MATHEMATICS OF COMPUTATION
VOLUME 50, NUMBER 182
APRIL 1988, PAGES 543–556

Quintic Polynomials and Real Cyclotomic Fields with Large Class Numbers

By René Schoof and Lawrence C. Washington

Abstract. We study a family of quintic polynomials discoverd by Emma Lehmer. We show that the roots are fundamental units for the corresponding quintic fields. These fields have large class numbers and several examples are calculated. As a consequence, we show that for the prime $p = 641491$ the class number of the maximal real subfield of the pth cyclotomic field is divisible by the prime 1566401. In an appendix we give a characterization of the "simplest" quadratic, cubic and quartic fields.

1. Introduction. Let p be a prime number and let $\mathbf{Q}(\zeta_p)^+$ denote the maximal real subfield of the field of pth roots of unity $\mathbf{Q}(\zeta_p)$. A classical conjecture of H. S. Vandiver asserts that $h(\mathbf{Q}(\zeta_p)^+)$, the class number of $\mathbf{Q}(\zeta_p)^+$, is prime to p. For small values of p, the class number of $\mathbf{Q}(\zeta_p)^+$ is small: assuming certain generalized Riemann hypotheses, Frank van der Linden [14] showed that it is 1 when p is less than 163. It had therefore been suggested that perhaps these class numbers are always less than p and hence that Vandiver's conjecture is true for "trivial" reasons. This was shown to be false in [4], [11]; the prime $p = 11290018777$ has the property that $h(\mathbf{Q}(\zeta_p)^+)$ is divisible by 16671734220, a number which exceeds p. This example was constructed by finding a prime p congruent to 1 mod 12 for which both the cubic and the quadratic subfields of $\mathbf{Q}(\zeta_p)^+$ have large class numbers. In fact, in this example, $p = n^2 + 3n + 9$ with $n = 106253$; so p is the conductor of a "simplest cubic field" and these fields are known to have large class numbers [13]. In this special case the class number of the cubic subfield of $\mathbf{Q}(\zeta_p)^+$ was found to be equal to 6209212 while the quadratic subfield has class number 2685. It follows from class field theory that $h(\mathbf{Q}(\zeta_p)^+)$ is divisible by the product of the class numbers of these subfields.

One can show [8], [9] that the primes dividing the class numbers of the subfields of $\mathbf{Q}(\zeta_p)^+$ of degrees 2, 3, 4 or 6 are less than p. This implies that the fields $\mathbf{Q}(\zeta_p)^+$ with large class numbers which are constructed by means of the class groups of their subfields of degree 2, 3, 4 or 6, will never give rise to counterexamples to Vandiver's conjecture. One might wonder whether for every prime p all prime divisors of $h(\mathbf{Q}(\zeta_p)^+)$ are smaller than p; this would again imply that Vandiver's conjecture is true for trivial reasons. We will show this to be false by exhibiting a prime number p for which the class number $h(\mathbf{Q}(\zeta_p)^+)$ is divisible by a prime exceeding p.

For the reasons just given, as is pointed out in the discussions in [4] and [12, p. 260], the natural place to look is cyclic quintic fields of prime conductor having

Received June 15, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R11, 11R16, 11R21, 11R27.
Key words and phrases. Cyclotomic fields, class number, unit group, geometry of numbers.

0025-5718/88 $1.00 + $.25 per page

small units, since the class numbers of such fields will be large and will not have the factorizations caused by proper subfields.

In 1986, Emma Lehmer exhibited a family of quintic fields which are analogous to the simplest cubic fields. These fields are cyclic over $\mathbf{Q}$ and the unit groups of their rings of integers are generated by units that are small in size. The fields in this family that have prime conductor p have a regulator of size only $O(\log^4 p)$. The Brauer-Siegel Theorem gives then that the class numbers of these fields are at least $p^{2-\varepsilon}$ for large p, for every $\varepsilon > 0$. It follows from class field theory that the class number of $\mathbf{Q}(\zeta_p)^+$ is divisible by the class number of its quintic subfield. In this way, one obtains examples of primes p for which the class number of $\mathbf{Q}(\zeta_p)^+$ is very large and probably for many p divisible by primes exceeding p.

In the present paper we report on some of our considerations and computations concerning the quintic fields of Emma Lehmer. We prove the following

THEOREM. *Let p be the prime* 641491. *The class number $h(\mathbf{Q}(\zeta_p)^+)$ is divisible by the prime* 1566401.

We will in fact show that the quintic subfield of $\mathbf{Q}(\zeta_p)^+$ has class number equal to 1566401.

In [7] Emma Lehmer explains how she obtained the family of quintic fields. In Section 3 we will study the polynomials and the fields exhibited by Emma Lehmer and we will show that the zeros of her polynomials are fundamental units of the rings of integers of these fields. We will need a result from geometry of numbers which is discussed in Section 2. In Section 4 we explain how the computations were done and we present a few examples of primes p of moderate size for which $h(\mathbf{Q}(\zeta_p)^+)$ exceeds p.

Acknowledgments. We thank Hendrik Lenstra for the proof of Theorem (2.2) and Armand Brumer for suggesting to us how to find the transformation formula (3.2). We especially thank Daniel Shanks, from whom we learned about Emma Lehmer's polynomials, for his continued interest in this project. This paper was written during a stay at MSRI in Berkeley. The second author was also partially supported by NSF.

2. Unit Groups of Cyclic Quintic Fields. Let K be a cyclic extension of degree five over $\mathbf{Q}$. The field K can be embedded into the real numbers and we fix once and for all one such embedding $K \subset \mathbf{R}$. Let G be the Galois group of K over $\mathbf{Q}$ and let σ denote a generator of G. In this section we will study O_K^*, the group of units of the ring of integers O_K of K.

The unit group O_K^* is a $\mathbf{Z}[G]$-module. There is a canonical G-homomorphism from O_K^* to the group ring $\mathbf{R}[G]$ given by

$$\varepsilon \to \sum_{\tau \in G} \log|\tau(\varepsilon)| \cdot [\tau], \tag{2.1}$$

where $\tau(\varepsilon)$ is viewed as an element of $\mathbf{R}$ via the fixed embedding $K \subset \mathbf{R}$. The kernel of this map is $\{1, -1\}$; since for every $\varepsilon \in \mathbf{O}_K^*$ the norm $\prod_{\tau \in G} \tau(\varepsilon)$ is either 1 or -1, the image L of O_K^* is contained in the augmentation ideal $V = \{\sum_{\tau \in G} \alpha_\tau \cdot [\tau] \colon \alpha_\tau \in \mathbf{R}, \sum_{\tau \in G} \alpha_\tau = 0\}$ of $\mathbf{R}[G]$. The augmentation ideal V is a 4-dimensional real vector space and by Dirichlet's Unit Theorem, $L \approx O_K^*/\{1, -1\}$ is a lattice of $\mathbf{Z}$-rank 4 in

V. Let $N = 1 + \sigma + \sigma^2 + \sigma^3 + \sigma^4 \in \mathbf{Z}[G]$ be the G-norm. We fix an isomorphism of the ring $\mathbf{Z}[G]/(N)$ with $\mathbf{Z}[\zeta_5]$, the ring generated by the 5th roots of unity, by having σ correspond with ζ_5, a fixed 5th root of unity. In this way, both V and $O_K^*/\{1,-1\}$ become modules over $\mathbf{Z}[\zeta_5]$.

