Reiter, C.
Osaka J. Math.
22 (1985), 755–765

EFFECTIVE LOWER BOUNDS ON LARGE FUNDAMENTAL UNITS OF REAL QUADRATIC FIELDS

CLIFFORD REITER

(Received October 5, 1984)

There is considerable interest in how large the fundamental units of real quadratic fields may be. For example, when factoring a rational integer using the Continued Fraction Method, see [2], one avoids expansions of quadratic surds in fields with too small a fundamental unit. More classically Gauss' conjecture that infinitely many real quadratic fields have class number one could be shown if fields with huge enough fundamental units were known.

In 1971 Yamamoto [4] gave classes of large fundamental units. It is well known that in real quadratic fields the class number and the logarithm of the fundamental unit are roughly inversely proportional. See Hua [1, p. 336] for a precise statement. Yamamoto's theorem, and ours, uses hypotheses about ideals being principal to imply lower bounds on fundamental units.

Let $\boldsymbol{N}$ denote the natural numbers and $\boldsymbol{Q}$ the rational numbers. For $d\in\boldsymbol{N}$ with $d>1$ and d not a square we write $\boldsymbol{Q}(\sqrt{d})$ for the quadratic field with discriminant $D=D_d$, fundamental unit $\varepsilon=\varepsilon_d$, class number $h=h_d$, and ring of integers $\mathcal{O}_d$. Yamamoto's theorem is:

Theorem 1.1 (Yamamoto). *Let $p_1, \cdots, p_n\in\boldsymbol{N}$ be primes. Let I be a set of infinitely many square-free positive integers. Suppose that for all $1\leq i\leq n$ and $d\in I$ that one has $(p_i)=\mathcal{P}_i\bar{\mathcal{P}}_i$, $gcd(p_i, d)=1$ and $\mathcal{P}_i$ principal in $\mathcal{O}_d$, then there is a constant c so that*

$$\log\varepsilon_d>c(\log d)^{n+1} \quad \textit{for } d\in I\,.$$

Yamamoto then gave a class of sets I with $n=2$. In this paper we will generalize his theorem so that it is effective. Since our theorem is not asymptotic there is no need for an infinite set I. The hypothesis that $p_1, \cdots, p_n$ be prime will be weakened. Furthermore, we will give many other classes of examples with $n=2$. That is, we will give many fields whose fundamental units are large in this sense. It should be remarked that these theorems fall far short of settling Gauss' conjecture.

1. Effective lower bounds on fundamental units

We give here several Lemmas that we will need. See Yamamoto [4]

and his references for proofs. He does not state the last lemmas; hence, we include proofs of these.

A quadratic irrational $\sigma=\frac{r+s\sqrt{d}}{t}$ is *reduced* if $\sigma>1$ and $\bar{\sigma}=\frac{r-s\sqrt{d}}{t}$ satisfies $-1<\bar{\sigma}<0$.

Lemma 1.1. *Let* $w=\frac{D+\sqrt{D}}{2}$ *where* D *is the discriminant of* $\boldsymbol{Q}(\sqrt{d})$. *Every ideal* $\mathcal{A}$ *of* $\mathcal{O}_d$ *has the unique canonical form* $\mathcal{A}=a\boldsymbol{Z}+(b+cw)\boldsymbol{Z}$ *with* a, b, c, $d\in\boldsymbol{Z}$ *satisfying*: (i) $a, c>0$ (ii) $ac=N(\mathcal{A})$ (iii) $a\equiv b\equiv 0 \pmod{c}$ (iv) $N(b+cw)\equiv 0 \pmod{ac}$ (v) $-a<b+c\overline{w}<0$.

For such $\mathcal{A}=a\boldsymbol{Z}+(b+cw)\boldsymbol{Z}$ we define the map $\alpha(\mathcal{A})=\frac{b+cw}{a}$. $\mathcal{A}$ is called a *reduced ideal* if $c=1$ and $\alpha(\mathcal{A})$ is a reduced quadratic irrational.

Lemma 1.2. *The above map* $\mathcal{A}\mapsto\alpha(\mathcal{A})$ *gives a bijection of the set of all reduced ideals to the set* A *of reduced quadratic irrationals with discriminant* D. *It induces a bijection of the ideal class group of* $\boldsymbol{Q}(\sqrt{d})$ *to the set* $\{A_1, A_2, \cdots, A_{h_d}\}$ *of the equivalence classes of* A.

