

# Math Circles: Number Theory III

Centre for Education in Mathematics and Computing

University of Waterloo

March 9, 2011

## A prime-generating polynomial

The polynomial  $f(n) = n^2 - n + 41$  generates a lot of primes ...

$$f(0) = 41$$

$$f(1) = 41$$

$$f(2) = 43$$

$$f(3) = 47$$

$$f(4) = 53$$

$$f(5) = 61$$

$$f(6) = 71$$

$$f(7) = 83$$

$$f(8) = 97$$

$$f(9) = 113$$

$$f(10) = 131$$

$$f(11) = 151$$

$$f(12) = 173$$

$$\vdots$$

$$f(36) = 1301$$

$$f(37) = 1373$$

$$f(38) = 1447$$

$$f(39) = 1523$$

$$f(40) = 1601$$

$$f(41) = 41^2$$

Why?

# Quadratic forms

## Definition

A *quadratic form* is a function  $f$  of the form

$$f(x, y) = ax^2 + bxy + cy^2,$$

where  $a, b, c$  are integers,  $\gcd(a, b, c) = 1$ , and  $a > 0$ .

The *discriminant* of  $f$  is defined to be  $D = b^2 - 4ac$ .

## Exercise

- ▶ Find a quadratic form of discriminant  $-4$ .
- ▶ Find a quadratic form of discriminant  $-8$ .
- ▶ Find a quadratic form of discriminant  $-3$ .
- ▶ Find a quadratic form of discriminant  $-163$ .

# Equivalence of quadratic forms

## Definition

- ▶ Let  $f(x, y) = ax^2 + bxy + cy^2$  be a quadratic form. An integer  $n$  is *of the form*  $ax^2 + bxy + cy^2$  if there exist integers  $x, y \in \mathbb{Z}$  such that  $n = ax^2 + bxy + cy^2$ .
- ▶ Equivalently, we say that  $f(x, y)$  *represents* the integer  $n$ .
- ▶ Two quadratic forms  $f(x, y)$  and  $g(x, y)$  are said to be *equivalent* if the set of integers represented by each is identical.

## Exercise

- ▶ Find two different quadratic forms of discriminant  $-4$ . Are they equivalent?
- ▶ Find two different quadratic forms of discriminant  $-8$ . Are they equivalent?
- ▶ True or false: Two quadratic forms of the same discriminant are equivalent.

## Examples of equivalence

1. Are  $f(x, y) = ax^2 + bxy + cy^2$  and  $g(x, y) = ax^2 - bxy + cy^2$  equivalent?
2. Are  $f(x, y) = ax^2 + bxy + cy^2$  and  $g(x, y) = cx^2 + bxy + ay^2$  equivalent?
3. Are  $x^2 + y^2$  and  $x^2 + 2y^2$  equivalent?

## Examples of equivalence

1. Are  $f(x, y) = ax^2 + bxy + cy^2$  and  $g(x, y) = ax^2 - bxy + cy^2$  equivalent?

$$f(x, y) = g(x, -y)$$

$$g(x, y) = f(x, -y)$$

2. Are  $f(x, y) = ax^2 + bxy + cy^2$  and  $g(x, y) = cx^2 + bxy + ay^2$  equivalent?

3. Are  $x^2 + y^2$  and  $x^2 + 2y^2$  equivalent?

## Examples of equivalence

1. Are  $f(x, y) = ax^2 + bxy + cy^2$  and  $g(x, y) = ax^2 - bxy + cy^2$  equivalent?

$$f(x, y) = g(x, -y)$$

$$g(x, y) = f(x, -y)$$

2. Are  $f(x, y) = ax^2 + bxy + cy^2$  and  $g(x, y) = cx^2 + bxy + ay^2$  equivalent?

$$f(x, y) = g(y, x)$$

$$g(x, y) = f(y, x)$$

3. Are  $x^2 + y^2$  and  $x^2 + 2y^2$  equivalent?

## Examples of equivalence

1. Are  $f(x, y) = ax^2 + bxy + cy^2$  and  $g(x, y) = ax^2 - bxy + cy^2$  equivalent?

$$f(x, y) = g(x, -y)$$

$$g(x, y) = f(x, -y)$$

2. Are  $f(x, y) = ax^2 + bxy + cy^2$  and  $g(x, y) = cx^2 + bxy + ay^2$  equivalent?

$$f(x, y) = g(y, x)$$

$$g(x, y) = f(y, x)$$

3. Are  $x^2 + y^2$  and  $x^2 + 2y^2$  equivalent?

3 is of the form  $x^2 + 2y^2$ , but 3 is not of the form  $x^2 + y^2$ .