In order to describe the metric structure of the lattice L in the Euclidean space V, we need a result from geometry of numbers.

For any scalar product $\langle\ ,\ \rangle$ on a real vector space W we will write $\|\mathbf{x}\|$ for $\langle \mathbf{x}, \mathbf{x}\rangle^{1/2}$. If M is a lattice of maximal rank in W, we denote by $\det(M)$ the volume of W/M measured with respect to the scalar product $\langle\ ,\ \rangle$.

(2.2) THEOREM. *Let V be a 4-dimensional real vector space with a scalar product $\langle\ ,\ \rangle$. Let $L \subset V$ be a lattice in V of $\mathbf{Z}$-rank 4 and let G be a group of order 5 which acts isometrically on V and respects L. Suppose that the norm $N = \sum_{\tau \in G} \tau$ annihilates V. Then there exists a vector $\mathbf{x}$, which generates L as a G-module, satisfying*

$$\|\mathbf{x}\| \leq 2^{1/2} 5^{-1/8} \det(L)^{1/4}.$$

Proof. Let σ be a generator of G. Both V and L are $\mathbf{Z}[G]/(N)$-modules; we will regard them as $\mathbf{Z}[\zeta_5]$-modules using the isomorphism $\mathbf{Z}[G]/(N) = \mathbf{Z}[\zeta_5]$ mentioned above. The fact that G acts isometrically is easily checked to be equivalent to

$$\langle \alpha \mathbf{x}, \mathbf{y}\rangle = \langle \mathbf{x}, \bar{\alpha}\mathbf{y}\rangle \quad \text{for all } \mathbf{x}, \mathbf{y} \in V \text{ and } \alpha \in \mathbf{Z}[\zeta_5], \tag{2.3}$$

where the overhead bar denotes the automorphism of $\mathbf{Z}[\zeta_5]$ given by $\zeta_5 \to \zeta_5^{-1}$.

Let $\mathbf{x} \neq \mathbf{0}$ be a shortest vector in L. Since L is a $\mathbf{Z}[\zeta_5]$-module, we have that $\mathbf{Z}[\zeta_5] \cdot \mathbf{x} \subset L$. The vectors $\mathbf{b}_i = \zeta_5^i \mathbf{x}$ with $0 \leq i \leq 3$ form a $\mathbf{Z}$-basis for $\mathbf{Z}[\zeta_5] \cdot \mathbf{x}$. Note that $\|\mathbf{b}_i\| = \|\mathbf{x}\|$ for every i, because multiplication by ζ_5 is an isometry. By a standard result in geometry of numbers [6, Lemma (7.2)], there exists, given $\mathbf{y} \in V$, a vector $\mathbf{z} \in \mathbf{Z}[\zeta_5] \cdot \mathbf{x}$ with $\|\mathbf{y} - \mathbf{z}\|^2 < \sum_{i=0}^{3} \frac{1}{4}\|\mathbf{b}_i\|^2 = \|\mathbf{x}\|^2$, where the inequality is strict since the $\mathbf{b}_i$ are not orthogonal; after all, if the $\mathbf{b}_i$ were orthogonal, then $\zeta_5^4 \mathbf{x}$ would by (2.3) be orthogonal to each of them, which is clearly impossible. When we apply this result to a vector $\mathbf{y} \in L$ we find, since $\mathbf{x}$ is a shortest vector, that $\mathbf{y} = \mathbf{z} \in \mathbf{Z}[\zeta_5] \cdot \mathbf{x}$. We conclude that $\mathbf{x}$ generates L as a G-module and hence that $V = \mathbf{R} \otimes_{\mathbf{Z}} \mathbf{Z}[\zeta_5]$ as a $\mathbf{Z}[\zeta_5]$-module.

Let us note in passing that an application of the above argument to the lattice L which one gets by embedding an ideal of $\mathbf{Z}[\zeta_5]$ in $\mathbf{R} \otimes_{\mathbf{Z}} \mathbf{Z}[\zeta_5]$ implies the well-known fact that the ring $\mathbf{Z}[\zeta_5]$ is a principal ideal domain.

The 4-dimensional representation $V = \mathbf{R} \otimes_{\mathbf{Z}} \mathbf{Z}[\zeta_5]$ decomposes with respect to the invariant scalar product into an orthogonal sum of two $\mathbf{R}$-irreducible 2-dimensional representations. On one factor, σ acts as a rotation by $2\pi/5$, and on the other as rotation by $4\pi/5$. We will identify each of the factors with $\mathbf{C}$; on the first factor, ζ_5 acts as multiplication by $e^{2\pi i/5}$, and on the second as multiplication by $e^{4\pi i/5}$. It follows from (2.3) that the scalar product, restricted to each factor, is "Hermitian" with respect to the action of $\mathbf{Z}[\zeta_5]$. Therefore, we can choose a basis of $V = \mathbf{C} \oplus \mathbf{C}$ such that the length of $\mathbf{z} = (z_1, z_2) \in V$ is given by

$$\|(z_1, z_2)\| = \sqrt{z_1\bar{z}_1 + z_2\bar{z}_2} = \sqrt{|z_1||z_2|}\sqrt{\left|\frac{z_1}{z_2}\right| + \left|\frac{z_2}{z_1}\right|}. \tag{2.4}$$

It is easy to see that the lattice $\mathbf{Z}[\zeta_5](1,1) \subset V$ corresponds to the embedding $\mathbf{Z}[\zeta_5] \subset \mathbf{C} \oplus \mathbf{C}$ via the two complex places of the fields $\mathbf{Q}(\zeta_5)$. A standard volume calculation shows that $\det(\mathbf{Z}[\zeta_5](1,1)) = 2^{-2}5^{3/2}$. Therefore, with $\mathbf{x} = (x_1, x_2)$, we have that $\det(L) = \det(\mathbf{Z}[\zeta_5](x_1, x_2)) = |x_1|^2|x_2|^2 2^{-2}5^{3/2}$. We obtain from (2.4) that

$$\|\mathbf{x}\| = \det(L)^{1/4} 5^{-3/8} 2^{1/2} \sqrt{\left|\frac{x_1}{x_2}\right| + \left|\frac{x_2}{x_1}\right|}. \tag{2.5}$$

