Introduction to Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

1. Quadratic Forms
   - Equivalence
   - Reduction
   - Proper Representations by Binary Forms
   - Sums of Two Squares
   - Sums of Four Squares

Subsection 1

Equivalence

Binary Quadratic Forms and the Discriminant

- A **binary quadratic form** is an expression

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

where a, b, c are integers.

- By the **discriminant** of f we mean the number

$$d = b^2 - 4ac.$$

- Note that

$$d \equiv \begin{cases} 0 \pmod 4, & \text{if } b \text{ is even} \\ 1 \pmod 4, & \text{if } b \text{ is odd} \end{cases}$$

Principal Forms

- We noted that

$$d \equiv \begin{cases} 0 \pmod 4, & \text{if } b \text{ is even} \\ 1 \pmod 4, & \text{if } b \text{ is odd} \end{cases}$$

- The forms

$$f(x,y) = \begin{cases} x^2 - \frac{1}{4}dy^2, & \text{for } d \equiv 0 \pmod 4 \\ x^2 + xy + \frac{1}{4}(1-d)y^2, & \text{for } d \equiv 1 \pmod 4 \end{cases}$$

  are called the **principal forms with discriminant** d.
- Note that these have indeed:
  - integer coefficients;
  - discriminant d.

Definiteness

- Consider again $f(x,y) = ax^2 + bxy + cy^2$.

  We have

$$\begin{array}{rcl} 4af(x,y) & = & 4a^2x^2 + 4abxy + 4acy^2 \\ & = & (2ax+by)^2 - b^2y^2 + 4acy^2 \\ & = & (2ax+by)^2 - (b^2 - 4ac)y^2 \\ & = & (2ax+by)^2 - dy^2. \end{array}$$

  - If $d < 0$, the values taken by f are all of the same sign (or zero); f is called **positive** or **negative definite** accordingly.
  - If $d > 0$, then f takes values of both signs and it is called **indefinite**.

Unimodular Substitutions

- An **integral unimodular substitution**, is a substitution of the form

$$x = px' + qy', \quad y = rx' + sy',$$

where p, q, r, s are integers with $ps - qr = 1$.

- Alternatively, an integral unimodular substitution is represented by the matrix

$$U = \begin{pmatrix} p & q \\ r & s \end{pmatrix},$$

with $\det U = ps - qr = 1$.

- Note that

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Equivalence of Quadratic Forms

- We say that two quadratic forms

$$f(x,y) = ax^2 + bxy + cy^2 \quad \text{and} \quad f'(x',y') = a'x'^2 + b'x'y' + c'y'^2$$

are **equivalent** if one can be transformed into the other by an integral unimodular substitution, i.e., if $f'(x',y') = f(px'+qy', rx'+sy')$.

- Equivalence of quadratic forms is an equivalence relation.
  - We have $f(x,y) \sim f(x,y)$ via the identity matrix.
  - If $f(x,y) \sim f'(x',y')$ via U, then $f'(x',y') \sim f(x,y)$ via U^{-1}.
  - If $f(x,y) \sim f'(x',y')$ via U and $f'(x',y') \sim f''(x'',y'')$ via V, then $f(x,y) \sim f''(x'',y'')$ via UV.

Values on Pairs of Relative Primes

- Let $f(x,y) = ax^2 + bxy + cy^2$.
- The values of $f(x,y)$ are completely determined by its values of relatively prime pairs of integers.
- Let x and y be such that $x = (x,y)k$ and $y = (x,y)\ell$, where (x,y) is the greatest common divisor of x and y.

  Then, we have:

$$\begin{aligned} f(x,y) &= a((x,y)k)^2 + b(x,y)k(x,y)\ell + c((x,y)\ell)^2 \\ &= a(x,y)^2k^2 + b(x,y)^2k\ell + c(x,y)^2\ell^2 \\ &= (x,y)^2(ak^2 + bk\ell + c\ell^2) \\ &= (x,y)^2 f(k,\ell). \end{aligned}$$

  Since $(k,\ell) = 1$, the result follows.