Lemma 1.3. *If an ideal* $\mathcal{A}$ *satisfies* $N(\mathcal{A})<\frac{\sqrt{D}}{2}$ *and* $gcd(\mathcal{A}, \overline{\mathcal{A}})=1$ *where* $\overline{\mathcal{A}}$ *is the conjugate ideal to* $\mathcal{A}$, *then* $\mathcal{A}$ *is reduced.*

Next, we need the following integral:

Lemma 1.4. $$\underset{\substack{x_1+\cdots+x_n\le b\\ x_i\ge 0}}{\int\cdots\int}(x_1+x_2+\cdots+x_n)^k\,dx_1\cdots dx_n=\frac{b^{k+n}}{(n-1)!\,(k+n)}$$

Now letting $x_i=c_iz_i$ we get the following easy corollary of Lemma 1.4.

Lemma 1.5. $$\underset{\substack{c_1z_1+\cdots+c_nz_n\le b\\ z_i\ge 0}}{\int\cdots\int}(c_1z_1+\cdots+c_nz_n)^k dz_1\cdots dz_n=\frac{b^{k+n}}{c_1\cdots c_n(n-1)!\,(n+k)}$$

We want to replace the primality of $p_1, \cdots, p_n$ in Yamamoto's theorem by the following notion.

DEFINITION 1.6. $a_1, \cdots, a_n\in\boldsymbol{Q}$ are said to be *quadratically independent* provided

$$|\boldsymbol{Q}(\sqrt{|a_1|}, \sqrt{|a_2|}, \cdots, \sqrt{|a_n|}): \boldsymbol{Q}|=2^n.$$

Now we can get a theorem giving effective lower bounds on some fundamental units.

Theorem 1.7. *Let the quadratic number field* $\boldsymbol{Q}(\sqrt{d})$ *have discriminant* D *and fundamental unit* ε. *Suppose* $a_1, \cdots, a_n\in\boldsymbol{N}$ *are quadratically independent*

with $(a_i)=\mathcal{A}_i\bar{\mathcal{A}}_i$ *where* $\mathcal{A}_i$ *is principal and* $gcd(\mathcal{A}_i, \bar{\mathcal{A}}_j)=1$ *for* $1\leq i,j\leq n$. *Then*

$$\log \varepsilon > \frac{1}{2P(n+1)!}\left(\log \frac{\sqrt{D}}{2}\right)^{n+1}$$

provided $\log \frac{\sqrt{D}}{2} > \max\{Q^2, 4en(n+1)Q+2\}$ *where* $P=\log a_1 \cdots \log a_n$, $Q=\sqrt{n}\sqrt{(\log a_1)^2+\cdots+(\log a_n)^2}$ *and e is the base of the natural logarithm.*

Proof. Consider the ideals of the form $\mathcal{B}=\prod_{i=1}^{n}\mathcal{A}_i^{e_i}$; since $gcd(\mathcal{A}_i, \bar{\mathcal{A}}_j)=1$ we can apply Lemma 1.3. Therefore, such a $\mathcal{B}$ is reduced provided $N(\mathcal{B})<\frac{\sqrt{D}}{2}$. Denote these principal, reduced ideals by $\mathcal{B}_1, \cdots, \mathcal{B}_t$. As before, $\varepsilon=\prod \alpha(\mathcal{B}) > \prod_{i=1}^{t}\alpha(\mathcal{B}_i) > \left(\frac{\sqrt{D}}{2}\right)^t \prod_{j=1}^{t}\frac{1}{a_1^{e_1}\cdots a_n^{e_n}}$ where the first product is over $\mathcal{B}$ principal and reduced. Notice that the e_i's depend on j. Let $L=\log\frac{\sqrt{D}}{2}$. So,

$$t = \operatorname{card}\{(e_1, \cdots, e_n): e_1 \log a_1+\cdots+e_n \log a_n<L\} \geq \int \cdots \int dx_1\cdots dx_n$$

where the integral is for $x_i\geq 0$ with $x_1 \log a_1+\cdots+x_n \log a_n<L-Q$. Notice that Q was chosen to move the hyperplane inward the distance of the length of the diagonal of the n-dimensional cube. This ensures that the integral underestimates the number of lattice points. By Lemma 1.5 we see that

$$t\geq \frac{1}{P}\frac{(L-Q)^n}{n!}.$$

Likewise,

$$S = \log\left(\prod_{j=1}^{t} a_1^{e_1}\cdots a_n^{e_n}\right) = \Sigma(e_1 \log a_1+\cdots+e_n \log a_n)$$

