Primes of the Form $x^2 + 17y^2$

Ben Galin*

July 1, 2006

Following conjectures first given by Fermat, prominent mathematicians such as Euler, Lagrange, Legendre, and Gauss studied primes of the form $x^2 + ny^2$, where n is a fixed positive integer and x and y are any two integers. In this paper we examine the special case of primes of the form $x^2 + 17y^2$. As we shall see, finding necessary and sufficient conditions for primes represented by this form cannot be achieved by elementary genus theory and the theory of quadratic forms. Thus, we will turn to the fascinating theory of Hilbert class fields, where a solution to our question arises as a special case of results on when prime ideals split completely in an Hilbert class field.

We begin with a quick survey of results from the theory of quadratic forms. It is known that quadratic forms can be grouped into equivalence classes, where forms in a given class represent the same numbers. Recall that a primitive positive definite quadratic form $ax^2 + bxy + cy^2$ is said to be *reduced* if it satisfies the following conditions: (i) $|b| \leq a \leq c$, and (ii) if $|b| = a$ or $a = c$ then $b \geq 0$. The usefulness of this definition becomes clear when combined with the following result (see in [1, p. 29]):

Theorem 1. *Let $D < 0$ be fixed. Then the number $h(D)$ of classes of primitive positive definite forms of discriminant D is equal to the number of reduced forms of discriminant D.*

Finding reduced forms of a given discriminant D is a simple finite algorithm. One starts by looking for values of a satisfying $a \leq \sqrt{\frac{-D}{3}}$, then continues by checking values of b of the same parity as D and satisfying conditions (i) and (ii) above. Lastly, the value of c is determined by the values of a, b, and D.

Note that $x^2 + 17y^2$ is a quadratic form of discriminant $D = -68$. Running through the algorithm presented above, we find that the reduced forms of discriminant $D = -68$ are

$$x^2 + 17y^2\,, \qquad 2x^2 + 2xy + 9y^2\,, \tag{1}$$

$$3x^2 + 2xy + 6y^2\,, \text{ and} \qquad 3x^2 - 2xy + 6y^2\,, \tag{2}$$

so that $h(-68) = 4$. We would like to find simple congruence conditions for numbers that are represented by each of the four forms in (1) and (2), and we hope that the congruence condition satisfied by $x^2 + 17y^2$ (the *principal form*) is not also satisfied by any of the other three forms.

Unfortunately, this is not the case. To see why, recall that *genera* are collections of quadratic forms that represent the same numbers modulo D. If a genus consists of more than one class, then a simple congruence condition cannot separate between the classes of the genus. In addition, we have the following theorem (see [1, pp. 54, 59]):

Theorem 2. *Let n be a positive integer. Then every genus of forms of discriminant $-4n$ consists of a single class if and only if whenever $ax^2 + bxy + cy^2$ is a reduced form of discriminant $-4n$, then either $b = 0$, $a = b$, or $a = c$. In addition, all genera consist of the same number of classes.*

In our case, we see that the two reduced forms in (2) do not satisfy $b = 0$, $a = b$, or $a = c$. Thus we can conclude that no genus consists of only one class, and in particular, the principal form $x^2 + 17y^2$ is not the only reduced form in its genus. In fact, it can be shown that the other form in (1), $2x^2 + 2xy + 9y^2$, is in the same genus, called the *principal genus*, as the principal form: both forms are of order less than 2 in the class group, and the principal genus consists of all elements of order 1 or 2.

Our next approach, which will yield a solution, utilizes the theory of Hilbert class fields. We have the following main theorem (in [1, p. 98]):

Theorem 3. *Let $n > 0$ be an integer satisfying the following condition:*

$$n \text{ squarefree, } n \not\equiv 3 \pmod 4\,. \tag{3}$$

Then there is a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ such

that if an odd prime divides neither n nor the discriminant of $f_n(x)$, then

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ and } f_n(x) \equiv 0 \pmod{p} \\ \text{has an integer solution.} \end{cases}$$

Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer α for which $L = K(\alpha)$ is the Hilbert class field *of $K = \mathbb{Q}(\sqrt{-n})$.*

Note that this is indeed a stronger classification than the one presented by the two previous theorems. It is the requirement that $f_n(x) \equiv 0 \pmod{p}$ has an integer solution which allows to separate between classes in the same genus.

For our case, we see that $n = 17$ satisfies the conditions in (3). Hence the theorem applies. Using quadratic reciprocity, the supplementary laws, and the homomorphism of the Lagendre symbol, it is easy to determine when $\left(\frac{-17}{p}\right) = 1$. That is, we want

$$1 = \left(\frac{-17}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{17}\right).$$

But this is the case if and only if (i) $p \equiv 1 \pmod 4$ and $p \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$, or (ii) $p \equiv 3 \pmod 4$ and $p \equiv 3, 5, 6, 7, 10, 11, 12, 14 \pmod{17}$. Put together, we must have $p \equiv 1, 3, 7, 9, 11, 13, 21, 23, 25, 27, 31, 33, 39, 49, 53, 63 \pmod{68}$.

