## Math 437/537—Group Work #7

Tuesday, October 29, 2024

We say that an integer $n$ is *represented* by a binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$ if there exist integers $x, y$ such that $f(x,y) = n$. We proved the following theorem in class last week: a positive integer $n$ is represented by $x^2 + y^2$ if and only if $v_q(n)$ is even for every prime $q \equiv 3 \pmod 4$.

We say that an integer $n$ is *properly represented* by a binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$ if there exist *coprime* integers $x, y$ such that $f(x,y) = n$. The goal of this group work is to (almost) prove the following theorem: a positive integer $n$ is properly represented by $x^2+y^2$ if and only if $4 \nmid n$, and every odd prime $p \mid n$ satisfies $p \equiv 1 \pmod 4$. (Exercise for later: prove that this theorem implies the theorem in the previous paragraph.)

*1. Show that the congruence* $t^2 \equiv -1 \pmod n$ *has a solution if and only if:* $4 \nmid n$*, and every odd prime* $p \mid n$ *satisfies* $p \equiv 1 \pmod 4$.

First we determine the prime powers $p^\alpha$ for which $t^2 \equiv -1 \pmod{p^\alpha}$ has a solution.

- When $p = 2$, we check by hand that $t^2 \equiv -1 \pmod 2$ has the solution $t \equiv 1 \pmod 2$, while $t^2 \equiv -1 \pmod{2^2}$ does not have a solution; this latter fact automatically implies that $t^2 \equiv -1 \pmod{2^\alpha}$ doesn't have a solution when $\alpha \ge 2$.
- Similarly, when $p \equiv 3 \pmod 4$, the congruence $t^2 \equiv -1 \pmod p$ doesn't have a solution since $\left(\frac{-1}{p}\right) = -1$ for these primes; this fact automatically implies that $t^2 \equiv -1 \pmod{p^\alpha}$ doesn't have a solution for any $\alpha \ge 1$.
- When $p \equiv 1 \pmod 4$, the congruence $t^2 \equiv -1 \pmod p$ does have a solution since $\left(\frac{-1}{p}\right) = 1$ for these primes. Any such solution must be nonsingular: the derivative of $t^2 + 1$ is $2t$, which vanishes modulo $p$ only when $t \equiv 0 \pmod p$, but this is not a root of $t^2 + 1 \equiv 0 \pmod p$ anyway. Therefore Hensel's lemma tells us that $t^2 \equiv -1 \pmod{p^\alpha}$ has a solution for every $\alpha \ge 1$ when $p \equiv 1 \pmod 4$.

By the Chinese remainder theorem, the congruence $t^2 \equiv -1 \pmod n$ has a solution if and only if $t^2 \equiv -1 \pmod{p^\alpha}$ has a solution for every $p^\alpha \mid n$; we quickly see that this is equivalent to the condition in the statement of the problem.

*2. Suppose that* $x^2 + y^2$ *is a proper representation of* $n$*, so that* $(x,y) = 1$ *and* $x^2 + y^2 = n$.

(a) *Let* $p^\alpha$ *be a prime power dividing* $n$*. Show that* $x^2 \equiv -y^2 \pmod{p^\alpha}$*. Conclude that there is a solution to* $t^2 \equiv -1 \pmod{p^\alpha}$.

(b) *Show that* $t^2 \equiv -1 \pmod n$ *has a solution.*

(a) Since $p^\alpha \mid n = x^2+y^2$, we have $x^2+y^2 \equiv 0 \pmod{p^\alpha}$, or equivalently $x^2 \equiv -y^2 \pmod{p^\alpha}$. It's not possible for $(y, p^\alpha) > 1$: this would imply that $y \equiv 0 \pmod p$ and hence $x^2 \equiv -y^2 \equiv 0 \pmod p$ as well, and so $p \mid x$ and $p \mid y$, contadicting the coprimality assumption. Therefore $y$ is invertible modulo $p^\alpha$, and we can write $(xy^{-1})^2 \equiv 1 \pmod{p^\alpha}$, which shows that $t^2 \equiv -1 \pmod{p^\alpha}$ has a solution. Equivalently, $x^2 \equiv -y^2 \pmod{p^\alpha}$ implies $x^2 \equiv -y^2 \pmod p$ implies $\left(\frac{x}{p}\right)^2 = \left(\frac{x^2}{p}\right) = \left(\frac{-y^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{y}{p}\right)^2$; if either $\left(\frac{x}{p}\right)$ or $\left(\frac{y}{p}\right)$ equals $0$, than so does the other one by this identity, again leading to the contradiction $p \mid (x,y)$; therefore $1 = \left(\frac{x}{p}\right)^2 = \left(\frac{-1}{p}\right)\left(\frac{y}{p}\right)^2 = \left(\frac{-1}{p}\right) \cdot 1$, showing that $t^2 \equiv -1 \pmod{p^\alpha}$ has a solution. (Compare this to the proof of Fermat's theorem, about not-necessarily-proper representations, for which $p \mid x$ and $p \mid y$ is actually a possibility.)

(b) Since $t^2 \equiv -1 \pmod{p^\alpha}$ has a solution for every $p^\alpha \mid n$ by part (a), the Chinese remainder theorem immediately implies that $t^2 \equiv -1 \pmod{n}$ has a solution. (Compare, if you like, to the main paragraph in the proof of Theorem 3.13, which holds for more general binary quadratic forms; I find that proof's factorization of $4|n|$ into $m_1 m_2$ to be less intuitive than the standard factor-into-prime-powers argument.)