# Reduced forms

## Definition

We say the quadratic form  $f(x, y) = ax^2 + bxy + cy^2$  is *reduced* if  $0 \leq b \leq a \leq c$ .

## Theorem

Every quadratic form  $f_0(x, y) = a_0x^2 + b_0xy + c_0y^2$  of discriminant  $D < 0$  is equivalent to some reduced form  $ax^2 + bxy + cy^2$  of the same discriminant.

## Proof.

- ▶ Let  $f(x, y) = ax^2 + bxy + cy^2$  be a form equivalent to  $f_0(x, y)$  with the same discriminant and  $b$  minimal.
- ▶ If  $b$  is negative, make it positive.
- ▶ If  $a > c$ , reverse  $a$  and  $c$ .
- ▶ Claim:  $b \leq a$ .

## Reduced forms

### Proof.

If  $b > a$ , then write  $b = 2aq + r$ , with  $|r| \leq a$ . Then

$$\begin{aligned}g(x, y) &= f(x - qy, y) = ax^2 + (b - 2aq)xy + (c - bq + aq^2)y^2 \\ &= ax^2 + rxy + c'y^2\end{aligned}$$

satisfies the following properties:

1. It is equivalent to  $f(x, y)$  (the reverse operation is  $f(x, y) = g(x + qy, y)$ ).
2. It has the same discriminant:  
 $(b - 2aq)^2 - 4a(c - bq + aq^2) = b^2 - 4ac$ .
3. It has middle coefficient  $|r| < b$ .

So  $b$  wasn't minimal. □

## Computing reduced forms

- ▶ Suppose  $f(x, y) = ax^2 + bxy + cy^2$  is a reduced form of discriminant  $D < 0$ .
- ▶ Then  $b^2 \leq a^2$ , and  $a \leq c$ , so

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2,$$

- ▶ In other words,

$$a \leq \sqrt{\frac{-D}{3}}. \tag{1}$$

- ▶ This inequality means that we can easily find all reduced forms of any given discriminant  $D < 0$ , since there are only finitely many values of  $a$  to consider.

## Reduced forms with $D = -4$

- ▶ We already have one example of a reduced form of discriminant  $-4$ , namely,  $x^2 + y^2$ .
- ▶ Are there any other quadratic forms  $ax^2 + bxy + cy^2$  with  $D = -4$ ?
- ▶ Since  $a \leq \sqrt{(-D)/3} = \sqrt{4/3}$ , we conclude that  $a = 1$ .
- ▶ Reduced forms have  $b \leq a$ , so  $b = 0$  or  $1$ .
- ▶ Choosing  $b = 0$  recovers  $x^2 + y^2$ .
- ▶ Choosing  $b = 1$ , we see that there is no form  $x^2 + xy + cy^2$  having discriminant  $-4$ .

Hence there is only one reduced quadratic form of discriminant  $-4$ .

$$D = -20$$

Equation (1) tells us that  $a \leq \sqrt{20/3} = 2.582\dots$ , so  $a = 1$  or  $a = 2$ .

- ▶  $a = 1$ : Reduced forms have  $0 \leq b \leq a$ , so  $b = 0$  or  $1$ .
  - ▶  $b = 0$ : We get  $x^2 + 5y^2$ .
  - ▶  $b = 1$ :  $x^2 + xy + cy^2$  never has discriminant  $-20$ .
- ▶  $a = 2$ : Here  $b = 0, 1$ , or  $2$ .
  - ▶  $b = 0$ :  $2x^2 + cy^2$  never has discriminant  $-20$ .
  - ▶  $b = 1$ :  $2x^2 + xy + cy^2$  never has discriminant  $-20$ .
  - ▶  $b = 2$ : We get  $2x^2 + 2xy + 3y^2$ .

Hence, the two reduced forms of discriminant  $-20$  are  $x^2 + 5y^2$  and  $2x^2 + 2xy + 3y^2$ .

# Algorithm for computing reduced forms

Given  $D < 0$ :

For each of the finitely many  $a$  such that  $0 < a \leq \sqrt{(-D)/3}$

- ▶ For each of the finitely many  $b$  such that  $0 \leq b \leq a$ 
  - ▶ Set  $D = b^2 - 4ac$
  - ▶ Solve for  $c = \frac{b^2 - D}{4a}$
  - ▶ Check if  $c$  is an integer
  - ▶ If  $c$  is an integer, then we have a reduced form, otherwise not.