Let ε denote the unit $\zeta_5 + \zeta_5^{-1} \in \mathbf{Z}[\zeta_5]$. Suppose that $|x_1|/|x_2| > \frac{1}{2} + \frac{1}{2}\sqrt{5}$ and let $\mathbf{y} = \varepsilon^{-1} \cdot \mathbf{x}$; since $|y_1||y_2| = |x_1||x_2|$ and $|y_1|/|y_2| = (\frac{1}{2} + \frac{1}{2}\sqrt{5})^{-2} \cdot |x_1|/|x_2|$, it follows easily that $|y_1/y_2| + |y_2/y_1| < |x_1/x_2| + |x_2/x_1|$ and hence by (2.4) that $\mathbf{y}$ is shorter than $\mathbf{x}$. This is impossible, and we conclude that $|x_1|/|x_2| \leq \frac{1}{2} + \frac{1}{2}\sqrt{5}$. By a similar argument one concludes that $|x_2|/|x_1| \leq \frac{1}{2} + \frac{1}{2}\sqrt{5}$. A glance at the function $t \to t + 1/t$ gives then that $|x_1/x_2| + |x_2/x_1| \leq \frac{1}{2} + \frac{1}{2}\sqrt{5} + (\frac{1}{2} + \frac{1}{2}\sqrt{5})^{-1} = \sqrt{5}$, and the desired inequality follows from (2.5). This proves the theorem. □

(2.6) COROLLARY. *Let K be a cyclic extension of degree 5 over $\mathbf{Q}$ with $G = \mathrm{Gal}(K/\mathbf{Q})$. There exists a unit $\varepsilon \in O_K^*$ which generates $O_K^*/\{1,-1\}$ as a G-module and which satisfies*

$$\left(\sum_{\tau \in G} \log^2 |\tau(\varepsilon)|\right)^{1/2} \leq \sqrt{2} R_K^{1/4},$$

where R_K is the regulator of K.

Proof. The G-homomorphism in (2.1) turns $O_K^*/\{1,-1\}$ into a lattice in the 4-dimensional real vector space $V = \{\sum_{\tau \in G} \alpha_\tau \cdot [\tau] \colon \alpha_\tau \in \mathbf{R}, \sum_{\tau \in G} \alpha_\tau = 0\} \subset \mathbf{R}[G]$. The space $V \subset \mathbf{R}[G]$ is a G-module, annihilated by the G-norm and equipped with the usual Euclidean scalar product: for $\mathbf{x} = \sum_{\tau \in G} x_\tau \cdot [\tau]$ and $\mathbf{y} = \sum_{\tau \in G} y_\tau \cdot [\tau]$ we let

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{\tau \in G} x_\tau \cdot y_\tau.$$

With respect to this scalar product, the group G acts isometrically on V.

From Theorem (2.2) we conclude that there is a unit $\varepsilon \in O_K^*$ which generates $O_K^*/\{1,-1\}$ as a G-module and which satisfies

$$\|\varepsilon\| \leq 2^{1/2} 5^{-1/8} \det(L)^{1/4},$$

where the determinant $\det(L)$ is the volume V/L measured with respect to the metric induced by the scalar product on $\mathbf{R}[G]$. The regulator R_K is obtained by projecting V onto $\mathbf{R}^4$, using (say) the first four coordinates in $\mathbf{R}[G]$, and then computing the volume of V/L with respect to the usual measure on $\mathbf{R}^4$. The first volume is $\sqrt{5}$ times larger, so that $\det(L) = \sqrt{5} R_K$ and the result follows easily. □

The "Hermite constant" $2^{1/2}5^{-1/8}$ in the above theorem is best possible: Take L to be the ideal generated by $1 - \zeta_5$ in $\mathbf{Z}[\zeta_5]$ and let $V = \mathbf{R} \otimes_{\mathbf{Z}} \mathbf{Z}[\zeta_5] = \mathbf{C} \oplus \mathbf{C}$ have the scalar product induced by (2.4). The determinant of L equals $\mathrm{Norm}(1 - \zeta_5) \cdot \det(\mathbf{Z}[\zeta_5]) = 5 \cdot 5^{3/2} 2^{-2} = 5^{5/2} 2^{-2}$, and the vector $\mathbf{x} = 1 - \zeta_5$ in L has length

$$\|\mathbf{x}\| = \sqrt{(1 - \zeta_5)(1 - \zeta_5^{-1}) + (1 - \zeta_5^2)(1 - \zeta_5^{-2})} = \sqrt{5};$$

this implies that

$$\frac{\|\mathbf{x}\|}{\det(L)^{1/4}} = \frac{\sqrt{5}}{2^{-1/2}5^{5/8}} = 2^{1/2}5^{-1/8}.$$

Our Hermite constant for lattices of rank 4 with action by $\mathbf{Z}[\zeta_5]$ is slightly smaller than the Hermite constant for arbitrary lattices of rank 4 which equals $2^{1/4}$, see [2, p. 332].

(2.7) COROLLARY. *Let K be a cyclic extension of degree 5 over $\mathbf{Q}$. Let f denote the conductor and let R_K denote the regulator of K. We have that*

$$R_K \geq \frac{1}{25}\log^4\left(\frac{f}{2}\right).$$

Proof. Our approach is similar to Cusick's [3]. By Corollary (2.6), we can find a unit $\varepsilon \in O_K^*$ with

$$\left(\sum_{\tau\in G}\log^2|\tau(\varepsilon)|\right)^{1/2} \leq \sqrt{2}R_K^{1/4}. \tag{2.8}$$

Let $\varepsilon_1 \leq \varepsilon_2 \leq \varepsilon_3 \leq \varepsilon_4 \leq \varepsilon_5$ denote the conjugates of ε in $K \subset \mathbf{R}$. The discriminant $\Delta = f^4$ of K over $\mathbf{Q}$ satisfies

$$\Delta \leq \prod_{1\leq i<j\leq 5}(\varepsilon_i - \varepsilon_j)^2 = \prod_{1\leq i<j\leq 5}\left(1-\frac{\varepsilon_i}{\varepsilon_j}\right)^2 \prod_{j=1}^{5}\varepsilon_j^{2(j-1)} \leq M\prod_{j=1}^{5}\varepsilon_j^{2(j-3)},$$

where

$$M = \sup_{0<|x_1|\leq\cdots\leq|x_5|}\prod_{i<j}\left(1-\frac{x_i}{x_j}\right)^2.$$

Here we used that $\prod_j \varepsilon_j^2 = 1$. It was shown by M. Pohst in [10, p. 467] that $M = 16$. Therefore, by the Cauchy-Schwarz inequality,

$$\log\left(\frac{\Delta}{16}\right) \leq 2\sum_{j=1}^{5}(j-3)\log|\varepsilon_j| \leq 2\left(\sum_{j=1}^{5}(j-3)^2\right)^{1/2}\left(\sum_{j=1}^{5}\log^2|\varepsilon_j|\right)^{1/2},$$

and hence by (2.8),

$$\log\left(\frac{f^4}{16}\right) = \log\left(\frac{\Delta}{16}\right) \leq 2\sqrt{10}\left(\sum_{j=1}^{5}\log^2|\varepsilon_j|\right)^{1/2} \leq 2\sqrt{10}\cdot\sqrt{2}\cdot R_K^{1/4}.$$

This easily implies the desired result. □

A similar estimate was obtained by G. Gras and M.-N. Gras in [5]. Their estimate is better for very large f, but ours seems to be more useful for the applications in Section 3.