Unimodular Substitution and Pairs of Relative Primes

- Suppose $x = px' + qy'$ and $y = rx' + sy'$ is a unimodular substitution. Then $(x, y) = 1$ iff $(x', y') = 1$.
- It suffices, by symmetry, to show that if $(x', y') = 1$, then $(x, y) = 1$

  Let $d = (x, y)$, $x = dk$ and $y = d\ell$.

  Then
  $$\left\{\begin{array}{rcl} px' + qy' & = & dk \\ rx' + sy' & = & d\ell \end{array}\right\} \Rightarrow \left\{\begin{array}{rcl} x' & = & dks - d\ell q \\ y' & = & pd\ell - rdk \end{array}\right\}$$

  It follows that $d \mid x'$ and $d \mid y'$.

  Since $(x', y') = 1$, $d = 1$.

  Therefore, $(x, y) = 1$.

Values of Equivalent of Quadratic Forms

- The set of values assumed by equivalent forms as x, y run through the integers are the same.
- Note that, by a previous remark, it suffices to show that they assume the same set of values as the pair x, y runs through all relatively prime integers.

  Suppose $f(x,y) \sim f'(x',y')$ via $U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$.

  Then, for $(x',y') = (k,\ell)$, with $(k,\ell) = 1$, we have

  $$f'(k,\ell) = f(pk + q\ell, rk + s\ell),$$

  where, by the preceding slide, $(pk + q\ell, rk + s\ell) = 1$.

Parameters of Equivalent Quadratic Forms

- Suppose

$$\begin{array}{rcl} f(x,y) & = & ax^2+bxy+cy^2, \\ f'(x',y') & = & f(px'+qy',rx'+sy'). \end{array}$$

Then, we get

$$\begin{array}{rcl} f'(x',y') & = & a(px'+qy')^2+b(px'+qy')(rx'+sy')+c(rx'+sy')^2 \\ & = & a(p^2x'^2+2pqx'y'+q^2y'^2) \\ & & +b(prx'^2+(ps+qr)x'y'+qsy'^2) \\ & & +c(r^2x'^2+2rsx'y'+s^2y'^2) \\ & = & (ap^2+bpr+cr^2)x'^2 \\ & & +(2apq+b(ps+qr)+2crs)x'y' \\ & & +(aq+bqs+cs^2)y'^2 \\ & = & f(p,r)x'^2+(2apq+b(ps+qr)+2crs)x'y'+f(q,s)y'^2. \end{array}$$

Thus $f'(x',y')=a'x'^2+b'x'y'+c'y'^2$, where $a'=f(p,r)$, $b'=2apq+b(ps+qr)+2crs$, $c'=f(q,s)$.

Discriminant of Equivalent Quadratic Forms

- Equivalent forms have the same discriminant.
- We found that, if $f(x,y) = ax^2 + bxy + cy^2$, then

$$f'(x',y') = a'x'^2 + b'x'y' + c'y'^2,$$

where $a' = f(p,r)$, $b' = 2apq + b(ps+qr) + 2crs$, $c' = f(q,s)$.

$$\begin{aligned}
&b'^2 - 4a'c' \\
&= (2apq + b(ps+qr) + 2crs)^2 - 4(ap^2 + bpr + cr^2)(aq^2 + bqs + cs^2) \\
&= 4a^2p^2q^2 + b^2p^2s^2 + 2b^2psqr + b^2q^2r^2 + 4c^2r^2s^2 \\
&+ 4abp^2qs + 4abpq^2r + 4bcprs^2 + 4bcqr^2s + 8acpqrs \\
&- 4a^2p^2q^2 - 4abp^2qs - 4acp^2s^2 - 4abpq^2r - 4b^2pqrs \\
&- 4bcprs^2 - 4acq^2r^2 - 4bcqr^2s - 4c^2r^2s^2 \\
&= b^2p^2s^2 - 2b^2pqrs + b^2q^2r^2 + 8acpqrs - 4acp^2s^2 - 4acq^2r^2 \\
&= b^2(p^2s^2 - 2pqsr + q^2r^2) - 4ac(p^2s^2 - 2pqrs + q^2r^2) \\
&= (b^2 - 4ac)(ps - qr)^2 = b^2 - 4ac.
\end{aligned}$$