where the sum is over the positive integers $e_1, \cdots, e_n$ with $e_1 \log a_1+\cdots+e_n \log a_n<L$. Then we see:

$$S<\int \cdots \int (x_1 \log a_1+\cdots+x_n \log a_n)\, dx_1\cdots dx_n$$

where the integral is over $x_i\geq 0$ with

$$x_1 \log a_1+\cdots+x_n \log a_n<L+Q$$

Therefore,

$$S<\frac{1}{P}\frac{(L+Q)^{n+1}}{(n-1)!\,(n+1)}.$$

Combining these yields:

$$\begin{aligned}\log \varepsilon &> tL-S\\ &> \frac{L}{P}\frac{(L-Q)^n}{n!}-\frac{1}{P}\frac{(L+Q)^{n+1}}{(n-1)!\,(n+1)}\\ &= \frac{1}{P(n-1)!}\left[\frac{1}{n}\sum_{k=0}^{n}\binom{n}{k}L^{k+1}(-Q)^{n-k}-\frac{1}{(n+1)}\sum_{k=0}^{n+1}L^k\,Q^{n+1-k}\binom{n+1}{k}\right]\\ &= \frac{1}{P(n-1)!}\left\{\sum_{k=0}^{n}\left[\frac{1}{n}\binom{n}{k}(-1)^{n-k}-\frac{1}{(n+1)}\binom{n+1}{k+1}\right]L^{k+1}\,Q^{n-k}-\frac{Q^{n+1}}{n+1}\right\}.\end{aligned}$$

But by distributing the factor $(n-1)!$ we see

$$\begin{aligned}&\frac{n!\,(-1)^{n-k}}{n!\,k!\,(n-k)!}-\frac{n(n-1)!}{(n-1)!\,(k+1)!\,(n-k)!}\\ &\quad=\frac{(k+1)\,(-1)^{n-k}-n}{(k+1)!\,(n-k)!}>\frac{-(k+1+n)}{(k+1)!\,(n-k)!}.\end{aligned}$$

Therefore,

$$\log \varepsilon > \frac{1}{P}\left[\frac{L^{n+1}}{(n+1)!}-\sum_{k=0}^{n-1}\frac{n+k+1}{(k+1)!\,(n-k)!}L^{k+1}\,Q^{n-k}-\frac{nQ^{n+1}}{(n+1)!}\right].$$

Estimating the second term we see that

$$\begin{aligned}\sum_{k=0}^{n-1}L^{k+1}\,Q^{n-k}\frac{n+k+1}{(n-k)!\,(k+1)!} &= \frac{QL}{(n-1)!}\sum_{k=0}^{n-1}\binom{n-1}{k}L^k\,Q^{n-1-k}\frac{(n+k+1)}{(n-k)\,(k+1)}\\ &\le \frac{2LQ}{(n-1)!}(L+Q)^{n-1},\quad \text{since } \frac{n+k+1}{(k+1)\,(n-k)}\le 2\\ &< \frac{2LQ}{(n-1)!}\left(L+\frac{L}{n}\right)^{n-1} \text{ provided } L>nQ\\ &< \frac{2L^nQ}{(n-1)!}\,e.\end{aligned}$$

Since $\left(1+\frac{1}{n}\right)^{n-1}$ increases to e as n goes to infinity. Now we estimate the third term of the sum:
$\frac{nQ^{n+1}}{(n+1)!}\le\frac{(nQ)^{n-1}\,Q^2}{(n+1)!}\le\frac{L^n}{(n+1)!}$ provided that $L>Q^2$ and $L>nQ$. Assuming the above provisos we get

$$\begin{aligned}\log \varepsilon &> \frac{1}{P}\left[\frac{L^{n+1}}{(n+1)!}-\frac{2eL^nQ}{(n-1)!}-\frac{L^n}{(n+1)!}\right]\\ &> \frac{1}{2P}\frac{L^{n+1}}{(n+1)!}\end{aligned}$$

provided

$$\frac{1}{2}\frac{L^{n+1}}{(n+1)!}>\frac{2eL^nQ}{(n-1)!}+\frac{L^n}{(n+1)!};$$

that is, $L>4e(n+1)nQ+2$. Notice that this implies $L>nQ$. Therefore we see that $L>\max\{Q^2, 4e(n+1)nQ+2\}$ is the needed hypothesis. This completes the proof.

In order to handle the assumption that $gcd(\mathcal{A}_i, \bar{\mathcal{A}}_j)=1$ we need the following lemma.

