixed field of σ, i.e. $\mathbb{Z}/p$. It follows that $ker(N^*)$ has size $(p^n-1)/(p-1)$.

This implies that u^2 has order dividing $(p^n-1)/(p-1)$, and therefore u has order dividing $2(p^n-1)/(p-1)$. This is less than p^n-1 for $p \neq 2, 3$. □

3.1 Tables

Below are given four examples where $U = L$ and the theoretical maximum length $U.L$ is attained by the given Lenstra-Hurwitz clique. In these examples, Lenstra's unit clique method cannot work, L being smaller than the packing constant $M = (n!/n^n)\,|\Delta|^{1/2}$ of [Lenstra, 1977]; however, since $U.L > M$, the fields are class number one as a result of Theorem 1.1.

Coordinates of elements of $\mathcal{O}(k)$ are given with respect to the basis $\{1\,,\,\zeta\,,\,\zeta^2\,,\,\ldots\,,\,\zeta^{n-1}\}$, where ζ is a root of the defining polynomial, and n is its degree.

$p(x) = x^3 - x^2 - 4x + 3$

$\Delta = 257\ ,\ \ U = L = 3\ ,\ \ M = 3.56$

$$\begin{array}{(rrr)}
5, & -2, & -1 \\
5, & -1, & -2 \\
5, & 0, & -2 \\
4, & 1, & -2 \\
4, & -1, & -1 \\
4, & 0, & -1 \\
3, & 1, & -1 \\
3, & 0, & -1 \\
0, & 0, & 0
\end{array}$$

$p(x) = x^4 - 4x^2 - x + 1$

$\Delta = 1957\ ,\ \ U = L = 3\ ,\ \ M = 4.15$

$$\begin{array}{(rrrr)}
7, & -4, & -31, & -15 \\
0, & 7, & 2, & -2 \\
-2, & 3, & 1, & -1 \\
-1, & 1, & 1, & 0 \\
0, & 11, & 1, & -3 \\
0, & 1, & -3, & -2 \\
2, & 1, & 0, & 0 \\
-1, & 0, & 2, & 1 \\
0, & 0, & 0, & 0
\end{array}$$

$p(x) = x^5 - 5x^3 - x^2 + 3x + 1$

$\Delta = 24217\ ,\ \ U = L = 5\ ,\ \ M = 5.98$

$$\begin{array}{(rrrrr)}
1, & 0, & -9, & 0, & 2 \\
9, & 1, & -19, & -1, & 4 \\
-3, & -1, & 6, & 0, & -1 \\
1, & 7, & -4, & -2, & 1 \\
2, & 7, & -4, & -2, & 1 \\
-5, & -6, & 9, & 2, & -2 \\
-7, & -2, & 19, & 1, & -4 \\
-6, & -3, & 14, & 1, & -3 \\
-6, & -9, & 1, & 2, & 0 \\
-2, & -4, & 0, & 1, & 0 \\
-1, & 1, & 9, & 0, & -2 \\
1, & 0, & -5, & 0, & 1 \\
-1, & 1, & 5, & 0, & -1 \\
-5, & -7, & 14, & 2, & -3 \\
-5, & -2, & 9, & 1, & -2 \\
4, & 2, & -14, & -1, & 3 \\
0, & 3, & -4, & -1, & 1 \\
1, & 4, & 0, & -1, & 0 \\
-3, & 0, & 1, & 0, & 0 \\
-3, & -4, & 5, & 1, & -1 \\
0, & 1, & 0, & 0, & 0 \\
3, & 3, & -9, & -1, & 2 \\
-2, & 1, & 9, & 0, & -2 \\
-2, & -3, & 9, & 1, & -2 \\
0, & 0, & 0, & 0, & 0
\end{array}$$