However, finding the polynomial $f_{17}(x)$ is not as trivial. Knowledge of the minimal polynomial is equivalent to knowledge of the Hilbert class field of $K = \mathbb{Q}(\sqrt{-17})$. That is, we need to find the primitive element α of the Hilbert class field L of K. In general, one can find this generator from properties of complex multiplication, but this is out of the scope of this paper. Instead, we will find the polynomial $f_{17}(x)$ as a consequence of proving the following proposition.

Proposition 4. *The Hilbert class field of $K = \mathbb{Q}(\sqrt{-17})$ is $L = K(\alpha)$, where $\alpha = \sqrt{\frac{1+\sqrt{17}}{2}}$.*

Proof. By definition, a Hilbert class field L^* of a field K^* is a finite Galois extension such that (i) L^* is an unramified Abelian extension of K^*, and (ii) any unramified Abelian extension of K^* lies in L^*. Thus, if we show that the extension L/K is an unramified Abelian extension of degree $h(-68) = 4$, then we would have proved that L is indeed the Hilbert class field of K.

Consider the diagram of fields in Figure 1. First, the extension L/K is Galois. To see why, note that α is a root of the monic polynomial $p(x) = x^4 - x^2 - 4$. The

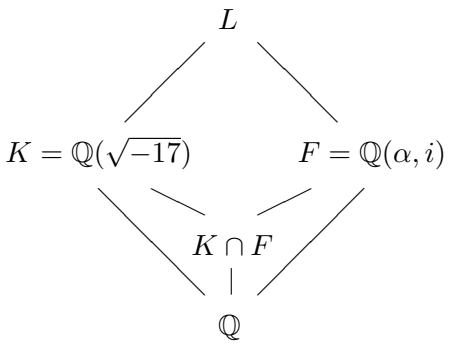

Figure 1: A Field Extension Diagram

other three roots are $-\alpha$, $\beta = \sqrt{\frac{1-\sqrt{17}}{2}}$, and $-\beta$. In particular, this shows that $p(x)$ is irreducible over $\mathbb{Q}$: it is not a product of a cubic and a monic in $\mathbb{Q}[x]$, as it has no rational roots; and it is not a product of two quadratics in $\mathbb{Q}[x]$, as the quadratic formula reveals for $p(x^2)$. Since $\alpha\beta = 2i$, and $\pm i$ are the two roots of $x^2 + 1$, we have that $F = \mathbb{Q}(\alpha, i)$ is a splitting field extension of $\mathbb{Q}$ and is separable. That is, $F/\mathbb{Q}$ is Galois. From $i = \frac{2\alpha^2-1}{\sqrt{-17}} \in L$, we have $L = K(\alpha) = K(\alpha, i)$ so that L/K is Galois, and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(F/F \cap K)$ (see [2, p. 571]).

Next, we show that L/K is of degree 4. Since α is a real number, we know that $i \notin \mathbb{Q}(\alpha)$ In addition, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, as these field extensions are obtained by adjoining roots of a quadratic and a quartic, respectively. Thus, $[F : \mathbb{Q}] = 8$. Note that $2\alpha^2 - 1 = \sqrt{17}$ so the quadratic extension $\mathbb{Q}(\sqrt{17})$ is a subfield of F. But then $\sqrt{-17} = i\sqrt{17} \in F$. That is, $K \cap F = K$. We conclude that $[L : K] = [F : F \cap K] = [F : K] = 4$, as needed. A modified diagram of fields is presented in Figure 2.

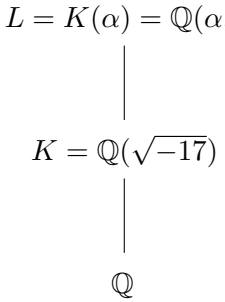

Figure 2: A Modified Field Extension Diagram

We now show that L/K is Abelian. An automorphism $\sigma \in \mathrm{Gal}(L/K)$ is transitive on the roots of $p(x)$ and of x^2+1, but fixes $\sqrt{-17}$. We see that α can be mapped to any of the four roots, but since we have the relation $\alpha\beta = 2i$, we must have $\sigma(\alpha)\sigma(\beta) = \sigma(\alpha\beta) = \sigma(2i) = 2\sigma(i)$. In addition, $\sigma(-\alpha) = -\sigma(\alpha)$ and $\sqrt{-17} = \sigma(\sqrt{-17}) = \sigma(i)\sigma(\sqrt{17}) = \sigma(i)\sigma(2\alpha^2-1) = 2\sigma(i)\sigma(\alpha)^2+1$. It follows that the automorphism σ is completely determined by its action on a single root α, and since the degree of the extension is 4, each such map is indeed an automorphism (see [2, p. 542] for more details). If we define $\sigma \in \mathrm{Gal}(L/K)$ by $\sqrt{17} \mapsto -\sqrt{17}$ and $i \mapsto -i$, then σ is a generator of $\mathrm{Gal}(L/K)$. It follows that the Galois group is cyclic and isomorphic to $\mathbb{Z}/4\mathbb{Z}$, an Abelian group.