Lemma 1.8. *Let $\mathcal{A}_1, \cdots, \mathcal{A}_n$ be ideals of $\mathcal{O}_d$, $d>1$ square-free with $a_i=N(\mathcal{A}_i)$ and such that:*

(a) *$\mathcal{A}_1, \cdots, \mathcal{A}_n$ are principal*

(b) *$gcd(a_i, D)=1$, where D is the discriminant*

(c) *$a_1, \cdots, a_n$ are quadratically independent.*

Then there are ideals $\mathcal{B}_1, \cdots, \mathcal{B}_n$ with $b_i=N(\mathcal{B}_i)$ so that:

(i) *$\mathcal{B}_1, \cdots, \mathcal{B}_n$ are principal*

(ii) *$gcd(\mathcal{B}_i, \bar{\mathcal{B}}_j)=1$ for $1\leq i, j\leq n$*

(iii) *$\boldsymbol{Q}(\sqrt{a_1}, \cdots, \sqrt{a_j})=\boldsymbol{Q}(\sqrt{b_1}, \cdots, \sqrt{b_j})$ for $1\leq j\leq n$*

(iv) *$\log_2 b_j\leq \sum_{u=1}^{j}\prod_{v=1}^{u}\log_2 a_{j+1-v}$ for $1\leq j\leq n$*

Proof. We proceed by induction on k in $\mathcal{B}_1, \cdots, \mathcal{B}_k$.

For $k=1$, let $Q=gcd(\mathcal{A}_1, \bar{\mathcal{A}}_1)$. Then we can write $\mathcal{A}_1=Q\bar{Q}\mathcal{B}_1$ where $gcd(\mathcal{B}_1, \bar{\mathcal{B}}_1)=1$. We used the fact that $gcd(Q, \bar{Q})=1$ since $gcd(a_1, D)=1$. Furthermore, by the quadratic independence of a_1 and the fact that $Q\bar{Q}=(q)$ where $N(Q)=q$ we see that $\mathcal{B}_1$ is principal and $\boldsymbol{Q}(\sqrt{a_1})=\boldsymbol{Q}(\sqrt{b_1})$. Notice that $b_1\leq a_1$; hence, $\log_2 b_1\leq\log_2 a_1$.

Now suppose we have constructed $\mathcal{B}_1, \cdots, \mathcal{B}_{k-1}$ satisfying the properties (i)–(iv). By hypothesis, $\mathcal{B}_1, \cdots, \mathcal{B}_{k-1}$ are products of prime ideals $\mathcal{P}_1, \cdots, \mathcal{P}_m$ where $gcd(\mathcal{P}_i, \bar{\mathcal{P}}_j)=1$. We can write $\mathcal{A}_k=\mathcal{P}_1^{e_1}\bar{\mathcal{P}}_1^{f_1}\cdots\mathcal{P}_m^{e_m}\bar{\mathcal{P}}_m^{f_m}\mathcal{A}$ where $\mathcal{P}_i$ and $\bar{\mathcal{P}}_i$ do not divide $\mathcal{A}$ for $i=1, \cdots, m$. Now we multiply by suitable powers of $\mathcal{B}_i$ so that we get an ideal

$$C=\mathcal{A}_k\prod_{i=1}^{k-1}\mathcal{B}_i^{d_i}=\mathcal{P}_1^{e_1'}\bar{\mathcal{P}}_1^{f_1'}\cdots\mathcal{P}_m^{e_m'}\bar{\mathcal{P}}_m^{f_m'}\mathcal{A}$$

with $e_i'\geq f_i'$. Let $Q=gcd(C, \bar{C})$. We again use the fact that $\mathcal{A}_k$ has no ramified factors since $gcd(a_k, D)=1$ to see that

$$C=Q\bar{Q}\,\mathcal{P}_i^{e_i''}\cdots\mathcal{P}_m^{e_m''}\mathcal{A}''$$

where $gcd(\mathcal{A}'', \bar{\mathcal{A}}'')=1$ and $e_i''=e_i'-f_i'\geq 0$. Now let $\mathcal{B}_k=\mathcal{P}_1^{e_1''}\cdots\mathcal{P}_m^{e_m''}\mathcal{A}''$ and

we see that $\mathcal{B}_k$ is principal, $\boldsymbol{Q}(\sqrt{a_1}, \cdots, \sqrt{a_k})=\boldsymbol{Q}(\sqrt{b_1}, \cdots, \sqrt{b_k})$ and $gcd(\mathcal{B}_i, \bar{\mathcal{B}}_j)=1$ for $1\leq i, j\leq k$.

