A result of Lemmermeyer on class numbers

Paul Monsky

Brandeis University, Waltham MA 02454-9110, USA
monsky@brandeis.edu

Abstract

I present Franz Lemmermeyer's proof that if p is a prime $\equiv 9\ (16)$ then the class number of $\mathbb{Q}\left(p^{\frac{1}{4}}\right)$ is $\equiv 2\ (4)$.

Let p be a prime $\equiv 1\ (4)$. Then the class number of $k = \mathbb{Q}\left(\sqrt{p}\right)$ is odd, and the fundamental unit of $\mathcal{O}_k$ has norm -1; this result in essence goes back to Gauss. Years ago I conjectured that if $p \equiv 9\ (16)$ then the class number of $\mathbb{Q}\left(p^{\frac{1}{4}}\right)$ is $\equiv 2\ (4)$. (Parry [2] had previously shown that it's even, and that when 2 is not a fourth power in $\mathbb{Z}/p$ it's $\equiv 2\ (4)$.) I gave a proof of my conjecture assuming that the elliptic curve $y^2 = x^3 - px$ has positive rank, as the Birch Swinnerton-Dyer conjecture predicts.

Recently I asked on Mathoverflow whether the elliptic curve assumption could be eliminated. Franz Lemmermeyer responded with an unconditional proof that starts with Gauss' result and continues with two applications of the ambiguous class number formula. His very nice argument deserves wider circulation, so I'm writing it up here.

Theorem 1. If $p \equiv 1\ (8)$, $\mathbb{Q}\left(p^{\frac{1}{4}}\right)$ has even class number.

Proof (Lemmermeyer). Let F be the quartic subfield of $\mathbb{Q}(\mu_p)$. Then $F \supset k = \mathbb{Q}(\sqrt{p})$. Since $p \equiv 1\ (8)$, the infinite prime of $\mathbb{Q}$ is unramified in F, and the only prime of $\mathbb{Q}$ that ramifies in F is (p).

Since $F\left(p^{\frac{1}{4}}\right)$ is the compositum of $\mathbb{Q}\left(p^{\frac{1}{4}}\right)$ and F it is a Galois extension of k with Galois group $\mathbb{Z}/2 \times \mathbb{Z}/2$. Since $p \neq 2$, the ramification is tame, and the prime above p cannot ramify totally in the extension. It follows that $\left(p^{\frac{1}{4}}\right)$ cannot ramify from $\mathbb{Q}\left(p^{\frac{1}{4}}\right)$ to $F\left(p^{\frac{1}{4}}\right)$. So $\mathbb{Q}\left(p^{\frac{1}{4}}\right)$ has an everywhere unramified extension, $F\left(p^{\frac{1}{4}}\right)$, of degree 2, and class-field theory gives the result. $\square$

Corollary 2. Suppose $p \equiv 1 \pmod 8$ and F is as in Theorem 1. If $F\left(p^{\frac{1}{4}}\right)$ has odd class number then the class number of $\mathbb{Q}\left(p^{\frac{1}{4}}\right)$ is $\equiv 2 \pmod 4$.

Proof. Suppose on the contrary that 4 divides the class number. Then $\mathbb{Q}\left(p^{\frac{1}{4}}\right)$ admits an unramified abelian extension of degree 4. Translating by F we get a degree 2 unramified extension of $F\left(p^{\frac{1}{4}}\right)$, contradicting the odd class number assumption. □

Lemma 3. The F of Theorem 1 is the unique degree 2 extension of k unramified outside of $(\sqrt{p})$.

Proof. Let F' be a second such extension. Since the class number of k is odd, k has no unramified extensions of degree 2 and $(\sqrt{p})$ must ramify in F'. There is a third quadratic extension, F'', of k contained in FF' and the same argument shows that $(\sqrt{p})$ ramifies in F''. So $(\sqrt{p})$ ramifies totally in FF', contradicting tameness. □

Theorem 4. If $p \equiv 1 \pmod 8$ and $\epsilon > 0$ is a unit of norm -1 in the ring of integers of k, then $F = k\left(\sqrt{\epsilon\sqrt{p}}\right)$.

Proof. $\epsilon\sqrt{p}$ and its $\mathbb{Q}$-conjugate $\epsilon^{-1}\sqrt{p}$ are both > 0. So neither of the infinite primes of k ramify in $k\left(\sqrt{\epsilon\sqrt{p}}\right)$. If $r^2 - sp^2 = -4$, r and s cannot both be odd. It follows that $\epsilon = a + b\sqrt{p}$ with a and b integers. Also, $0 < \epsilon + \epsilon^{-1} = 2b\sqrt{p}$, and $b > 0$. Now $a^2 - pb^2 = -1$. Since $pb^2 \equiv 1 \pmod 8$, 8 divides a^2 and 4 divides a. Furthermore every prime that divides b divides $a^2 + 1$, and so is $\equiv 1 \pmod 4$. Since $b > 0$, $b \equiv 1 \pmod 4$. Let P be a prime of $\mathcal{O}_k$ lying over (2). Then in the P-completion of $\mathcal{O}_k$, $\epsilon\sqrt{p} = bp + a\sqrt{p} \equiv 1 \pmod 4$. So P does not ramify in $k\left(\sqrt{\epsilon\sqrt{p}}\right)$. It follows that the only prime that can ramify in $k\left(\sqrt{\epsilon\sqrt{p}}\right)$ is $(\sqrt{p})$, and we apply Lemma 3. □

Corollary 5. $F\left(p^{\frac{1}{4}}\right) = F(\sqrt{\epsilon})$.