Discriminant of Equivalent Quadratic Forms (Matrices)

- Alternatively (and much more succinctly and elegantly), in matrix notation, we can write

$$f(x,y)=X^TFX \quad \text{and} \quad X=UX',$$

where

$$X=\begin{pmatrix} x \\ y \end{pmatrix}, X'=\begin{pmatrix} x' \\ y' \end{pmatrix}, F=\begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix}, U=\begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

- Then f is transformed into $X'^TF'X'$, where $F'=U^TFU$.
- But the determinant of U is 1.
- So the determinants of F and F' are equal.

Subsection 2

Reduction

Reduced Binary Forms

- We consider positive definite quadratic forms, i.e., we assume that $d < 0$ and that $a > 0$, whence, also, $c > 0$.
- By a finite sequence of unimodular substitutions of the form

$$x = y', \quad y = -x' \quad \text{and} \quad x = x' \pm y', \quad y = y',$$

  f can be transformed into another binary form for which $|b| \leq a \leq c$.
  - The first of these substitutions interchanges a and c, whence it allows one to replace $a > c$ by $a < c$;
  - The second changes b to $b \pm 2a$, leaving a unchanged, whence, by finitely many applications it allows one to replace $|b| > a$ by $|b| \leq a$.

  The process must terminate since whenever the first substitution is applied it results in a smaller value of a.

Example

- Suppose $f(x,y) = 5x^2 + 7xy + 3y^2$.

  We then proceed as follows:

$$f(x,y) \xrightarrow[]{\substack{x=y' \\ y=-x'}} 3x'^2 - 7x'y' + 5y'^2$$
$$\xrightarrow[]{\substack{x'=x''+y'' \\ y'=y''}} 3x''^2 - x''y'' + y''^2$$
$$\xrightarrow[]{\substack{x''=y''' \\ y''=-x'''}} x'''^2 + x'''y''' + 3y'''^2.$$

  We see that $|b'''| \leq a''' \leq c'''$.

Reduced Binary Forms (Cont'd)

- Suppose, now, we start with

$$f(x,y) = ax^2 + bxy + cy^2, \quad |b| \leq a \leq c.$$

- We can transform f into a binary form for which either

$$-a < b \leq a < c \quad \text{or} \quad 0 \leq b \leq a = c.$$

  - If $b = -a$, then the second of the above substitutions allows one to take $b = a$, leaving c unchanged;
  - If $a = c$, then the first substitution allows one to take $0 \leq b$.

A binary form for which one of the above conditions on a, b, c holds is said to be **reduced**.

The Class Number

Proposition

There are only finitely many reduced forms with a given discriminant d.

- Suppose $f(x,y) = ax^2 + bxy + cy^2$ is reduced.

  Then, since $|b| \leq a \leq c$,

  $$-d = 4ac - b^2 \geq 3ac.$$

  So a, c and $|b|$ cannot exceed $\frac{1}{3}|d|$.
- The number of reduced forms with discriminant d is called the **class number** and is denoted by $h(d)$.

  Example: We calculate the class number when $d = -4$.

  The inequality $3ac \leq 4$ gives $a = c = 1$.

  Hence, $b = 0$.

  It follows that $h(-4) = 1$.

Inequivalence of Reduced Forms

Theorem

Any two reduced binary quadratic forms are inequivalent.

- Let $f(x,y)$ be a reduced form. If $x,y \neq 0$, with $|x| \geq |y|$,

$$\begin{array}{rcl} f(x,y) & \geq & |x|(a|x| - |by|) + c|y|^2 \\ & \geq & |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c. \end{array}$$

  Similarly, if $|y| \geq |x|$, we have $f(x,y) \geq a - |b| + c$.

  Hence, the smallest values assumed by f for relatively prime integers x,y are a,c and $a - |b| + c$ in that order.