Lastly, we must check the bound on $\log_2 b_k$. From the factorization of $\mathcal{A}_k$ we see that $\sum_{i=1}^{m} f_i$, the number of $\bar{\mathcal{P}}_i$, is less than $\log_2 a_k$. From the definition of $\mathcal{B}_k$ and C we see:

$$b_k = N(\mathcal{B}_k)\leq N(C) = a_k \prod_{i=1}^{k-1} b_i^{d_i}.$$

Let $B=\max_{1\leq i\leq k-1} b_i$ and notice $\Sigma d_i\leq \Sigma f_i$ so that

$$b_k\leq a_k B^{\Sigma d_i}\leq a_k B^{\Sigma f_i}\leq a_k B^{\log_2 a_k}=a_k^{1+\log_2 B}.$$

The bounds on $b_1, \cdots, b_{k-1}$ given by induction hypothesis are increasing; hence,

$$\log_2 B\leq \sum_{u=1}^{k-1}\prod_{v=1}^{u} \log a_{k-v}.$$

Therefore,

$$\log_2 b_k\leq \log_2 a_k\Big(1+\sum_{u=1}^{k-1}\prod_{v=1}^{u} \log_2 a_{k-v}\Big)$$

$$=\sum_{u=1}^{k}\prod_{v=1}^{u} \log_2 a_{k+1-v}.$$

This completes the lemma.

Now we extend Theorem 1.7 to avoid the assumption that $gcd(\mathcal{A}_i, \bar{\mathcal{A}}_j)=1$.

Theorem 1.9. *Let the quadratic number field $\boldsymbol{Q}(\sqrt{d})$ have discriminant D and fundamental unit ε. Suppose $a_1, \cdots, a_n\in \boldsymbol{N}$ are quadratically independent with $(a_i)=\mathcal{A}_i\bar{\mathcal{A}}_i$ where $\mathcal{A}_i$ is principal and $gcd(a_i, D)=1$ for $1\leq i\leq n$. Then*

$$\log \varepsilon>\frac{1}{2P_0(n+1)!}\left(\log\frac{\sqrt{D}}{2}\right)^{n+1}$$

provided $\log\dfrac{\sqrt{D}}{2}>\max\{Q_0^2, 4en(n+1)Q_0+2\}$ *where*

$$P_0=\prod_{w=1}^{n}\sum_{u=1}^{w}\prod_{v=1}^{u} \log_2 a_{w+1-v} \text{ and}$$

$$Q_0^2 = n\sum_{w=1}^{n}\Big(\sum_{u=1}^{w}\prod_{v=1}^{u} \log_2 a_{w+1-v}\Big)^2.$$

(Here logarithms without explicit base are natural logarithms and e is the base.)

Proof. We use Lemma 1.8 to choose ideals $\mathcal{B}_1, \cdots, \mathcal{B}_n$ satisfying the hypo-

thesis of the effective theorem, Theorem 1.7, including $gcd(\mathcal{B}_i, \bar{\mathcal{B}}_j)=1$. The P and Q of the effective theorem are

$$P = \log b_1 \cdots \log b_n$$

$$Q^2 = n((\log b_1)^2 + \cdots + (\log b_n)^2)$$

where $b_i=N(\mathcal{B}_i)$. Using the bound from Lemma 1.8 we have

$$\log_2 b_k \leq \sum_{u=1}^{k} \prod_{v=1}^{u} \log_2 a_{k+1-v} \qquad \text{for } 1 \leq k \leq n .$$

We see that $P_0 \geq P$ and $Q_0 \geq Q$ and hence the theorem holds.

2. The monomial norm equation

We now turn to the problem of finding classes of D satisfying the hypotheses of Theorem 1.9. The main hypothesis is that $\mathcal{A}_i$ is principal; that is, there is an element of $\mathcal{O}_d$ with norm a_i for $i=1, 2, \cdots, n$. Notice that the following suffices: If we have $A_i, B_i, D \in \boldsymbol{Z}[x]$, $e_i \in \boldsymbol{N}$, p a prime and

$$A_1^2 - B_1^2 D = p$$

$$A_i^2 - B_i^2 D = c_i x^{e_i} \qquad i = 2, \cdots, n$$

then the class of fields given by $D(p^k)$ has principal ideals of norm $p, c_2, \cdots, c_n$.

