Primes Represented by Quadratic Forms

Peter Stevenhagen

Begin again with the representation of the prime $p = x^2 + y^2$ as the sum of squares. We write $p = \pi\overline{\pi}$, where $\pi = x + yi \in \mathbb{Z}[i]$; since $\mathbb{Z}[i]$ has a finite unit group and is a principal ideal domain, p is a norm if and only if $p = 2$ or $p \equiv 1 \pmod 4$. This statement is old and due to Fermat.

Take also $p = x^2+2y^2$: treat it in exactly the same way, now look at $\mathbb{Q}(\sqrt{-2})$, which is also Euclidean; from splitting in $\mathbb{Q}(\zeta_8)$, we see that it is a norm if and only if $p = 2$ or $p \equiv 1, 3 \pmod 8$.

Already for $p = x^2 + 3y^2$, one looks at the ring $\mathbb{Z}[\sqrt{-3}]$, which is no longer the ring of integers; instead, now we have $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Z}[\zeta_3]$, so

$$p = (x + \zeta_3 y)(x + \zeta_3^2 y) = x^2 - xy + y^2 = (x - y/2)^2 + (3/4)y^2,$$

so we need y even. Given that $(\mathcal{O}/2\mathcal{O})^* \simeq \langle\zeta_3\rangle$, after multiplication by ζ_3, one gets that the element $x+\zeta_3 y$ is congruent to 1, so since $\mathbb{Z}[\sqrt{-3}] = \mathbb{Z}+2\mathcal{O}$, we conclude that $p = x^2 + 3y^2$ if and only if $p = 3$ or $p \equiv 1 \pmod 3$.

For $p = x^2 + 4y^2$, this is not a further restriction (either x or y is even if $p = x^2 + y^2$), so this holds if and only if $p \equiv 1 \pmod 4$.

The case $p = x^2 + 5y^2 = \pi\overline{\pi} \in \mathbb{Z}[\sqrt{-5}]$ is harder because $\mathbb{Z}[\sqrt{-5}]$ is no longer a factorization in a UFD (it has nontrivial class group, isomorphic to $\mathbb{Z}/2\mathbb{Z}$). Now our general strategy no longer works. We see by congruence conditions that we expect $p = 5$ and $p \equiv 1, 9 \pmod{20}$. Is the converse true? Euler decided on numerical evidence that this is true.

To prove this, we combine the techniques we have seen. Then if $\left(\frac{-5}{p}\right) = 1$ ($p = 1, 3, 7, 9 \pmod{20}$), then $(p) = \mathfrak{p}\overline{\mathfrak{p}} \in \mathbb{Z}[\sqrt{-5}]$. But we also need that $\mathfrak{p}$ is principal: by class field theory, $\mathrm{Cl} \simeq \mathrm{Gal}(H/\mathbb{Q}(\sqrt{-5})) \cong \mathbb{Z}/2\mathbb{Z}$, so we need it to split all the way up to the Hilbert class field H. Now H is unramified at all primes, and so we see easily that H can be realized by factoring $-20 = -4 \cdot 5$, so we take the compositum of the discriminants -4 and 5, which is $H = \mathbb{Q}(\sqrt{-5}, i)$. It is enough to show that it is unramified: and since H is only ramified at 5 since it is obtained by adjoining $\sqrt{5}$, but it is only ramified at 2 since it is obtained by adjoining i. Looking at $H \subset \mathbb{Q}(\zeta_{20})$, we see that $\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/H) = \langle\overline{9} \pmod{20}\rangle$, so we have the result.

We have also treated $p = x^2 + 23y^2$ in the exercise, and the criterion was that $p = 23$ or $X^3 - X - 1$ splits completely modulo p. The Hilbert class field is now obtained by adjoining a root of this polynomial, and $\mathbb{Z}[\sqrt{-23}] \subset \mathcal{O} = \mathbb{Z}[(1 + \sqrt{-23})/2]$ has index 2, and $p = \pi\overline{\pi}$ if and only if $p = x^2 + xy + 6y^2$, and one shows

that y is even so one can complete the square and write $p = (x+y/2)^2 + (23/4)y^2$, which is true by looking already modulo 2.

What is the general statement? If $p = x^2 + ny^2 = \pi\overline{\pi} \in \mathbb{Z}[\sqrt{-n}] \subset \mathbb{Q}(\sqrt{-n})$. If this is the ring of integers (n is squarefree and $n \not\equiv 3 \pmod 4$), then this is equivalent to p splits completely in the Hilbert class field of $\mathbb{Q}(\sqrt{-n})$ or $p = n$ or $n = 1$ and $p = 2$.