  These values are taken at $(1,0)$, $(0,1)$ and either $(1,1)$ or $(1,-1)$.

  The sequences of values assumed by equivalent forms for relatively prime x,y are the same, except for a rearrangement.

  Thus, if f' is a form equivalent to f, and f' is reduced, then $a = a'$, $c = c'$ and $b = \pm b'$. We must show that, if $b = -b'$, then $b = 0$.

Inequivalence of Reduced Forms (Cont'd)

Claim: If $b = -b'$, then in fact $b = 0$.

We can assume here that $-a < b < a < c$.

In fact, since f' is reduced, we have

- $-a < -b$;
- if $a = c$, then $b \geq 0$, $-b \geq 0$, whence $b = 0$.

So $f(x,y) \geq a - |b| + c > c > a$, for all integers $x, y \neq 0$.

For the substitution taking f to f', we have $a = f(p,r)$.

Thus, $p = \pm 1$, $r = 0$. Since $ps - qr = 1$, we obtain $s = \pm 1$.

Further, we have $c = f(q,s)$, whence $q = 0$.

Hence, the only substitutions taking f to f' are

$$\left\{ \begin{array}{lcl} x & = & x' \\ y & = & y' \end{array} \right\} \quad \text{and} \quad \left\{ \begin{array}{lcl} x & = & -x' \\ y & = & -y' \end{array} \right\}.$$

These give $b = 0$.

Subsection 3

Proper Representations by Binary Forms

Proper Representation by a Binary Form

- A number n is said to be **properly represented by a binary form** $f(x,y) = ax^2 + bxy + cy^2$ if
$$n = f(x,y),$$
for some integers x, y, with $(x,y) = 1$.

Characterization of Proper Representation

Theorem

A number n is properly represented by some binary form with discriminant d if and only if the congruence $x^2 \equiv d \pmod{4n}$ is soluble.

- Suppose first that b is a solution.

  Then, there exists a c, such that

  $$b^2 - d = 4nc.$$

  Consider the form

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

  It has discriminant d.

  It properly represents n, since $f(1,0) = n$.

Characterization of Proper Representation (Converse)

- Conversely, let $f(x,y) = ax^2 + bxy + cy^2$ be such that
  - f has discriminant d;
  - $n = f(p,r)$, for some integers p, r with $(p,r) = 1$.

  Since $(p,r) = 1$, there exist integers q and s, such that $ps - qr = 1$.

  We consider the form $f'(x',y') = f(px' + qy', rx' + sy')$.
  - We know that $a' = f(p,r) = n$.
  - The discriminant is $d = b'^2 - 4a'c' = b'^2 - 4nc'$.

  This shows that b' is a solution of

$$x^2 \equiv d \pmod{4n}.$$

Subsection 4

Sums of Two Squares

Expression as a Sum of Two Squares

Theorem

A natural number n can be expressed in the form x^2+y^2, for some integers x,y if and only if every prime divisor p of n, with $p \equiv 3 \pmod 4$ occurs to an even power in the standard factorization of n.

- Suppose that $n=x^2+y^2$ and that n is divisible by a prime $p \equiv 3 \pmod 4$.

  Then $x^2 \equiv -y^2 \pmod p$.

  But -1 is a quadratic non-residue $\pmod p$.

  Therefore, p divides x and y.

  Now, we obtain

  $$\left(\frac{x}{p}\right)^2+\left(\frac{y}{p}\right)^2=\frac{n}{p^2}.$$

  It follows by induction that p divides n to an even power.

Expression as a Sum of Two Squares (Converse)

- Suppose that every prime divisor p of n, with $p \equiv 3 \pmod 4$ occurs to an even power in the standard factorization of n.

  It suffices to show that the square-free part of n can be represented as $x^2 + y^2$.

  So assume, to start with, that n is square-free and each odd prime divisor p of n satisfies $p \equiv 1 \pmod 4$.

  The quadratic form $x^2 + y^2$ is reduced with discriminant -4.

  We have seen that $h(-4) = 1$.

  So it is the only such reduced form.