A slight optimization:  $D$  is odd if and only if  $b$  is odd. So we can rule out half the values of  $b$ .

$$D = -163$$

We have  $a \leq \sqrt{163/3} = 7.37\dots$ , so  $a = 1, 2, 3, 4, 5, 6$ , or  $7$ .

▶  $a = 1$ :

▶  $b = 1$ :  $c = (1^2 + 163)/4 = 41$  is an integer, producing  $x^2 + xy + 41y^2$ .

▶  $a = 2$ :

▶  $b = 1$ :  $c = (1^2 + 163)/8 = 41/2$  is not an integer.

▶  $a = 3$ :

▶  $b = 1$ :  $c = 41/3$  is not an integer.

▶  $b = 3$ :  $c = 43/3$  is not an integer.

▶  $a = 4$ :

▶  $b = 1$ :  $c = 41/4$  is not an integer.

▶  $b = 3$ :  $c = 43/4$  is not an integer.

▶  $a = 5$ :

▶  $b = 1$ :  $c = 41/5$  is not an integer.

▶  $b = 3$ :  $c = 43/5$  is not an integer.

▶  $b = 5$ :  $c = 47/5$  is not an integer.

$$D = -163$$

- ▶  $a = 6$ :
  - ▶  $b = 1$ :  $c = 41/6$  is not an integer.
  - ▶  $b = 3$ :  $c = 43/6$  is not an integer.
  - ▶  $b = 5$ :  $c = 47/6$  is not an integer.
- ▶  $a = 7$ :
  - ▶  $b = 1$ :  $c = 41/7$  is not an integer.
  - ▶  $b = 3$ :  $c = 43/7$  is not an integer.
  - ▶  $b = 5$ :  $c = 47/7$  is not an integer.
  - ▶  $b = 7$ :  $c = 53/7$  is not an integer.

We see that the **only** reduced form of discriminant  $-163$  is  $x^2 + xy + 41y^2$ .

# Class number theorem

## Definition

An integer  $D < 0$  has *class number 1* if there is exactly one reduced form of discriminant  $D$ .

## Theorem (Class Number 1 Theorem (Heegner, Baker, Stark))

*The negative integers with class number 1 are precisely*

$$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

# A remarkable theorem

## Theorem (Main Theorem)

*If a prime  $p$  divides  $n^2 - n + 41$ , then  $p$  is of the form  $x^2 + xy + 41y^2$  for some integers  $x, y$ .*

This theorem explains why 41 primes appear:

1. For  $0 \leq n \leq 40$ , we have  $f(n) = n^2 - n + 41 < 41^2$
2. Hence any nontrivial prime divisor  $p$  of  $f(n)$  is less than 41
3. But the theorem says  $p = x^2 + xy + 41y^2$
4.  $p = x^2 + xy + 41y^2$  is always at least 41!!!

# Proof of the theorem

Proof.

- ▶ Suppose  $p$  divides  $n^2 - n + 41$ .
- ▶ Write  $p \cdot k = n^2 - n + 41$ .
- ▶ Let  $f(x, y) = x^2 + xy + 41y^2$ .
- ▶ Set  $g(x, y) := f(nx + y, -x)$ .
- ▶ Then

$$\begin{aligned}g(x, y) &= f(nx + y, -x) \\&= (nx + y)^2 + (nx + y) \cdot (-x) + 41(-x)^2 \\&= (n^2 - n + 41)x^2 + (2n - 1)xy + y^2 \\&= pkx^2 + (2n - 1)xy + y^2.\end{aligned}$$

- ▶ The discriminant of  $g(x, y)$  is  $(2n - 1)^2 - 4(n^2 - n + 41) = -163$ , so  $g(x, y)$  is equivalent to  $f(x, y)$ .

# Proof of the main theorem

Proof.

- ▶  $f(x, y) = x^2 + xy + 41y^2$
- ▶  $g(x, y) = pkx^2 + (2n - 1)xy + y^2$ ,  $\text{disc}(g) = -163$
- ▶ Set  $h(x, y) = px^2 + (2n - 1)xy + ky^2$
- ▶  $\text{disc}(h) = (2n - 1)^2 - 4pk = \text{disc}(g) = -163$

Hence  $h(x, y)$  is equivalent to  $f(x, y)$ .

- ▶  $p$  is clearly of the form  $h(x, y)$ , since  $p = h(1, 0)$ .
- ▶ It follows that  $p$  is of the form  $f(x, y) = x^2 + xy + 41y^2$ .