3. The Quintic Fields of Emma Lehmer. In [7] Emma Lehmer exhibits a family of polynomials $F_n(X) \in \mathbf{Z}[X]$ for $n \in \mathbf{Z}$. The polynomials are given by

$$X^5 + n^2X^4 - (2n^3+6n^2+10n+10)X^3 + (n^4+5n^3+11n^2+15n+5)X^2 + (n^3+4n^2+10n+10)X + 1.$$

Their discriminants are equal to $(n^3+5n^2+10n+7)^2(n^4+5n^3+15n^2+25n+25)^4$, and their zeros in $\mathbf{R}$ are approximately

$$\theta_1 \approx -(n+1)^2-2, \quad \theta_2 \approx n+1, \quad \theta_3 \approx -(n+1)^{-3},$$
$$\theta_4 \approx (n+1)+1 \quad \text{and} \quad \theta_5 \approx -(n+1)^{-1}.$$

In the sequel we will need rather precise estimates of the zeros θ_i.

(3.1) LEMMA. *When $n \in \mathbf{Z}$ satisfies $|n+1| \geq 20$, the zeros θ_i of $F_n(X)$ in $\mathbf{R}$ satisfy*

$$\log|\theta_1| = 2\log|n+1| + \delta_1, \qquad \log|\theta_2| = \log|n+1| + \delta_2,$$
$$\log|\theta_3| = -3\log|n+1| + \delta_3, \qquad \log|\theta_4| = \log|n+1| + \delta_4$$
$$\textit{and } \log|\theta_5| = -\log|n+1| + \delta_5,$$

where $|\delta_i| < 1/10$.

Proof. We considered each θ_i separately, but here only θ_5 will be discussed as an example. In the following computations, the symbolic manipulation language MACSYMA was used.

Let $G_n(X) = X^5 F_n(X^{-1})$ and expand $G_n(-(n+1))$ as a polynomial in n. It is easily seen that $G_n(-(n+1)) < 0$ for $|n+1| \geq 20$. Next expand $G_n(-.91(n+1))$ and observe it is positive for $n+1 \leq -20$. Similarly one finds that $G_n(-1.1(n+1)) > 0$ for $n+1 \geq 20$. Therefore, there is a zero of $G_n(X)$ between $-.91(n+1)$ and $-1.1(n+1)$ and hence a zero of $F_n(X)$ between $(-.91(n+1))^{-1}$ and $(-1.1(n+1))^{-1}$. The estimate for $\log|\theta_5|$ follows. The other estimates are treated similarly, except for the case of θ_2 and θ_4 with $n \geq 19$. In this case $F_n(n+1)$, $F_n(1.1(n+1))$ and $F_n(.91(n+1))$ are all positive; so we observe that $F_n(n+2) = -(n^3+5n^2+10n+7)$ which is negative. This yields the desired estimates. □

It is easy to see that $F_n(X)$ is irreducible for every $n \in \mathbf{Z}$ by considering it modulo 2. It is more difficult to show that the zeros of $F_n(X)$ generate a cyclic extension K of degree 5 over $\mathbf{Q}$. This can be done by verifying that the transformation

$$X \to \frac{(n+2)+nX-X^2}{1+(n+2)X} \tag{3.2}$$

permutes the roots of $F_n(X)$ cyclically. This is a tedious calculation, and we used the symbolic manipulation language MACSYMA to perform it.

The transformation formula (3.2) was found as follows. We explicitly computed the action of the Galois group on the roots of $F_n(X)$ for small values of n; this was done using the relation (3.4) between the roots and the Gaussian periods. The computations indicated that the 5-cycle $\sigma = (12345)$ generates the Galois group. This is moreover the only 5-cycle yielding the correct absolute value $\sqrt{p}$ of the Gaussian sums $\tau(\chi)$ in (4.6).

Now let θ be a root of $F_n(X)$. Since the splitting field K is of degree 5 over $\mathbf{Q}$, the six elements $1, \theta, \theta^2, \sigma(\theta), \theta\sigma(\theta), \theta^2\sigma(\theta)$ are linearly dependent. This shows that $\sigma(\theta)$ can be expressed as a quotient of two quadratic polynomials in θ. Since the same is true for all conjugates of θ, we obtained a system of equations that we solved numerically for small values of n. It was then easy to guess the general rule.

From now on we will assume that $n \in \mathbf{Z}$ is such that $p = n^4+5n^3+15n^2+25n+25$ is a prime number; this clearly implies that p is congruent to 1 mod 5. In this case, there is another way to see that the roots of $F_n(X)$ generate a cyclic extension of $\mathbf{Q}$. Emma Lehmer gives in [7] an explicit description of the roots of $F_n(X)$: For a coset C of the subgroup $((\mathbf{Z}/p\mathbf{Z})^*)^5$ in $(\mathbf{Z}/p\mathbf{Z})^*$, the Gaussian period η_C is given by

$$\eta_C = \sum_{x \in C} e^{2\pi i x/p}. \tag{3.3}$$

The roots of $F_n(X)$ will be denoted by θ_C; they are given by

$$\theta_C = \left(\frac{n}{5}\right)\eta_C + \left(\left(\frac{n}{5}\right) - n^2\right)/5, \tag{3.4}$$

where $(\frac{n}{5})$ denotes the Legendre symbol modulo 5.

The Galois group of $\mathbf{Q}(\zeta_p)$ is canonically isomorphic to $(\mathbf{Z}/p\mathbf{Z})^*$, and the η_C are in the field of $((\mathbf{Z}/p\mathbf{Z})^*)^5$-invariants, which is of degree 5 over $\mathbf{Q}$. So, from this description of the zeros of $F_n(X)$ it follows at once that K, the splitting field of $F_n(X)$, is the unique quintic subfield of $\mathbf{Q}(\zeta_p)$. As in the previous section, we fix an embedding $K \subset \mathbf{R}$. When viewing the zeros θ_C of $F_n(X)$ in K as elements in $\mathbf{R}$, we denote them, as in Lemma (3.1), by θ_i, where the index is to be taken modulo 5. Let G be the Galois group of K over $\mathbf{Q}$ and let σ denote the generator of G that corresponds with the 5-cycle mentioned above.