  It follows by the preceding subsection, that n is properly represented by $x^2 + y^2$ if and only if the congruence $x^2 \equiv -4 \pmod{4n}$ is soluble.

  By hypothesis, -1 is a quadratic residue $\pmod p$, for each prime divisor p of n.

  Hence, -1 is a quadratic residue $\pmod n$ and the result follows.

Remarks on the Proof

- The argument involves the Chinese remainder theorem, but this can be avoided by appeal to the identity

$$(x^2+y^2)(x'^2+y'^2)=(xx'+yy')^2+(xy'-yx')^2,$$

  which enables one to consider only prime values of n.

  There is a well known proof of the theorem based on this identity alone.
- The demonstration here can be refined to furnish the number of representations of n as x^2+y^2.

  The number is given by $4\sum_{\substack{m|n \\ m \text{ odd}}} \left(\frac{-1}{m}\right)$.

  Example: Each prime $p\equiv 1 \pmod 4$ can be expressed in precisely eight ways as the sum of two squares.

Subsection 5

Sums of Four Squares

Expression as a Sum of Four Squares

Theorem (Bachet-Lagrange)

Every natural number can be expressed as the sum of four integer squares.

- The proof is based on the identity

$$\begin{aligned}(x^2+y^2+z^2+w^2)&(x'^2+y'^2+z'^2+w'^2)\\ &=(xx'+yy'+zz'+ww')^2+(xy'-yx'+wz'-zw')^2\\ &\quad+(xz'-zx'+yw'-wy')^2+(xw'-wx'+zy'-yz')^2,\end{aligned}$$

  which is related to the theory of quaternions.
- In view of the identity and the representation

$$2=1^2+1^2+0^2+0^2,$$

  it suffices to prove the theorem for odd primes p.

Expression as a Sum of Four Squares (Cont'd)

- Note that the numbers
  - x^2, with $0 \le x \le \frac{1}{2}(p-1)$, are mutually incongruent $\pmod{p}$;
  - $-1-y^2$, with $0 \le y \le \frac{1}{2}(p-1)$, are mutually incongruent $\pmod{p}$.

  Thus, there exist x, y, such that

  $$x^2 \equiv -1-y^2 \pmod{p},$$

  satisfying

  $$x^2+y^2+1 < 1+2\left(\frac{1}{2}p\right)^2 < p^2.$$

  So, for some integer m, with $0 < m < p$,

  $$mp = x^2+y^2+1.$$

Sum of Four Squares (Fermat's Method of Infinite Descent)

- Let ℓ be the least positive integer such that

$$\ell p = x^2 + y^2 + z^2 + w^2,$$

for some integers x, y, z, w.

By the preceding slide, $\ell \leq m < p$.

We show that ℓ must be odd.

Suppose ℓ is even.

Then an even number of x, y, z, w would be odd.

So we could assume that $x+y$, $x-y$, $z+w$, $z-w$ are even.

Since

$$\frac{1}{2}\ell p = \left(\frac{1}{2}(x+y)\right)^2 + \left(\frac{1}{2}(x-y)\right)^2 + \left(\frac{1}{2}(z+w)\right)^2 + \left(\frac{1}{2}(z-w)\right)^2,$$

this is inconsistent with the minimal choice of ℓ.

To prove the theorem we have to show that $\ell = 1$.

Sum of Four Squares (Conclusion)

- Suppose that $\ell > 1$.

  Let x', y', z', w' be the numerically least residues of $x, y, z, w \pmod{\ell}$. Set $n = x'^2 + y'^2 + z'^2 + w'^2$.
  - $n \equiv 0 \pmod{\ell}$;
  - $n > 0$, since otherwise ℓ would divide p.
  - Since ℓ is odd, $n < 4(\frac{1}{2}\ell)^2 = \ell^2$.

    Thus, $n = k\ell$, for some integer k, with $0 < k < \ell$.

  By the identity, $(k\ell)(\ell p)$ is expressible as a sum of four integer squares.

  Moreover, each of these squares is divisible by ℓ^2.

  Thus kp is expressible as a sum of four integer squares contradicting the definition of ℓ.