We call the following generalization of this the Monomial Norm Equation:

$$A_i^2 - B_i^2 D = c_i x^{e_i} \qquad i = 1, \cdots, n$$

where $A_i, B_i, D \in \boldsymbol{Q}[x]$, $e_i \in \boldsymbol{N}$ and $c_1, \cdots, c_n$ are quadratically independent.

Many properties of the monomial norm equation are studied in Reiter [3]. We give some fundamental properties here. The first shows that we need to consider the monomial norm equation and not a constant norm equation.

We can divide $A_i^2 - B_i^2 D = c_i$ by a square so that A_i can be taken to be monic. Then the highest coefficient of D is a square; therefore, we can factor it out so that we may assume B_i and D are monic also.

With these conventions in mind we can prove the uniqueness of the constant norm for a fixed $D(x)$.

Theorem 2.1. *Suppose $A_i, B_i, D \in \boldsymbol{Q}[x]$ with D nonconstant but not necessarily square-free and with $A_i^2 - B_i^2 D = c_i$ for $i=1, 2$. Then c_1, c_2 are quadratically dependent.*

Proof. Suppose not, choose A_i, B_i, c_i so that B_1 has the smallest possible degree and B_2 has the smallest degree possible once the degree of B_1 is fixed where c_1, c_2 are quadratically independent. Let deg $B_i = j_i$ and deg $D = 2k$.

So deg $A_i=j_i+k$ and $j_1\leq j_2$.

We have seen that we can take A_i, B_i, D to be monic. Now $A_1^2-B_1^2D=c_1$ and $A_2^2-B_2^2D=c_2$ implies $A_1^2B_2^2-B_1^2B_2^2D=c_1B_2^2$ and $A_2^2B_1^2-B_1^2B_2^2D=c_2B_1^2$. Thus, $(A_1B_2-A_2B_1)(A_1B_2+A_2B_1)=A_1^2B_2^2-B_1^2A_2^2=c_1B_2^2-c_2B_1^2$. Let $\deg(A_1B_2-A_2B_1)=e$, so $0\leq e<j_1+j_2+k$. By comparing degrees of the above we have $e+j_1+j_2+k=2j_2$; i.e., $e=j_2-j_1-k$.

We also see that $(A_1-B_1\sqrt{D})(A_2+B_2\sqrt{D})=A_1A_2-B_1B_2D+(A_1B_2-A_2B_1)\sqrt{D}$ has norm c_1c_2. Now c_1, c_1c_2 are quadratically independent since c_1, c_2 were taken to be. By the minimality of j_2 we see that $j_2\leq\deg(A_1B_2-A_2B_1)=e$. So $j_2\leq j_2-j_1-k$; i.e., $k+j_1\leq 0$. This is the desired contradiction since $0<\deg D=2k$.

This theorem excludes the wild hope of finding polynomials $D(x)$, $E(x)$ so that $A(x, y)^2-B(x, y)^2D(x)=E(y)$ where $D(x)$ and $E(y)$ take on infinitely many quadratically independent values. In particular it excludes two quadratically independent values. Since no $D(x)$ can have polynomial witnesses to two independent constant norms we will need to study the monomial norm equation to get sequences of length two or more to which we can apply Yamamoto type theorems.

Next we get some control on the degree of D in terms of the number of monomial norms.

Theorem 2.2. *Let* $A_i^2-B_i^2D=c_i x^{2f_i}$, $A_i, B_i, D\in\boldsymbol{Q}[x]$, $f_i\in\boldsymbol{N}$ *for* $1\leq i\leq n$ *and with* $c_1, \cdots, c_n$ *quadratically independent. Suppose* $x^2\nmid D$ *and let* $t=$*power of* 2 *dividing* deg D. *Then* $n\leq t$.

Proof. Let $G=\langle\sigma_1\rangle\times\cdots\times\langle\sigma_n\rangle$ be the Galois group of $\boldsymbol{Q}(\sqrt{c_1}, \cdots, \sqrt{c_n})$ over $\boldsymbol{Q}$. This is generated by the automorphisms $\sigma_1, \cdots, \sigma_n$ where σ_i: $\sqrt{c_i}\mapsto-\sqrt{c_i}$ and leaves everything else fixed. We want to show that that $D=\prod_{\sigma\in G}D_n^{\sigma_2}$ for some $D_n\in\boldsymbol{Q}(\sqrt{c_1}, \cdots, \sqrt{c_n})[x]$. Then $2^n=|G|$ will divide deg D and we will have our result.