Since $F_n(0) = 1$, the zeros of $F_n(X)$ are *units* in the ring of integers O_K of K. We will now show that these zeros generate the group O_K^*.

(3.5) THEOREM. *Let $p = n^4+5n^3+15n^2+25n+25$ be prime and let $F_n(X) \in \mathbf{Z}[X]$ be as above. The zeros of $F_n(X)$ generate the unit group O_K^* of the quintic subfield K of $\mathbf{Q}(\zeta_p)$.*

The regulator R_K equals $R = |\det(\log|\theta_{i+j}|)_{1\le i,j\le 4}|$.

Proof. Since the product of the zeros of $F_n(X)$ is equal to $-F_n(0) = -1$, we see that the group generated by the zeros contains -1. Let U denote the group of units generated by the zeros modulo $\{1,-1\}$. It suffices to show that U is equal to $O_K^*/\{1,-1\}$.

We prove this in three steps:

Step 1. *If $|n+1| \ge 20$, then the index $i_\theta = [O_K^*/\{1,-1\}: U]$ is less than* 11.

The index i_θ is equal to R/R_K. We will compare $R = |\det(\log|\theta_{i+j}|)_{1\le i,j\le 4}|$ with R_K, the regulator of K. First we estimate R. By [15, Lemma 5.26] we have that

$$R = \frac{1}{5}\prod_{\chi\neq 1}\sum_{\sigma\in G}\chi(\sigma)\log|\sigma(\theta_1)|,$$

where the product runs over the nontrivial characters of G. From this formula we obtain

$$R = \frac{1}{5}\prod_{\substack{\varsigma^5=1\\ \varsigma\neq 1}}(\log|\theta_1| + \varsigma\log|\theta_2| + \varsigma^2\log|\theta_3| + \varsigma^3\log|\theta_4| + \varsigma^4\log|\theta_5|),$$

and since $|n+1| \geq 20$, it follows from Lemma (3.1) that

$$R = \frac{1}{5}\log^4|n+1| \prod_{\substack{\zeta^5=1 \\ \zeta \neq 1}} (2+\zeta-3\zeta^2+\zeta^3-\zeta^4+\varepsilon_\zeta),$$

where $|\varepsilon_\zeta| < 1/2\log|n+1|$. From this we get

$$R \leq \left(71 + \frac{36}{\log|n+1|}\right)\log^4|n+1|. \tag{3.6}$$

We obtain, on the other hand, from Corollary (2.7) that

$$R_K \geq \frac{1}{25}\log^4\left(\frac{p}{2}\right)$$

and hence, since $i_\theta = [O_K^*/\{1,-1\}: U] = R/R_K$, that

$$i_\theta \leq \frac{25R}{\log^4(p/2)}. \tag{3.7}$$

Writing $p = n^4+5n^3+15n^2+25n+25$ and eliminating R from (3.6) and (3.7) gives an upper bound for i_θ in terms of n, which is easily seen to be less than 11 when $|n+1| \geq 20$.

Step 2. *The index* $i_\theta = [O_K^*/\{1,-1\}: U]$ *is not divisible by* 5.

Both U and $O_K^*/\{1,-1\}$ are $\mathbf{Z}[G]$-modules which are annihilated by the G-norm N, and therefore $\mathbf{Z}[\zeta_5]$-modules. Here we identify the ring $\mathbf{Z}[G]/(N)$ with the Dedekind domain $\mathbf{Z}[\zeta_5]$ as we did in Section 2. By Corollary (2.6) we can find a unit $\varepsilon \in O_K^*$ that generates $O_K^*/\{1,-1\}$ as a $\mathbf{Z}[\zeta_5]$-module. Fixing one zero θ of $F_n(X)$, we have that $U = \mathbf{Z}[\zeta_5]\cdot\theta$. Since $\theta \in O_K^*$, there is $\alpha \in \mathbf{Z}[\zeta_5]$ such that $\theta = \pm\alpha\cdot\varepsilon$. The quotient group $O_K^*/\{1,-1\}U$ is therefore, as a $\mathbf{Z}[\zeta_5]$-module, isomorphic to $\mathbf{Z}[\zeta_5]/\alpha\mathbf{Z}[\zeta_5]$, and we have

$$i_\theta = [O_K^*/\{1,-1\}: U] = \operatorname*{Norm}_{\mathbf{Z}[\zeta_5]/\mathbf{Z}}(\alpha). \tag{3.8}$$

Up to a unit, the only element α in $\mathbf{Z}[\zeta_5]$ of norm 5 is $1-\zeta_5$. Therefore, if 5 divides i_θ, we have that $1-\zeta_5$ divides α, and we see that $\theta = (1-\zeta_5)\cdot\eta = \pm\eta/\sigma(\eta)$ for some $\eta \in O_K^*$. Let $\mathbf{p}$ denote the prime ideal over p in O_K; since p is totally ramified in the extension K over $\mathbf{Q}$, the Galois group G acts trivially modulo $\mathbf{p}$. It follows that $\theta \equiv \pm 1 \pmod{\mathbf{p}}$ and hence that

$$F_n(X) \equiv (X \pm 1)^5 \bmod p,$$

which is easily seen to be impossible.

Step 3. *The index* $i_\theta = [O_K^*/\{1,-1\}: U]$ *is equal to one.*

In Step 1 we showed that $i_\theta < 11$ whenever $|n+1| \geq 20$. For the remaining n for which $p = n^4+5n^3+15n^2+25n+25$ is prime, we replace the estimate (3.6) by an accurate approximation of R; the approximations of R are given in Table (4.7). It follows readily from (3.7) that $i_\theta < 11$ for all primes, except for $p = 31$ or 101. In these cases one merely obtains that $i_\theta < 16$.

Formula (3.8) gives restrictions on the possible values of i_θ: If q is the largest power of a prime dividing i_θ, then $q \equiv 0$ or $1 \pmod 5$. Since, by Step 2, the index i_θ is not divisible by 5, it follows at once that $i_\theta = 1$ when p is not 31 or 101. For the remaining two values of p we only obtain that $i_\theta = 1$ or 11.

One can show that $i_\theta \neq 11$ as follows: Let q be a prime number which is 1 (mod 11) and which splits in K. Let $W = (O_K/qO_K)^*/((O_K/qO_K)^*)^{11}$. As a G-module, W is isomorphic to $\mathbf{F}_{11}[G]$, and the image of O_K^* in W is contained in the augmentation ideal $\{\sum_{\sigma\in G} \alpha_\sigma \cdot [\sigma] \in \mathbf{F}_{11}[G]\colon \sum_{\sigma\in G} \alpha_\sigma = 0\}$, which is a vector space of dimension 4 over $\mathbf{F}_{11}$. One can easily check whether or not the group generated by the zeros of $F_n(X)$ mod q in W is equal to the augmentation ideal by computing a 4 by 4 determinant. If the determinant is not congruent to 0 mod 11, one concludes that the image of O_K^* in W is generated by the zeros of $F_n(X)$ modulo 11th powers and that 11 cannot divide i_θ.