3. *Suppose that $t^2 \equiv -1 \pmod{n}$ has a solution. Show that there exists a binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$, of discriminant $b^2 - 4ac = -4$, such that $f(1,0) = n$. Conclude that there exists a binary quadratic form of discriminant $-4$ that properly represents $n$.*

Choose an integer $k$ such that $k^2 \equiv -1 \pmod{n}$, so that $k^2 = nc - 1$ for some integer $c$. Then the binary quadratic form $f(x,y) = nx^2 + 2kxy + cy^2$ has discriminant $(2k)^2 - 4nc = -4$, and $f(1,0) = n \cdot 1^2 + 2k \cdot 1 \cdot 0 + c \cdot 0^2 = n$. In particular, $\gcd(1,0) = 1$, so this binary quadratic form of discriminant $-4$ properly represents $n$. (Compare to the first paragraph in the proof of the more general Theorem 3.13.)

*4. Define $f_0(x,y) = 109x^2 + 152xy + 53y^2$, and let $n = 109$. (Note that $152^2 - 4 \cdot 109 \cdot 53 = -4$.)*

(a) *Why does $f_0(x,y)$ properly represent $n$?*

(b) *Define $f_1(x,y) = f_0(y,x)$. Why does $f_1(x,y)$ properly represent $n$?*

(c) *Define $f_2(x,y) = f_1(x+my,y)$, where $m$ is chosen so that if $f_2(x,y) = ax^2 + bxy + cy^2$, then $|b| < a$. Why does $f_2(x,y)$ properly represent $n$?*

(d) *Keep alternating the previous two steps, creating binary quadratic forms $f_3, f_4, \ldots$. What ends up happening?*

(a) We see immediately that $f_0(1,0) = 109 = n$, and $\gcd(1,0) = 1$, so this is a proper represenation.

(b) We have $f_1(x,y) = 53x^2 + 152xy + 109y^2$. The old inputs $(1,0)$ are mapped to the new inputs $(0,1)$, and indeed $f_1(0,1) = 109$ is a proper representation of $n$.

(c) We have

$$f_2(x,y) = 53x^2 + (106m + 152)xy + (53m^2 + 152m + 109)y^2.$$

Choosing $m = -1$ makes the middle coefficient equal to $152 - 106 = 46$, which is small enough in absolute value. Therefore we set $f_2(x,y) = 53x^2 + 46xy + 10y^2$. Can we find $x, y$ so that $(x+my,y) = (x-y,y) = (0,1)$ as ordered pairs? Certainly, because the change of variables $(x,y) \mapsto (x-y,y)$ is inverted by $(x,y) \mapsto (x+y,y)$, so we can just take $(x,y) = (0+1,1) = (1,1)$; and indeed $f_2(1,1) = 53 + 46 + 10 = n$ is a proper representation.

(d) Continuing the pattern:

- We set $f_3(x,y) = f_2(x,y) = 10x^2 + 46xy + 53y^2$, and see that $f_3(1,1) = n$ is a proper representation.
- We set $f_4(x,y) = f_3(x+my,y) = 10x^2 + (20m+46)xy + (10m^2 + 46m + 53)y^2$; we want to choose $m$ so that $|46 + 20m| < 10$, and the appropriate choice is $m = -2$. Therefore $f_4(x,y) = 10x^2 + 6xy + y^2$. The change of variables $(x,y) \mapsto (x-2y,y)$ is inverted by $(x,y) \mapsto (x+2y,y)$, so we can take $(x,y) = (1+2\cdot 1, 1) = (3,1)$; and indeed $f_4(3,1) = 90 + 18 + 1 = n$ is a proper representation. (We can check directly

that $\gcd(3,1)=1$; but also notice that if $\gcd(x,y)=1$, then $\gcd(x+my,y)=1$ as well for any integer $m$; so this type of variable change automatically preserves proper representations.

- We set $f_5(x,y)=f_4(y,x)=x^2+6xy+10y^2$, and we see that $f_5(1,3)=n$ is a proper representation.
- We set $f_6(x,y)=f_5(x+my,y)=x^2+(2m+6)xy+(m^2+6m+10)y^2$; since we want $6+2m$ to be small, we choose $m=-3$. Therefore $f_6(x,y)=x^2+y^2$. The change of variables $(x,y)\mapsto(x-3y,y)$ is inverted by $(x,y)\mapsto(x+3y,y)$, so we can take $(x,y)=(1+3\cdot3,3)=(10,3)$; and indeed $f_6(10,3)=10^2+3^2=109$ is a proper representation.

This process of "reducing" a binary quadratic form to one with the same discriminant and small coefficients is the subject of Section 3.5 of Niven, Zuckerman, & Montgomery. For discriminant $-4$, we will always end up with $x^2+y^2$, as it turns out. In the general case, however, there could be several different binary quadratic forms at the final step. Indeed, these changes of variable generate equivalence classes that partition the set of all binary quadratic forms of a particular discriminant; there are finitely many such classes (see Theorems 3.18 and 3.19), and the number of classes is called the *class number* of that discriminant. And yes, this set of equivalence classes can be endowed with a group structure based on "composition" of forms, turning it into the *class group*; and yes, this class group (for binary quadratic forms of discriminant $d$) is isomorphic to the class group coming from equivalence classes of ideals (in the quadratic extension $\mathbb{Q}(\sqrt{d})$). Indeed, class groups in rings of integers of number fields were investigated to generalize the phenomenon of class groups coming from binary quadratic forms.