We first show the following fact: Any factor $F\in\boldsymbol{Q}(\sqrt{c_1}, \cdots, \sqrt{c_{k-1}})[x]$ of D factors as $F=F_1F_1^{\sigma_k}$ where $F_1\in\boldsymbol{Q}(\sqrt{c_1}, \cdots, \sqrt{c_k})[x]$. Suppose we have such an F, so $D=FE$ and $B_k^2FE=B_k^2D=(A_k+\sqrt{c_k}x^{f_k})(A_k-\sqrt{c_k}x^{f_k})$. Let J be any irreducible factor of F and $A_k+\sqrt{c_k}x^{f_k}$ in $\boldsymbol{Q}(\sqrt{c_1}, \cdots, \sqrt{c_k})[x]$. Then $J^{\sigma_k}|F^{\sigma_k}=F$. If $J=J^{\sigma_k}$ then $J=J^{\sigma_k}|(A_k-\sqrt{c_k}x^{f_k})$ so $J|(A_k+\sqrt{c_k}x^{f_k})-(A_k-\sqrt{c_k}x^{f_k})=2\sqrt{c_k}x^{f_k}$; hence, J is a monomial. $D=FE$ has an even number of irreducible factors since B_k^2 and B_k^2D do; therefore, such a $J=J^{\sigma_k}$ would require another $K=K^{\sigma_k}$ also dividing D. Then x^2 divides JK which divides D; this is a contradiction. Thus $J\neq J^{\sigma_k}$ and hence $JJ^{\sigma_k}|F$. Repeating this argument for the other irreducible factors of F we see $F=F_1F_1^{\sigma_k}$ for $F_1\in\boldsymbol{Q}(\sqrt{c_1}, \cdots, \sqrt{c_k})[x]$ as desired.

We now use the above fact repeatedly. First, $k=1$ and $F=D$ gives $D=D_1D_1^{\sigma_1}$; then $k=2$ and $F=D_1$ gives $D_1=D_2D_2^{\sigma_2}$; hence $D=\prod_{\sigma\in\langle\sigma_1\rangle\times\langle\sigma_2\rangle} D_2^{\sigma}$. We continue this and conclude $D=\prod_{\sigma\in G} D_n^{\sigma}$ as suffices to prove the theorem.

We get the following immediate Corollary.

Corollary 2.3. *Let* $A_i^2-B_i^2D=c_i\,x^{e_i}$, A_i, B_i, $D\in\boldsymbol{Q}[x]$, $e_i\in\boldsymbol{N}$ *for* $1\leq i\leq n$ *and with* $c_1, \cdots, c_n\in\boldsymbol{Q}$ *quadratically independent. Suppose* $x\nmid D$ *and let* t *be the power of* 2 *dividing* deg D. *Then if the* e_i *are even,* $n\leq t$, *but in any case* $n\leq t+1$.

Proof. If some e_i is odd map $x\mapsto x^2$. Then apply the theorem with $t+1$ replacing t.

We mention, without giving the tedious proof, the following theorem from Reiter [3].

Theorem 2.4. *If* $D=A_i^2-c_i\,x^{e_i}$ *where* D, $A_i\in\boldsymbol{Q}[x]$, $i=1, \cdots, n$ *and* $c_1, \cdots, c_n\in\boldsymbol{Q}$ *are quadratically independent, then* $n\leq 2$.

In order to get $n=3$ with this monomial norm approach we can have at most one constant norm; Corollary 2.3 implies $4\mid\deg D$; and Theorem 2.4 implies nonconstant B's will be needed. Thus, the simplest solution to the Monomial Norm Equation with $n=3$ must be fairly complicated; the author conjectures such a solution exists. We now turn to new examples with $n=2$.

3. Classes of large fundamental units

In this section we give two broad classes of D's which have fundamental units which are large in the sense that $\log \varepsilon_d>c\,(\log d)^3$ as was the case in Yamamoto's example. The first class gives a two parameter family of D's for every factorization of x^j-1 for j odd. Yamamoto's example arises from the trivial factoriation $x-1=1(x-1)$. The second class also gives a two parameter family of D's for every factorization of x^j-1 for j odd. These new examples use higher degree B.

