MATH 115, SUMMER 2012
LECTURE 22

JAMES MCIVOR

1. How to use the Reduction Theorem to get good results like the Sum of Two Squares Theorem

- **NOTE**: in this lecture, form always means pos def form, unless stated otherwise.

This is what it's all about - we did some theory about quadratic forms (even though we skipped some proofs), and now we get the payoff: tons of results that are similar to Fermat's Two Squares Thm that we proved earlier in the course.

For convenience, we recall the definition of reduced (in the special case where the form is pos def, so we can ignore the absolute values) and the statements of the two important theorems:

Definition 1. A positive definite form $f(x,y) = ax^2 + bay + cy^2$ is **reduced** if either $-a < b \leq a < c$ or $0 \leq b \leq a = c$.

- Recall also that for a positive definite form, we have $a, c > 0$ and $d < 0$.

Theorem 1 (The Reduction Theorem)**.** *Let $f(x,y) = ax^2+bxy+cy^2$ be a primitive positive definite QF (integral and binary as usual). Then*

1. *f is equivalent to a unique reduced form.*
2. *$|b| \leq a \leq \sqrt{-d/3}$*
3. *The number of equivalence classes of positive definite forms of discriminant d (which is the class number $H_p(d)$) is less than or equal to $-2d/3$.*

we'll also use the following theorem from last week:

Theorem 2. *Let p be and odd prime and d any integer congruent to 0 or 1 mod 4. Then p is represented by a form of discriminant d if and only if d is a square mod p.*

- One way to apply the theorem is to go through all the possible values of d. Recall that d must be a square mod 4 in order for there to be a form with discriminant d. Since we are interested in pos def forms, d must also be negative.
- Thus the allowed values of d are $d = -3, -4, -7, -8, -11, -12, \ldots$.

Example 1.1. Let d be -3. Then part (3) of the theorem says that there are at most 2 inequivalent reduced forms of discriminant d. Let's try to find them. We can actually do this without the theorem, as follows: Given that $b^2 - 4ac = -3$, what could a, b, c be? Since f is reduced, $|b| \leq a$, so $b^2 \leq a^2$, and also $a \leq c$, so

$$3 = 4ac - b^2 \geq 4a^2 - b^2 = 3a^2 + (a^2 - b^2) \geq 3a^2,$$

and this shows that $a \leq 1$. It can't be less than one by positive definiteness, so $a = 1$.

- since $|b| \leq a$, $b = \pm 1$

- If $c > 1$, then $3 = 4ac - b^2 > 4a^2 - b^2 = 4 - 1 = 3$, contradiction. So $c = 1$.

- thus we are in the 2nd case of the definition of reduced, which says b is non-negative, so actually $b = 1$. Thus the only reduced form of discriminant -3 is $f(x, y) = x^2 + xy + y^2$.

- now see how much easier it is with the theorem: part (2) says $|b| \leq a \leq 1$. a can't be zero, so it's 1. Then it follows that $b = c = 1$ just as above.

Now we can ask: which primes are represented by this form? By Thm 2, p is represented by some form of discriminant -3 iff -3 is a square mod p.

- since, up to equivalence, there is only one form of $d = -3$, the Thm says p is represented by our form $x^2 + xy + y^2$ iff -3 is a square mod p.

- this happens when $p|3$, i.e., $p = 3$, or if $\left(\frac{-3}{p}\right) = 1$.

- exercise: for which primes p is $\left(\frac{-3}{p}\right) = 1$? Answer: $p \equiv 1 \mod 3$.

Example 1.2. Now let $d = -4$. The theorem again says there are at most 2 forms with this discriminant. But actually we don't need the theorem to figure this out: since $-4 = b^2 - 4ac$, we must have $b = 0$, and $a = c = 1$. So the only form with this discriminant is $x^2 + y^2$.

Applying Thm 2 to this gives: a prime $p > 2$ is represented by $x^2 + y^2$ if and only if -4 is a square mod p. Since 4 is a square mod p no matter what, this happens if and only if $\left(\frac{-1}{p}\right) = 1$.

Example 1.3. Let's skip ahead to a more negative value of d, say $d = -20$. Then we have by part (2) of the reduction Thm, $|b| \leq a \leq \sqrt{20/3} < \sqrt{7} < 3$. What possible values of a, b, c could satisfy these inequalities and also $4ac - b^2 = 20$?

- If $b = 0$, we have $4ac = 20$, so since $a < 3$, we get $a = 1$ and $c = 5$, giving the form $f_5 = x^2 + 5y^2$, our old friend. $b = 1$ is impossible since $4ac$ cannot equal 21. If $b = 2$, we get $4ac = 24$, so $ac = 6$, hence $a = 2$, $c = 3$; this form, namely $g(x, y) = 2x^2 + 2xy + 3y^2$, is another primitive reduced form.

- There are no others, since $a, b < 3$.

- Now apply Thm 2: an odd prime p is represented by a form of $d = -20$ iff -20 is a square mod p iff -5 is a square mod p iff $p = 5$ or $\left(\frac{-5}{p}\right) = 1$.

- We now show that our conjecture from the other day, namely that p is represented by f_5 iff $p = 5$ or $p \equiv 1$ or $9 \mod 20$, is correct.

Proposition 1. *The odd prime p is represented by $f_5(x, y) = x^2 + 5y^2$ if and only if $p = 5$ or $p \equiv 1$ or $9 \mod 20$.*

Proof. First assume p is represented by f_5, say $p = a^2 + 5b^2$, for some integers a, b. Reducing mod 5 shows that $p \equiv a^2 \mod 5$, so p is a square mod 5, meaning $p = 5$ or $p \equiv 1$ or 4 mod 5. Reducing mod 4 shows that $p \equiv a^2 + b^2 \mod 4$. Since p is odd, one of a, b must be even, and the other odd, and this shows that $p \equiv 1 \mod 4$. The only possibilities are $p \equiv 1, 9 \mod 20$, using CRT.

Now for the harder direction. We assume p is one of the three types, and deduce that p is represented by f_5. If $p = 5$, this is clear. Now assume $p \equiv 1 \mod 20$, so $p \equiv 1 \mod 5$ and $p \equiv 1 \mod 4$. Then

$$\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right) = 1,$$

since 1 is a square mod anything, and in using QRL, the sign doesn't change because $5 \equiv 1 \bmod 4$. So 5 is a square mod p. Also 4 is a square mod p, since 4 is always a square. Finally, -1 is a square mod p since $p \equiv 1 \mod 4$. Putting this all together we get that -20 is a square mod p, and this shows that p is represented by a form of discriminant -20, hence it must be represented by either f_5 or g.

Could such a prime p be represented by g? No, and here's why. Suppose it were - we would have

$$p = 2x^2 + 2xy + 3y^2$$

for some x, y. Now reduce mod 4:

$$p \equiv 2(x^2 + xy) - y^2 \mod 4$$

We know $p \equiv 1 mod 4$, and for this to happen, we would need $x^2 + xy$ odd and y odd. But if so, then $x^2 + xy = x(x + y)$ odd implies, both x and $x + y$ are odd, which means y is even, contradiction. So g does not represent any primes congruent to 1 mod 4, hence our prime p is not represented by g, so it must be represented by f_5.

Next assume $p \equiv 9 \mod 20$. Make a similar argument in the problem session.

□