For $p = 31$ we took the prime $q = 67$ and for $p = 101$ we used $q = 1277$. In both cases a little computation allowed us to conclude that $i_\theta \neq 11$.

This completes the proof of Theorem (3.5). □

4. Numerical Examples. We computed for small integral values of n the class numbers of the quintic subfields of $\mathbf{Q}(\zeta_p)$, where $p = n^4 + 5n^3 + 15n^2 + 25n + 25$ is a prime less than 10^7. In this section we explain how the computations were performed. We obtain several examples of small primes p for which $h(\mathbf{Q}(\zeta_p)^+)$ exceeds p. Another consequence of our computations is the following result, which shows that the class number of $\mathbf{Q}(\zeta_p)^+$ may be divisible by primes exceeding p.

(4.1) THEOREM. *Let p be the prime* 641491. *The class number of $\mathbf{Q}(\zeta_p)^+$ is divisible by the prime $q = 1566401$.*

Proof. As one reads off Table (4.7), the subfield K of degree 5 of $\mathbf{Q}(\zeta_p)^+$ for $p = 641491$ has class number equal to $q = 1566401$, which is a prime number. By class field theory, the norm map from the class group of $\mathbf{Q}(\zeta_p)^+$ to the class group of K is surjective, and it follows that q divides $h(\mathbf{Q}(\zeta_p)^+)$. This proves the theorem. □

In the sequel we let K denote the quintic subfield of $\mathbf{Q}(\zeta_p)^+$, where $p = n^4 + 5n^3 + 15n^2 + 25n + 25$ is as above. Let h_K denote the class number of K and let R_K denote its regulator. From Dirichlet's class number formula we obtain

$$h_K R_K = \frac{1}{16} \prod_{\chi\neq 1} \sqrt{p} L(1,\chi),$$

where the product runs over the nontrivial characters $\chi\colon \mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{C}^*$ and $L(1,\chi)$ denotes the value of Dirichlet's L-series $L(s,\chi)$ associated with χ at $s = 1$.

By Theorem (3.5) we know that the unit group of the ring of integers of K is generated by the zeros of Emma Lehmer's polynomial. So $R_K = R$, where R is the regulator of Emma Lehmer's units. We have

$$h_K = \frac{1}{16R} \prod_{\chi\neq 1} \sqrt{p} L(1,\chi), \tag{4.2}$$

which is the formula we used to compute the class numbers h_K. We evaluated an accurate approximation of the right-hand side and then used the fact that the class number is an integer to obtain h_K itself. The regulator R was readily obtained from the zeros of the polynomial $F_n(X)$, while these zeros were obtained with high accuracy using Newton's approximation method and the transformation formula (3.2). Since the size of $\sqrt{p}L(1,\chi)$ is roughly equal to $\sqrt{p}$ and since there are four

nontrivial characters of $\mathrm{Gal}(K/\mathbf{Q})$, it follows from (4.2) and the fact R_K is only $O(\log^4 p)$ that we must evaluate each $\sqrt{p}L(1,\chi)$ with an accuracy at least $\varepsilon p^{-1.5}$ to obtain the class number h_K with an error less than ε.

To approximate the quantities $\sqrt{p}L(1,\chi)$, the following formulas, which can be deduced from the functional equation of $L(s,\chi)$ as in [16], were used:

$$\sqrt{p}L(1,\chi) = \frac{\tau(\chi)}{\sqrt{p}} \sum_{n=1}^{\infty} \chi^{-1}(n) \int_{n^2\pi/p}^{\infty} \frac{e^{-t}}{t}\, dt + \sqrt{\frac{p}{\pi}} \sum_{n=1}^{\infty} \chi(n) \frac{2}{n} \int_{n\sqrt{\pi/p}}^{\infty} e^{-t^2}\, dt, \tag{4.3}$$

where $\tau(\chi)$ denotes the Gaussian sum

$$\tau(\chi) = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} \chi(x) e^{2\pi i x/p}, \tag{4.4}$$

which is in the field $K(\zeta_5)$, an extension of degree 20 over $\mathbf{Q}$. Replacing the infinite sums in this formula by sums up to N, one introduces, as in [16], an error not exceeding

$$p^2 \pi^{-2} N^{-3} e^{-(\pi/p)N^2}.$$

The integrals were evaluated using the following power series and continued fraction expansions (cf. [1, 5.1.11, 5.1.22, 7.1.5 and 7.1.14]):

$$\begin{aligned} \int_z^{\infty} \frac{e^{-t}}{t}\, dt &= -\gamma - \log(z) - \sum_{n=1}^{\infty} \frac{(-1)^n z^n}{n \cdot n!} \\ &= e^{-z} \left(\frac{1}{z+} \frac{1}{1+} \frac{1}{z+} \frac{2}{1+} \frac{2}{z+} \frac{3}{1+} \frac{3}{z+} \cdots \right) \end{aligned}$$

and

$$\begin{aligned} \int_z^{\infty} e^{-t^2}\, dt &= \frac{\sqrt{\pi}}{2} - \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n+1}}{n!(2n+1)} \\ &= \frac{1}{2} e^{-z^2} \left(\frac{1}{z+} \frac{\frac{1}{2}}{z+} \frac{1}{z+} \frac{\frac{3}{2}}{z+} \frac{2}{z+} \frac{\frac{5}{2}}{z+} \cdots \right) \end{aligned}$$

(here γ denotes Euler's constant).

The Taylor series were used for $0 < z < 2.2$, while the continued fraction expansions were used whenever $z \geq 2.2$. Both approximations converge exponentially rapidly. We did not use Formula (4.4) to evaluate the Gaussian sums $\tau(\chi)$ in (4.3); this would involve a lengthy summation over the residue classes modulo p. We used Emma Lehmer's polynomial instead: We have that

$$\tau(\chi) = \sum_C \chi(C) \eta_C, \tag{4.5}$$

where the η_C denote the Gaussian periods as in (3.3) and hence by (3.4)

$$\tau(\chi) = \left(\frac{n}{5}\right) \sum_C \chi(C) \theta_C, \tag{4.6}$$

where the summations run over the five cosets C of $((\mathbf{Z}/p\mathbf{Z})^*)^5$. Using (4.6), the Gaussian sums were evaluated very quickly and accurately.