Notice that if $4F_1F_2=c_2x^j-c_1$ then
$(F_1\,x^i-F_2)^2-c_1\,x^i=(F_1\,x^i+F_2)^2-c_2\,x^{i+j}$. In practice we want a prime norm. The easiest way to do this is to let $i=0$, $c_1=p$, $c_2=pq^j$. Then we get:

Theorem 3.1. *Let* p, $q\in\boldsymbol{Z}$, $p>2$ *a prime and* q *odd and quadratically independent with* $gcd(q,\ p-1)=1$. *Suppose* $F_1F_2=x^j-1$ *for* F_1, $F_2\in\boldsymbol{Z}[x]$ *and* $j\in\boldsymbol{N}$ *odd and let* $G_1(x)=F_1(qx)$, $G_2(x)=F_2(qx)$. *Then*

$$\begin{aligned} D &= (G_1-pG_2)^2-4p \\ &= (G_1+pG_2)^2-4pq^j\,x^j\,, \end{aligned}$$

and there is a constant c so that

$$\log \varepsilon_d > c\,(\log d)^3$$

where $d>b$ is the square-free part of $D(p^k)$ for some $k\in \boldsymbol{N}$, $k\geq 1$.
Here b and c are given explicitly in Theorem 1.9.

Proof. The fact that $(G_1-pG_2)^2-4p=(G_1+pG_2)^2-4pq^j x^j$ is clear.

Since j is odd, p and pq^j are quadratically independent. We need to check that $gcd(p, D_d)=1$, $gcd(q, D_d)=1$.

Notice that the constant terms of G_1 and G_2 are different and either 1 or -1. Hence, $D(p^k)\equiv(\pm 1)^2-0=1 \pmod p$, so $p\nmid D(p^k)$ and so $gcd(p, D_d)=1$. Let a prime $r\mid q$. We know $G_1(x)\equiv -G_2(x)\equiv \pm 1 \pmod r$, so $D(p^k)\equiv((\pm 1)-p(\pm 1))^2-0\equiv(1-p)^2$. Therefore $gcd(q, p-1)=1$ implies that $r\nmid D_d$; therefore $gcd(q, D_d)=1$. Thus we can apply Theorem 1.9 and get the claimed result.

We now turn our next broad class.

Lemma 3.2. *Suppose $F_1F_2=x^j-1$ for F_1, $F_2\in \boldsymbol{Z}[x]$ and $p\in \boldsymbol{Z}$. Let*

$$A = F_1^3 x^j+pF_1(2x^j+1)+p^2F_2$$
$$B = F_1^2+p$$
$$D = (F_1 x^j+pF_2)^2+4px^j .$$

Then $A^2-B^2D = -4p^3$.

We replace x by pqx and divide by p^2 to get:

Theorem 3.3. *Let F_1, $F_2\in \boldsymbol{Z}$ $[x]$ with $F_1F_2=x^j-1$, $j\geq 3$ odd, and p, $q\in \boldsymbol{Z}$, both odd, quadratically independent and with p a prime. Let $G_1(x)=F_1(pqx)$, $G_2(x)=F_2(pqx)$ and*

$$A = G_1^3 p^{j-1} q^j x^j+G_1(2p^j q^j x^j+1)+pG_2$$
$$B = G_1^2+p$$
$$D = (G_1 p^{j-1} q^j x^j+G_2)^2+4p^{j-1} q^j x^j$$

Then $A^2-B^2D = -4p$.

If d is the square-free part of $D(p^k)$ for $k\in \boldsymbol{N}$ then

$$\log \varepsilon_d > c\,(\log d)^3$$

for $d>b$ where b and c are effective constants given by Theorem 1.9.

Proof. We see that in $\mathcal{O}_d$ we get principal ideals of norm p and $p^{j-1} q^j p^{jk}$ and hence of norm p and q^j. Neither p nor any factor of q divides $D(p^k)$ since

G_2 has a constant term of ± 1 and p and q divide all the other terms. So there are two principal ideals with quadratically independent norms and no problems with ramification. Therefore, we can apply Theorem 1.9 to get the above bound on the fundamental unit.

Bibliography

[1] L.K. Hua: Introduction to number theory, English edition, Springer-Verlag, New York, 1982.

[2] M.A. Morrison and J. Brillhart: *A method of factoring and the factorization of* F_7, Math. Comp. **29** (1975), 183–205.

[3] C.A. Reiter: *Large fundamental units and the monomial norm equation*, Doctoral Dissertation, The Pennsylvania State University, 1984.

[4] Y. Yamamoto: *Real quadratic number fields with large fundamental units*, Osaka J. Math. **8** (1971), 261–270.

Department of Mathematics
Lafayette College
Easton, Pennsylvania 18042
U.S.A.