Proof. Both fields are degree 2 extensions of F. Since $\sqrt{\epsilon\sqrt{p}}$ is in F, $\sqrt{\epsilon}$ is in $F\left(p^{\frac{1}{4}}\right)$. □

We now give the idea of Lemmermeyer's proof. The class number of k is known to be odd. Lemmermeyer uses the ambiguous class number formula to deduce that $k(\sqrt{\epsilon})$ has odd class number. Then assuming $p \equiv 9 \pmod{16}$ he uses it once more to show that $F(\sqrt{\epsilon})$ has odd class number. Corollaries 5 and 2 complete the proof.

We introduce some notation. Suppose $L \supset K$ is a degree 2 extension of number fields with Galois group $G = \{\mathrm{id}, \sigma\}$. U_K consists of the units of $\mathcal{O}_K$ while h_L and h_K are the class numbers of L and K. C_L is the class group of L, while C_L^G, the ambiguous class group, consists of the elements of C_L fixed by σ. The following result is contained in Theorem 4.1 of [1].

Theorem 6. $|C_L^G| = h_K \cdot (2^{t-1}/j)$ where t is the number of primes of K, finite or infinite, that ramify in L, while j is the index in U_K of the subgroup consisting of elements that are norms from L. (Since this subgroup contains U_K^2, j is a power of 2.) Furthermore, if $|C_L^G|$ is odd, h_L is odd.

Lemma 7. Just two primes of k ramify in $k(\sqrt{\epsilon})$.

Proof. $\epsilon > 0$, and the $\mathbb{Q}$-conjugate $-\epsilon^{-1}$ of ϵ is < 0. So one of the two infinite primes ramifies. Also $\epsilon = a + b\sqrt{p}$ with $a \equiv 0 \ (4)$, $b \equiv 1 \ (4)$. So $\epsilon \equiv 1 \ (4)$ in the completion of $\mathcal{O}_k$ at $\left(2, \frac{1-\sqrt{p}}{2}\right)$, and $\epsilon \equiv -1 \ (4)$ in the completion of $\mathcal{O}_k$ at $\left(2, \frac{1+\sqrt{p}}{2}\right)$. Finally no other primes can ramify. □

Theorem 8. $k(\sqrt{\epsilon})$ has odd class number.

Proof. Theorem 6 and Lemma 7 show that the ambiguous class number for the extension $k(\sqrt{\epsilon}) \supset k$ is $\frac{2h_k}{j}$. So it suffices to show that $j > 1$. Now -1 is in U_k. But as we saw above there is an infinite prime of k ramifying in $k(\sqrt{\epsilon})$, and -1 evidently is not a local norm at that prime. □

Lemma 9. ϵ represents a primitive fourth root of unity in $\mathcal{O}_k/(\sqrt{p}) = \mathbb{Z}/p$. Furthermore the prime $(\sqrt{p})$ of k splits in $k(\sqrt{\epsilon})$.

Proof. $\epsilon = a + b\sqrt{p}$ with $a^2 - pb^2 = -1$. So mod $\sqrt{p}$, $\epsilon^2 \equiv a^2 \equiv -1$, giving the first result. Since $p \equiv 1 \ (8)$, any fourth root of unity in $(\mathbb{Z}/p)^*$ is a square, and the second result follows. □

Theorem 10 (Lemmermeyer)**.** Suppose $p \equiv 9 \ (16)$. Then the ambiguous class number for the extension $F(\sqrt{\epsilon}) \supset k(\sqrt{\epsilon})$ is odd. So $F(\sqrt{\epsilon})$ has odd class number, and Corollaries 5 and 2 show that the class number of $\mathbb{Q}\left(p^{\frac{1}{4}}\right)$ is $\equiv 2$ (4).

Proof. The only primes that can ramify are primes whose restriction to k ramifies in F. In view of Lemma 9 the only possibilities are the 2 primes of $k(\sqrt{\epsilon})$ lying over $(\sqrt{p})$; it's easy to see that they both ramify in $F(\sqrt{\epsilon})$. Furthermore $\sqrt{\epsilon}$ is not a local norm at either of these primes. (Because the prime ramifies it suffices to show that the image of $\sqrt{\epsilon}$ in the residue class field is not a square. But Lemma 9 shows that this image is a primitive eighth root of unity in $(\mathbb{Z}/p)^*$. And $p \not\equiv 1\ (16)$. So in our quadratic extension, $t = 2$ and j is even. Since $k(\sqrt{\epsilon})$ has odd class number, Theorem 6 gives the desired result. $\square$

References

[1] Serge Lang, Cyclotomic Fields II (1980), Springer Verlag, New York, Heidelberg, Berlin.

[2] Charles J. Parry, A genus theory for quartic fields, J. Reine Angew. Math. 314 (1980), 40–71.