As in [11], the following complication arises: without excessive computations, we cannot establish which zero in $\mathbf{R}$ of Emma Lehmer's polynomial corresponds to a

given coset C, and neither can we determine which Gaussian sum $\tau(\chi)$ corresponds to a given character $\chi\colon \mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{C}^*$. In fact, the Gaussian sum, which is an element of the field $K(\zeta_5)$, can only relatively easily be determined up to Galois conjugacy. This leaves us with twenty possibilities for the Gaussian sum in (4.3). In all cases considered, only one of these gave rise to an approximation of h_K sufficiently close to an integer.

Our computations, which were all done on a programmable desk calculator, yielded the following results:

(4.7) **Table.**

n	p	R	h
$-1, -2$	11	1.635694126	1
-3	31	30.36957651	1
1	71	70.61067564	1
-4	101	119.5256946	1
2	191	185.4390339	11
-6	631	478.3833457	11
4	941	580.2796987	16
-9	3931	1307.037778	$256 = 16^2$
7	5051	1436.693208	1451
8	7841	1763.648314	421
-11	9551	1964.717615	541
-18	80251	4524.280104	$37631 = 11^2 \cdot 311$
16	90281	4674.905564	19301
-21	154291	5663.923110	$108691 = 11 \cdot 41 \cdot 241$
-22	187751	6044.688165	$76901 = 11 \cdot 6991$
23	349211	7335.333173	$186091 = 71 \cdot 2621$
26	555671	8467.444092	$721151 = 661 \cdot 1091$
27	641491	8842.507837	1566401
-31	788231	9441.527007	$1217821 = 11 \cdot 110711$
-32	899321	9813.061662	$798256 = 16 \cdot 49891$
-36	1464901	11284.06551	$4628591 = 11 \cdot 420781$
-37	1640531	11647.87253	1636721
-42	2766691	13442.41069	$20599841 = 31 \cdot 664511$
41	3196631	13935.71793	$8088176 = 16 \cdot 505511$
51	7468771	17379.48515	$28850896 = 16 \cdot 521 \cdot 3461$
-54	7758151	17582.83476	$37142851 = 101 \cdot 367751$

In the table we list in the first column integers n for which $p = n^4 + 5n^3 + 15n^2 + 25n + 25$ is a prime less than 10^7. The prime p is listed in the second column. In the third column the regulator of the quintic subfield of $\mathbf{Q}(\zeta_p)$ is listed, and in the last column the class number of this field is given. The quintic fields of conductor 11, 31, 71 and 101 were already known to have class number one [5], [14]. The class numbers of the quintic subfields of $\mathbf{Q}(\zeta_p)^+$ for $p = 191$ and 631 were already shown to be equal to 11 by G. Gras and M.-N. Gras in [5].

Appendix. A Characterization of the Simplest Quadratic, Cubic, and Quartic Fields. Emma Lehmer [7] has shown that in the "simplest" quadratic, cubic, and quartic fields it is possible to obtain units by translating the Gaussian periods by integers. We show that this property characterizes these fields.

THEOREM. *Let $d = 2, 3,$ or 4. Let $p \equiv 1 \pmod{2d}$ be prime and let K be the subfield of $\mathbf{Q}(\zeta_p)$ of degree d over $\mathbf{Q}$. Suppose there is a (respectively quadratic, cubic or quartic) Gaussian period η and an integer k such that $\eta - k$ is a unit of K.*

(a) *If $d = 2$, then $p = n^2 + 4$ for some $n \in \mathbf{Z}$.*

(b) *If $d = 3$, then $p = n^2 + 3n + 9$ for some $n \in \mathbf{Z}$.*

(c) *If $d = 4$ and $\eta - k$ has norm (from K to $\mathbf{Q}$) equal to $+1$, then $p = n^2 + 16$ for some $n \in \mathbf{Z}$.*

We note that these are exactly the representations of p needed for K to be "simplest" quadratic, cubic, or quartic, defined by the polynomials

$$\begin{aligned} &X^2 - nX - 1 && (d = 2),\\ &X^3 - nX^2 - (n+3)X - 1 && (d = 3),\\ &X^4 - nX^3 - 6X^2 + nX + 1 && (d = 4). \end{aligned}$$

Remarks. For $p = 401$ and $d = 4$, the unit $\eta - 2$ has norm -1, so the extra assumption in (c) is needed. However, we do not know of any other examples of this type.

(Note added in proof: Don Zagier has pointed out that the question can be reduced to the single Diophantine equation

$$4X^2Y^2 - 1 = (Y^2 - YZ - X^2)(Y^2 - X^2).$$

Integral solutions for which $p = 16X^2 + Z^2$ is prime correspond to primes for which $\eta - k$, for some k, has norm -1. It seems possible that $(x, y, z) = (-5, -2, 1)$ and $(1, -2, 1)$ are the only solutions. They correspond to $p = 17$ (which is already covered by (c)) and $p = 401$.)

Calculations seem to indicate that if $d = 5$ then K must be one of Emma Lehmer's quintic fields, but we have been unable to prove this.

Proof of the Theorem. (a) The quadratic periods are roots of

$$X^2 + X + \frac{1-p}{4}.$$

If $\eta - k$ is a unit, then $k^2 + k + (1-p)/4 = \pm 1$, hence $p = (2k+1)^2 \pm 4$. The result follows easily.

(b) Write $4p = L^2 + 27M^2$ with $L \equiv 1 \pmod 3$. The cubic periods are the roots of

$$F_3(X) = X^3 + X^2 - \frac{(p-1)}{3}X - \frac{(L+3)p - 1}{27}.$$

Our assumption is that $F_3(k) = \pm 1$. Letting $z = 3k + 1$, we obtain $p(3z + L) = z^3 \pm 27$.

Consider the "minus" case: $p(3z + L) = z^3 - 27 = (z-3)(z^2 + 3z + 9)$. Suppose that p divides $z^2 + 3z + 9$, so $pa = z^2 + 3z + 9$ with $a \in \mathbf{Z}$. Then $3z + L = a(z - 3)$ and $(a - 3)z = L + 3a$. If $a = 1$, we are done. Since $z^2 + 3z + 9$ is odd, a must be odd. If $a = 3$, then $3 \mid z$ and hence $3 \mid p$, which is not possible. Therefore, $a \geq 5$.

The equation $z^2 + 3z + 9 = pa$ may be rewritten as

$$\left(\frac{L+3a}{a-3}\right)^2 + 3\left(\frac{L+3a}{a-3}\right) + 9 = \frac{L^2+27M^2}{4}a.$$

This becomes

$$(a-1)^2(a-4)L^2 + 36(1-a)L + 27(M^2a(a-3)^2 - 4a^2 + 12a - 12) = 0.$$

This equation, regarded as a quadratic polynomial in L, must have nonnegative discriminant, so

$$12(a-1)^2 \geq (a-1)^2(a-4)(M^2a(a-3)^2 - 4a^2 + 12a - 12),$$

hence

$$4(a-1) \geq a(a-4)M^2.$$

Since $a - 1 < a(a-4)$ for $a \geq 5$, we have $M^2 < 4$. Therefore, $M^2 = 1$ and $p = (L^2+27)/4 = n^2 + 3n + 9$ with $n = (L-3)/2$. If $p \mid (z-3)$, then $|z| \geq p - 3$, since $z - 3 = 3k - 2 \neq 0$. Therefore, $|L| < \sqrt{p} < |z| + 3$, so $|z| + 3 > p = (z^3 - 27)/(3z + L) \geq (|z|^3 - 27)/(4|z| + 3)$. This implies that $|z| < 7$, so $p < 10$, and hence that $p = 7$. But $7 = n^2 + 3n + 9$ with $n = -1$, so we are done.