It remains to show that L/K is unramified. Since K is an imaginary quadratic extension, any embedding of K must be into the complex field, so all infinite primes are unramified. Let $K_1 = K(\sqrt{17})$. Then we can write $K \subseteq K_1 \subseteq L$, each a degree-two extension. It suffices to show that each extension is unramified. We use the following lemma (in [1, p. 114]):

Lemma 5. *Let $L = K(\sqrt{u})$ be a quadratic extension with $u \in \mathcal{O}_K$, and let $\mathfrak{p}$ be prime in $\mathcal{O}_K$.*

(a) *If $2u \notin \mathfrak{p}$, then $\mathfrak{p}$ is unramified in L.*

(b) *If $2 \in \mathfrak{p}$, $u \notin \mathfrak{p}$, and $u = b^2 - 4c$ for some $b, c \in \mathcal{O}_K$, then $\mathfrak{p}$ is unramified in L.*

We shall not prove Lemma 5, but the result should appear plausible if one sees that $x^2 - u$ and $x^2 - bx + \frac{b^2-u}{4}$ are separable modulo $\mathfrak{p}$, where $\frac{-b+\sqrt{u}}{2}$ is a root of the second quadratic and a primitive element of the simple extension L.

Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. We have $K_1 = K(\sqrt{17}) = K(i) = K(\sqrt{-1})$ and $17 + (-1) = 16 = 2^4$. Thus, if $2 \notin \mathfrak{p}$, either $17 \notin \mathfrak{p}$ or $-1 \notin \mathfrak{p}$, so $\mathfrak{p}$ is unramified in L by part (a) of Lemma 5. Otherwise, $2 \in \mathfrak{p}$. But $17 = 2^4 + 1$ and 1 is a unit, so $17 \notin \mathfrak{p}$. In addition, $17 = 5^2 - 4 \cdot 2$, so by part (b) of Lemma 5, $\mathfrak{p}$ is unramified in L. Thus, we have established that K_1/K is an unramified extension.

Now consider $\mathfrak{p}$ a prime in $\mathcal{O}_{K_1}$. Let $\mu = \frac{1+\sqrt{17}}{2}$ and $\mu' = \frac{1-\sqrt{17}}{2}$. Then $\sqrt{\mu\mu'} = 2i \in K_1$. Hence, $L = K_1(\sqrt{\mu}) = K_1(\sqrt{\mu'})$, so we may assume that u in the theorem can be μ or μ'. Note that $\mu + \mu' = 1$, so for any proper ideal in $\mathcal{O}_{K_1}$ (in particular, a prime ideal $\mathfrak{p}$), it cannot be the case that both μ and μ' belong to the ideal. If $2 \notin \mathfrak{p}$, then either 2μ or $2\mu'$ is not in $\mathfrak{p}$, so $\mathfrak{p}$ is unramified in L by part (a) of the Lemma. Otherwise, $2 \in \mathfrak{p}$. Note that $\mu^2 - 4 = \frac{18+2\sqrt{17}}{4} - \frac{16}{4} = \mu$. Similarly, $\mu' = (\mu')^2 - 4$.

By part (b) of the Lemma, $\mathfrak{p}$ is unramified in L. It follows that L/K_1 and L/K are unramified extensions.

Thus, $\alpha = \sqrt{\frac{1+\sqrt{17}}{2}}$ is a primitive element of the simple extension L/K, where L is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-17})$, to conclude the proof of Proposition 4. $\square$

This essentially establishes necessary and sufficient conditions for primes of the form $x^2 + 17y^2$. According to Theorem 3, we know that $x^4 - x^2 - 4$, the minimal polynomial of α, can be taken to be $f_{17}(x)$. Its discriminant is $-2^6 17^2$, so Theorem 3 does not apply to the primes 2 (which is clearly not represented by $x^2 + 17y^2$) and 17 (which clearly is). We summarize the results in the following and final theorem:

Theorem 6. *Let $p \neq 17$ is an odd prime, then*

$$p = x^2 + 17y^2 \iff \begin{cases} \left(\frac{-17}{p}\right) = 1 \text{ and } x^4 - x^2 \equiv 4 \pmod{p} \\ \text{has an integer solution.} \end{cases}$$

References

[1] David A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons, Hoboken, NJ, 1989.

[2] David S. Dummit and Richard M. Foote, *Abstract Algebra*, 2nd ed., John Wiley & Sons, Hoboken, NJ, 2003.