If not, then look at the index $\mathbb{Z}[\sqrt{-n}] \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$; we write the discriminant $D = -4n = m^2 D_0$, where D_0 is the discriminant of $\mathbb{Q}(\sqrt{-n})$, and this index is m. Then we look at the kernel

$$\mathcal{O}^* \to (\mathcal{O}/m\mathcal{O})^* \to \mathrm{Cl}_{(m)} \to \mathrm{Cl} \to 0$$

In the case $n > 4$, since $\mathbb{Z}[\sqrt{-n}] = \mathbb{Z} + m\mathcal{O}$, we have

$$\begin{array}{ccccccccc}
\{\pm 1\} & \longrightarrow & (\mathcal{O}/m\mathcal{O})^* & \longrightarrow & \mathrm{Cl}_{(m)} & \longrightarrow & \mathrm{Cl} & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & (\mathcal{O}/m\mathcal{O})^*/(\mathbb{Z}/m\mathbb{Z})^* & \longrightarrow & C(D) & \longrightarrow & \mathrm{Cl} & \longrightarrow & 0
\end{array}$$

where $C(D)$ is the *ring class group of* $\mathbb{Z}[\sqrt{-n}]$, with an extension

$$\begin{array}{ccc}
 & H_{(m)} & \\
 & \Big| \; (\mathbb{Z}/m\mathbb{Z})^\times/\pm 1 & \\
\mathrm{Cl}_{(m)} \Big(& R_D & \\
 & \Big| \; C(D) \cong \mathrm{Cl}(\mathbb{Z}[\sqrt{n}]) & \\
 & \mathbb{Q}(\sqrt{-n}) & \\
 & \Big| & \\
 & \mathbb{Q} &
\end{array}$$

We see that $p = x^2 + ny^2$ if and only if $p = n$ or p splits completely in the ring class field R_D of the ring $\mathbb{Z}[\sqrt{-n}]$ of discriminant $D = -4n$.

As another example, suppose we want to consider primes $p = 3x^2 + xy + 4y^2$; this quadratic form has discriminant -47, and 1 out of every 5 primes can be written in this form. If $R = \mathbb{Z}[(D + \sqrt{D})/2]$ is the order of discriminant $D < 0$, then $C(D) = I(R)/P(R)$, where $I(R)$ is the set of invertible R-ideals, and $P(R)$ is the set of principal R-ideals.

Then if we want to represent $p = ax^2 + bxy + cy^2$, $D = b^2 - 4ac$, then p might also be represented by another form—there is an action of $SL_2(\mathbb{Z})$ on the coordinates (x, y), and representation of primes by these forms is independent of this action. Therefore if it can be represented by such, then it can be by $(x, y) = (1, 0)$. It is a theorem due to Gauss that the set of all quadratic forms of a given

discriminant can be identified

$$\{ax^2+bxy+cy^2 : \gcd(a,b,c)=1, D=b^2-4ac<0, a>0\}/SL_2(\mathbb{Z}) \leftrightarrow C(D)$$

where

$$(a,b,c) \mapsto [\mathbb{Z}1+\mathbb{Z}(-b+\sqrt{D})/2a] \in C(D)$$

and

$$I=[\mathbb{Z}1+\mathbb{Z}\alpha] \mapsto (X-\alpha Y)(X-\overline{\alpha}Y)/N(I).$$

(Take α in the upper-half plane.) Then $N(I)=1/a$, the order is $R=\mathbb{Z}[a\alpha]$.

Then F of discriminant D represents p if and only if $\phi(\overline{F}) \in C(D)$ contains an ideal of norm p. Under $C(D) \cong \mathrm{Gal}(R_D/\mathbb{Q}(\sqrt{D}))$, this amounts to having $p=\mathfrak{p}\mathfrak{p}'$ in the maximal order $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ with $\mathfrak{p}$ having a prescribed Frobenius in the Galois group $C(D)$, so the Chebotarev density theorem already gives a density for the set of primes represented by a form.

In the case $D=-47$, using the method of reduced binary quadratic forms (let the root be in the fundamental domain for the action of $SL_2(\mathbb{Z})$, $|b| \le a \le c$, $D=b^2-4ac \le -3a^2$), then $C(D)=\{(1,1,12),(2,\pm 1,6),(3,\pm 1,4)\}$, so $\mathrm{Cl}=\mathbb{Z}/5\mathbb{Z}$, and using this and the Cheboratev density theorem that we get the density $1/5$.

