Quadratic Forms

Aaron Pixton

June 14, 2011

1 Reciprocity first

Quadratic reciprocity provides a complete answer to the following important question: which residues modulo an odd prime p are squares? The notation used for this is the *Legendre symbol*

$$\left(\frac{a}{p}\right),$$

which is defined to equal 0 if a is a multiple of p, 1 if a is a nonzero quadratic residue, and -1 otherwise.

Then the following facts suffice to compute any Legendre symbol:

- $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ for $a \equiv b \bmod p$.
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
- $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
- $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
- Quadratic Reciprocity: $\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)$ for any odd primes p and q.

Example: 7 is a square mod $p \neq 2, 7$ if and only if $p \equiv 1, 3, 9, 19, 25$, or 27 mod 28.

2 What is a quadratic form?

A *quadratic form* is a homogeneous polynomial of degree 2 in some number of variables:

$$f(x_1, \dots, x_k) = \sum_{1 \le i \le j \le k} a_{ij} x_i x_j.$$

Here the coefficients a_{ij} can live in any ring, but usually we'll be interested in integer quadratic forms.

Example: $x^2 + y^2 + yz + z^2$.

A (real) quadratic form $f(x_1, \dots, x_k)$ is *positive-definite* if $f(x_1, \dots, x_k) \ge 0$ for all $x_1, \dots, x_k$ and $f(x_1, \dots, x_k) = 0$ only when $x_1 = x_2 = \cdots = x_k$. A (real) quadratic form is *indefinite* if f takes on both positive and negative values.

Examples: $x^2 + y^2 + z^2 + w^2$ is positive-definite, $x^2 - 2y^2$ is indefinite.

Binary quadratic forms are particularly pleasant to work with because they factor over a quadratic extension of the rationals:

$$x^2 + ny^2 = (x + y\sqrt{-n})(x - y\sqrt{-n}).$$

Even if you don't know very much about the algebraic number theory of quadratic extensions, this can still be used to construct identities like

$$(a^2 + nb^2)(c^2 + nd^2) = (ac - nbd)^2 + n(ad + bc)^2.$$

3 Representing numbers

We say that a quadratic form $f(x_1, \ldots, x_k)$ *represents* a number n if there exist $x_1, \ldots, x_n$ (in our coefficient ring, so usually integers) such that

$$f(x_1, \ldots, x_k) = n.$$

Determining the set of numbers represented by a given quadratic form can be quite a difficult problem, and a lot of beautiful number theory was developed by people who were working on this.

Here are some answers to questions of representability for certain quadratic forms:

- The Two Squares Theorem: A positive integer n is the sum of two squares if and only if every prime p congruent to 3 mod 4 divides n with even multiplicity. In fact,

$$\left|\{(x,y) \in \mathbb{Z}^2 : x^2 + y^2 = n\}\right| = 4(d_1(n) - d_3(n)),$$

  where $d_i(n)$ is the number of positive divisors of n congruent to i mod 4.

- The Three Squares Theorem: A positive integer is the sum of three squares if and only if it is not of the form $4^k(8m+7)$.

- The Four Squares Theorem: Any positive integer is the sum of four squares. In fact,

$$\left|\{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 : x_1^2 + x_2^2 + x_3^2 + x_4^2 = n\}\right| = 4 \sum_{d \mid n, 4 \nmid d} d.$$

- The 290 theorem: If a positive-definite quadratic form represents all positive integers up through 290, then it represents all positive integers.

- The Hasse-Minkowski theorem: If a quadratic form represents an integer over $\mathbb{R}$ and over $\mathbb{Q}_p$ for each p, then it represents that integer over $\mathbb{Q}$.

- Primes represented by binary quadratic forms have been particularly studied:
  - An odd prime p is the sum of two squares if and only if it is 1 mod 4.
  - An odd prime p is representable by $x^2 + 2y^2$ if and only if it is 1 or 3 mod 8.
  - A prime $p \neq 3$ is representable by $x^2 + 3y^2$ if and only if it is 1 mod 3.
  - A prime $p \neq 5$ is representable by $x^2 + 5y^2$ if and only if it is 1 or 9 mod 20.
  - A prime $p \neq 2, 5$ is representable by $2x^2 + 2xy + 3y^2$ if and only if it is 3 or 7 mod 20.
  - A prime p is representable by $x^2 + 14y^2$ if and only if $\left(\frac{-14}{p}\right) = 1$ and $(x^2+1)^2 \equiv 8 \bmod p$ has a solution.

- Pell equations: $x^2 - dy^2$ represents 1 in infinitely many different ways for any nonsquare positive d. These solutions to the equation

$$x^2 - dy^2 = 1$$

  come in a single infinite family generated by the smallest nontrivial solution $x_0 + y_0\sqrt{d}$.

  The generalized Pell equation $x^2 - dy^2 = n$ is more subtle; there could be no solutions or multiple disjoint infinite families of solutions.

4 Problems

1. Prove that any prime $p \equiv 1 \bmod 4$ is the sum of two squares. (If you've seen this, try the corresponding statements for $x^2 + 2y^2$ and $x^2 + 3y^2$.)

2. (Bulgaria 96) Prove that for any natural number $n \geq 3$, there exist odd numbers x and y such that

$$7x^2 + y^2 = 2^n.$$

3. (Romania TST 2004) Let p be an odd prime and define

$$f(x) = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) x^{k-1}.$$

Show that: if $p \equiv 3 \bmod 4$, then $x - 1$ divides $f(x)$ but $(x-1)^2$ does not; if $p \equiv 5 \bmod 8$, then $(x-1)^2$ divides $f(x)$ but $(x-1)^3$ does not.

4. Show that the equation $2y^2 = x^4 - 17z^4$ has no positive integer solutions.

5. (ELMO 2003) Let $f(x, y, z = 2xy + 2yz + 2zx - x^2 - y^2 - z^2$ and suppose that f represents a positive integer n. Show that there exist positive integers a, b, c that are the side lengths of a triangle and that satisfy $f(a, b, c) = n$.

6. (ISL 01/N4) Let $a > b > c > d$ be positive integers and suppose that $ac + bd = (b + d + a - c)(b + d - a + c)$. Prove that $ab + cd$ is not prime.

7. Show that the equation $x^5 - y^2 = 52$ has no positive integer solutions.

8. (ISL 04/N7) Let p be an odd prime and n a positive integer. In the coordinate plane, eight distinct points with integer coordinates lie on a circle with diameter of length p^n. Prove that there exists a triangle with vertices at three of the given points such that the squares of its side lengths are integers divisible by p^{n+1}.