The "plus" case is handled similarly.

(c) Write $p = A^2 + 16B^2$ with $A \equiv 1 \pmod 4$. The quartic periods are the roots of

$$F_4(X) = X^4 + X^3 - \frac{3(p-1)}{8}X^2 - \frac{3p - 2pA - 1}{16}X + \frac{(p-1)^2 - 4p(A-1)^2}{256}.$$

We have $F_4(k) = 1$. Letting $z = 4k + 1$, we obtain

$$p(6z^2 - 8Az - p + 4A^2) = (z^2 + 16)(z^2 - 16).$$

Suppose first that p divides $z^2 + 16$, so $pa = z^2 + 16$ with $a \in \mathbf{Z}$. Then

$$a(z^2 - 16) = 6z^2 - 8Az - p + 4A^2$$

and

$$a(z^2 - 16) - 2z^2 + p = 4(A - z)^2.$$

Let $\alpha = a - 1$ and replace z^2 by $pa - 16 = p\alpha + p - 16$:

$$\alpha(p\alpha - 32) = (2(A - z))^2.$$

If $2(A - z) = 0$, then $\alpha = 0$, so $a = 1$ and $p = z^2 + 16$ as desired. Therefore, assume that $2(A - z) \neq 0$. Since $z = 4k + 1$ is odd and $p \equiv 1 \pmod 8$, we have $a \equiv 1 \pmod 8$, hence $\alpha \equiv 0 \pmod 8$. Note that also $\alpha \geq 0$. Clearly, $\gcd(\alpha, p\alpha - 32)$ is a power of 2, so we have two cases:

(i) $\alpha = 2\delta^2$, $p\alpha - 32 = 2\varepsilon^2$ with $\delta, \varepsilon \in \mathbf{Z}$.

We have $p\delta^2 = \varepsilon^2 + 16$, so 3 does not divide δ and $\alpha \equiv 2 \pmod 3$. Therefore $3 \mid a$, so $z^2 + 16 \equiv 0 \pmod 3$, which is impossible.

(ii) $\alpha = \delta^2$, $p\alpha - 32 = \varepsilon^2$ with $\delta, \varepsilon \in \mathbf{Z}$.

Let 2^{2g} $(g \geq 2)$ be the highest power of 2 dividing α. Then $2^{4g} \parallel p\alpha^2$ and $2^{2g+5} \parallel 32\alpha$. Since the 2-adic valuation of $(2(A - z))^2 = p\alpha^2 - 32\alpha$ is even, we must have that $4g \leq 2g + 5$. Therefore $g \leq 2$, so $g = 2$. Let $\alpha = 16\beta$ with β odd. Then $\beta(p\beta - 2)$ is a square, which is impossible modulo 8.

It remains to consider the possibility that p divides $z^2 - 16 = (z+4)(z-4)$. Since $z \pm 4 = 4k + 1 \pm 4 \neq 0$, we have $|z| \geq p - 4$. Also $|A| \leq \sqrt{p} \leq (|z|+4)^{1/2}$. By inequalities similar to those used for the cubic case we obtain $|z| \leq 12$, so $p \leq 16$. Since $p \equiv 1 \pmod 8$, this is impossible. This completes the proof. □

Dipartimento di Matematica
Università di Pisa
Via Buonnaroti 2
56100 Pisa, Italy

Department of Mathematics
University of Maryland
College Park, Maryland 20742

1. M. ABRAMOWITZ & I. A. STEGUN, *Handbook of Mathematical Functions*, Dover, New York, 1964.

2. J. W. S. CASSELS, *An Introduction to the Geometry of Numbers*, Springer-Verlag, New York, 1971.

3. T. W. CUSICK, "Lower bounds for regulators," in *Number Theory*, Noordwijkerhout 1983, Proceedings of the Journées Arithmétiques, Lecture Notes in Math., vol. 1068, Springer-Verlag, New York, 1984.

4. G. CORNELL & L. C. WASHINGTON, "Class numbers of cyclotomic fields," *J. Number Theory*, v. 21, 1985, pp. 260–274.

5. G. GRAS & M.-N. GRAS, "Calcul du nombre de classes et des unités des extensions abéliennes réelles de **Q**," *Bull. Sci. Math.*, v. 101, 1977, pp. 97–129.

6. J. C. LAGARIAS, H. W. LENSTRA & C. P. SCHNORR, "Korkine-Zolotarev bases and successive minima of a lattice and its reciprocal lattice," submitted to *Combinatorica*.

7. E. LEHMER, "Connection between Gaussian periods and cyclic units," *Math. Comp.*, v. 50, 1988, pp. 535–541.

8. C. MOSER, "Nombre de classes d'une extension cyclique réelle de **Q**, de degré 4 ou 6 et de conducteur premier," *Math. Nachr.*, v. 102, 1981, pp. 45–52.

9. C. MOSER & J.-J. PAYAN, "Majoration du nombre de classes d'un corps cubique cyclique de conducteur premier," *J. Math. Soc. Japan*, v. 33, 1981, pp. 701–706.

10. M. POHST, "Regulatorabschätzungen für total reelle algebraische Zahlkörper," *J. Number Theory*, v. 9, 1977, pp. 459–492.

11. E. SEAH, L. C. WASHINGTON & H. C. WILLIAMS, "The calculation of a large cubic class number with an application to real cyclotomic fields," *Math. Comp.*, v. 41, 1983, pp. 303–305.

12. D. SHANKS, *Solved and Unsolved Problems in Number Theory*, 3rd ed., Chelsea, New York, 1985.

13. D. SHANKS, "The simplest cubic fields," *Math. Comp.*, v. 28, 1974, pp. 1137–1152.

14. F. VAN DER LINDEN, "Class numbers of real cyclotomic fields," *Math. Comp.*, v. 39, 1982, pp. 693–707.

15. L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, Graduate Texts in Math., vol. 83, Springer-Verlag, New York, 1982.

16. H. C. WILLIAMS & J. BROERE, "A computational technique for evaluating $L(1, \chi)$ and the class number of a real quadratic field," *Math. Comp.*, v. 30, 1976, pp. 887–893.