As a final example of this, we consider a post by Lemmermeyer, those primes represented by $p=x^2+7y^2$. The discriminant is -28, and the class group is trivial, so $p=7$ or $(-7/p)=1$, therefore $p \equiv 1,2,4 \pmod 7$. We consider the Mersenne primes, $M_p=2^p-1$, which is prime for several $p=2,3,5,7,13,17,19,31,61,\ldots$ (no one knows if this set is infinite). When $p \equiv 1 \pmod 3$, then $M_7=8^2+7\cdot 3^2$, $M_{13}=48^2+7\cdot 29^2$, $M_{19}=720^2+7\cdot 29^2$, and $M_{31}=43968^2+7\cdot 5533^2$, for example. In all of these cases, $8 \mid x$. By easy congruence conditions, $M_p \equiv -1 \pmod 8$, and one sees $4 \mid x$ and $y \equiv \pm 3 \pmod 8$. To unveil the mystery, we note that if $M_p=\mu\overline{\mu} \in \mathbb{Z}[\sqrt{-7}]$, where $\mu=x+y\sqrt{-7}$, then we want a certain congruence condition on x modulo 8. This field has ring of integers $\mathcal{O}=\mathbb{Z}[\pi]$ where $\pi^2-\pi+2=0$, $\pi=(1+\sqrt{-7})/2$, $\pi\overline{\pi}=2$. Since

$$(\mathcal{O}/8\mathcal{O})^* = (\mathcal{O}/\pi^3\mathcal{O})^* \times (\mathcal{O}/\overline{\pi}^3\mathcal{O})^* \ni \mu,$$

we mod out by ± 1 to get μ well-defined (with y up to sign). We see that $\pi \mapsto -2,3 \bmod 8 \in \mathcal{O}/\pi^3 \simeq \mathbb{Z}/8\mathbb{Z}$, so $2\pi-1 \mapsto \pm 5 \bmod 8$, so $\mu \mapsto (x+1,x-1)$ in this unit group, so μ must to be in the kernel of the map

$$f : (\mathcal{O}/8\mathcal{O})^*/\pm 1 \to (\mathcal{O}/\pi^3\mathcal{O})^*/\pm 1 \times (\mathcal{O}/\overline{\pi}^3\mathcal{O})^*/\pm 1.$$

This is now a question of a prime splitting all of the way to a certain field K, with Galois group over $\mathbb{Q}$ equal to D_4. Taking the norm $N : (\mathcal{O}/8\mathcal{O})^*/\pm 1 \to (\mathbb{Z}/8\mathbb{Z})^*/\pm 1$, we see that $\mathbb{Q}(\sqrt{2})$ must be in the field. We see that K can only ramify at $2,7,\infty$, and by looking at ramification indices, $K/\mathbb{Q}(\sqrt{2})$ is ramified only at $7,\infty$, with tame ramification. So we need only check that the prime

$$M_p = \frac{(1+\sqrt{2}^p)}{1+\sqrt{2}} \frac{(1-\sqrt{2}^p)}{1-\sqrt{2}}.$$

These elements are totally positive. $p \equiv 1 \pmod 6$, looking modulo 7 and each element is 1 mod 7, and it splits completely in K. In fact, K is obtained by adjoining certain square roots.

Exercises

An *integral positive definite binary quadratic form*, or *form* for short, is a polynomial $f = aX^2 + bXY + cY^2$ with a, b, $c \in \mathbb{Z}$, $a > 0$, $b^2 - 4ac < 0$. A prime number p is said to be *represented* by such a form f, if there are x, $y \in \mathbb{Z}$ with $p = f(x, y)$.

Exercise 8.1. Show that a prime number $p > 2$ is represented by the form $X^2 + 7Y^2$ if and only if $p \equiv 0, 1, 2$ or $4 \bmod 7$.

Exercise 8.2. Compute the density of the set of primes p that are represented by the form $X^2 + 11Y^2$. Can these primes be characterized as in the previous exercise, by a congruence condition modulo some number n?

Exercise 8.3. Prove that the set of primes p represented by the form $3X^2 + XY + 4Y^2$ has density $1/5$.

Exercise 8.4. Attempt to classify pairs f_1, f_2 of forms with the property that f_1 and f_2 represent 'almost' the same prime numbers. ('Almost' means that finitely many exceptional primes are allowed.) For very partial results, see the preprint *Positive definite binary quadratic forms that represent the same primes* by William C. Jagy and Irving Kaplansky.

Exercise 8.5. Let $L_1 \subset \overline{\mathbb{Q}}$ be the ray class field of $\mathbb{Q}(\sqrt{-7})$ of conductor 8, and $L_2 \subset \overline{\mathbb{Q}}$ the ray class field of $\mathbb{Q}(\sqrt{2})$ of conductor $7 \cdot \infty_1 \cdot \infty_2$. Put $L = L_1 \cap L_2$.

(a) Compute the Galois groups $\mathrm{Gal}(L_1/\mathbb{Q}(\sqrt{-7}))$ and $\mathrm{Gal}(L_2/\mathbb{Q}(\sqrt{2}))$.
(b) Show that L is normal of degree 8 over $\mathbb{Q}$, and determine $\mathrm{Gal}(L/\mathbb{Q})$.
(c) Show that Mersenne primes $M_p = 2^p - 1$ with $p \equiv 1 \bmod 3$ split completely in L.
(d) Can you find generators for L? Do you need them for (c)?

Mathematisch Instituut,
Universiteit Leiden,
Postbus 9512,
2300 RA Leiden,
The Netherlands
E-mail address: psh@math.leidenuniv.nl