$p(x) = x^6 - x^5 - 5x^4 + 4x^3 + 5x^2 - 2x - 1$

$\Delta = 592661\ ,\ \ U = L = 7\ ,\ \ M = 11.88$

$$\begin{array}{(rrrrrr)}
12, & -4, & -14, & 9, & 3, & -2 \\
14, & -10, & -18, & 14, & 4, & -3 \\
12, & -8, & -21, & 14, & 5, & -3 \\
12, & -12, & -20, & 18, & 5, & -4 \\
11, & -11, & -17, & 18, & 4, & -4 \\
13, & -10, & -21, & 18, & 5, & -4 \\
13, & -6, & -18, & 13, & 4, & -3 \\
13, & -10, & -21, & 14, & 5, & -3 \\
13, & -8, & -22, & 14, & 5, & -3 \\
13, & -8, & -21, & 14, & 5, & -3 \\
13, & -10, & -18, & 14, & 4, & -3 \\
14, & -7, & -21, & 13, & 5, & -3 \\
11, & -6, & -20, & 13, & 5, & -3 \\
12, & -8, & -20, & 13, & 5, & -3 \\
12, & -10, & -17, & 18, & 4, & -4 \\
12, & -9, & -18, & 14, & 4, & -3 \\
13, & -10, & -22, & 14, & 5, & -3 \\
16, & -7, & -22, & 13, & 5, & -3 \\
13, & -2, & -18, & 8, & 4, & -2 \\
10, & -8, & -14, & 13, & 3, & -3 \\
14, & -11, & -22, & 18, & 5, & -4 \\
12, & -11, & -21, & 14, & 5, & -3 \\
12, & -8, & -18, & 13, & 4, & -3 \\
12, & -10, & -21, & 14, & 5, & -3 \\
10, & -7, & -16, & 10, & 4, & -2 \\
11, & -5, & -18, & 9, & 4, & -2 \\
10, & -9, & -14, & 14, & 3, & -3 \\
12, & -5, & -18, & 9, & 4, & -2 \\
11, & -9, & -17, & 14, & 4, & -3 \\
13, & -12, & -21, & 18, & 5, & -4 \\
14, & -2, & -18, & 8, & 4, & -2 \\
11, & -6, & -17, & 13, & 4, & -3 \\
10, & -5, & -17, & 9, & 4, & -2 \\
12, & -9, & -20, & 14, & 5, & -3 \\
15, & -11, & -25, & 18, & 6, & -4 \\
11, & -6, & -17, & 9, & 4, & -2 \\
14, & -7, & -22, & 13, & 5, & -3 \\
12, & -8, & -18, & 14, & 4, & -3 \\
11, & -8, & -17, & 13, & 4, & -3 \\
12, & -7, & -18, & 13, & 4, & -3 \\
10, & -5, & -14, & 9, & 3, & -2 \\
10, & -6, & -13, & 9, & 3, & -2 \\
12, & -4, & -17, & 9, & 4, & -2 \\
10, & -9, & -17, & 14, & 4, & -3 \\
12, & -4, & -18, & 9, & 4, & -2 \\
13, & -5, & -18, & 9, & 4, & -2 \\
12, & -7, & -21, & 13, & 5, & -3 \\
12, & -3, & -17, & 8, & 4, & -2 \\
0, & 0, & 0, & 0, & 0, & 0
\end{array}$$

We conclude with a listing of the unit clique of size 18 for Lenstra's "near miss" sextic example. The field is $\mathbb{Q}(u,v)$, where $u = e^{2\pi i/5} + e^{-2\pi i/5}$, $v = e^{2\pi i/7} + e^{-2\pi i/7}$. Taking coordinates with respect to the basis $\{1\,,\,u\,,\,v\,,\,uv\,,\,v^2\,,\,uv^2\}$, the elements of the clique are

(2, −1, 0, −1, −2, 1)	(2, 0, 2, 1, 0, 1)
(−1, −2, −2, −1, −1, 0)	(0, 1, −1, −1, −1, −1)
(1, −2, 0, −2, −2, 2)	(1, 0, −1, −1, −1, 0)
(0, −1, −2, −1, 1, 1)	(1, 0, −1, 1, 0, −1)
(3, −2, 0, 1, −1, 1)	(1, −2, 0, 0, −1, 1)
(1, 0, 1, 1, 0, 0)	(2, 0, 0, 0, −1, 0)
(1, 0, 1, −1, −1, 1)	(2, 1, −1, 0, −1, −1)
(−1, 2, 0, −1, 0, −1)	(1, −1, −1, 0, −1, 0)
(1, −1, 0, 0, 0, 1)	(0, 0, 0, 0, 0, 0)

Experiments suggest that this clique might be maximal amongst unit cliques for this field; however, we have no reason to suppose that the Lenstra-Hurwitz clique of size 200 that we found is maximal.

4 Acknowledgments

The first author is partially supported by the National Science Foundation, and the second author is partially supported by the Simons Foundation.

References

[Fröhlich and Taylor, 1993] Fröhlich, A. and Taylor, M.J. (1993). Algebraic Number theory. *Cambridge Studies in Advanced Mathematics* 27, Cambridge University Press, 1993.

[Harper, 2004] Harper, M. (2004). $\mathbb{Z}[14]$ is Euclidean. *Canad. J. Math.*, 56 (1): 55–70.

[Lenstra, 1977] Lenstra, H.W. (1977). Euclidean number fields of large degree. *Inventiones Math.*, 38: 237–254.

[Motzkin, 1949] Motzkin, T. (1949). The Euclidean algorithm. *Bull. Amer. Math. Soc.*, 55: 1142–1146.

[Murty & Petersen, 2013] Murty, M.R. and Petersen, K.L. (2013). The Euclidean algorithm for number fields and primitive roots. *Proc. Amer. Math. Soc.*, 141: 181–190.

[Weinberger, 1973] Weinberger, P.J. (1973). On Euclidean rings of algebraic integers. *Proc. Symposia Pure Math. (AMS)*, 24: 321–332.

Department of Mathematics, University of California, Santa Barbara, CA 93106
Department of Mathematics, University of Tennessee, Knoxville, TN 37996
long@math.ucsb.edu, morwen@math.utk.edu
www.math.ucsb.edu/~long, www.math.utk.edu/~morwen