Rational Points on Conics, and Local-Global Relations in Number Theory

Joseph Lipman

Purdue University
Department of Mathematics

lipman@math.purdue.edu

http://www.math.purdue.edu/~lipman

November 26, 2007

Rational Points on Conics, and Local-Global Relations in Number Theory

Abstract

What are all the integer solutions of $x^2 + y^2 = z^2$?
Of $2x^2 + 3y^2 = 5z^2$?
Or, in general, of $Q(x, y, z) = 0$, where Q is a homogeneous degree-two polynomial with integer coefficients?

If you can find one solution then you get them all by passing lines through the corresponding point on the plane conic $Q = 0$, and finding the other intersection of each such line with the conic.
But there may not be any solution at all.

A beautiful theorem of Legendre gives a criterion for when there is.
Legendre's theorem has evolved into the *Hasse principle,* relating "local" and "global" solutions, even for more variables. This will all be sketched, as an introduction to local-global relations, a key theme in modern Number Theory.

Outline

1. Diophantine equations.
2. Ternary quadratic forms, and conics.
3. When is there any solution? Legendre's theorem.
4. Quadratic reciprocity (brief remarks).
5. Hasse-Minkowski theorem
6. Local to global

Diophantine equations

A basic theme of Number Theory

Study the set of integer n-tuples $(\mathbf{x}) = (x_1, \ldots, x_n)$ satisfying a given system of polynomial equations

$$f_1(\mathbf{x}) = f_2(\mathbf{x}) = \cdots = f_r(\mathbf{x}) = 0 \qquad (f_i \in \mathbb{Z}[X_1, \ldots, X_n]).$$

Phony simplification: theoretically enough to consider $r = 1$, because

$$f_1(\mathbf{x}) = \cdots = f_r(\mathbf{x}) = 0 \iff f_1(\mathbf{x})^2 + \cdots + f_r(\mathbf{x})^2 = 0.$$

Hilbert's tenth problem

Find an algorithm to decide, for *any* $F \in \mathbb{Z}[X_1, \ldots, X_n])$, whether $F(\mathbf{x}) = 0$ has an integer solution.

Shown in the 1970s to be impossible.

Homework. Google "Diophantine equations" and "Hilbert's tenth problem."

Ternary quadratic forms

Of course for specific classes of equations there may be algorithms. For example, the case of systems of linear equations is well-understood, via "Smith canonical form" for integer matrices (MA 554).

Let us then go on to quadratic equations, specifically to $Q = 0$ where Q is a homogeneous quadratic form in three variables (ternary quadratic form) with integer coefficients:

$$Q(X, Y, Z) = aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ.$$

From linear algebra one knows that for some 3×3 integer matrix A, the change of variables

$$\mathbf{X} = A\mathbf{X}_1$$

changes Q into

$$Q_1(X_1, Y_1, Z_1) = a_1X_1^2 + b_1Y_1^2 + c_1Z_1^2$$

So there is no essential loss in generality in assuming in the first place that, in Q, we have $d = e = f = 0$.
Thus we are concerned with an equation of the form

$$aX^2 + bY^2 + cZ^2 = 0.$$

Here, clearly, we may assume that a, b and c have no common factor > 1 (otherwise, divide it out).

Connection with geometry

The real projective plane $\mathbf{P}^2_{\mathbf{R}}$ has as its points equivalence classes of real triples $(x, y, z) \neq (0, 0, 0)$ under the equivalence relation

$$(x, y, z) \equiv (x', y', z') \iff \exists \lambda \neq 0 \text{ such that } (x, y, z) = \lambda(x', y', z').$$

It may be thought of as the affine plane $\big(=$ the points $(x, y, 1)\big)$ plus a projective line at ∞ consisting of points where $Z = 0$.

The (equivalence classes of) triples satisfying $Q = 0$ form a conic in $\mathbf{P}^2_{\mathbf{R}}$.

Example: finding integer solutions of $X^2 + Y^2 = Z^2$ (Pythagorean triples) leads to consideration of the circle $\{\, (x, y, 1) \mid x^2 + y^2 = 1 \,\}$.

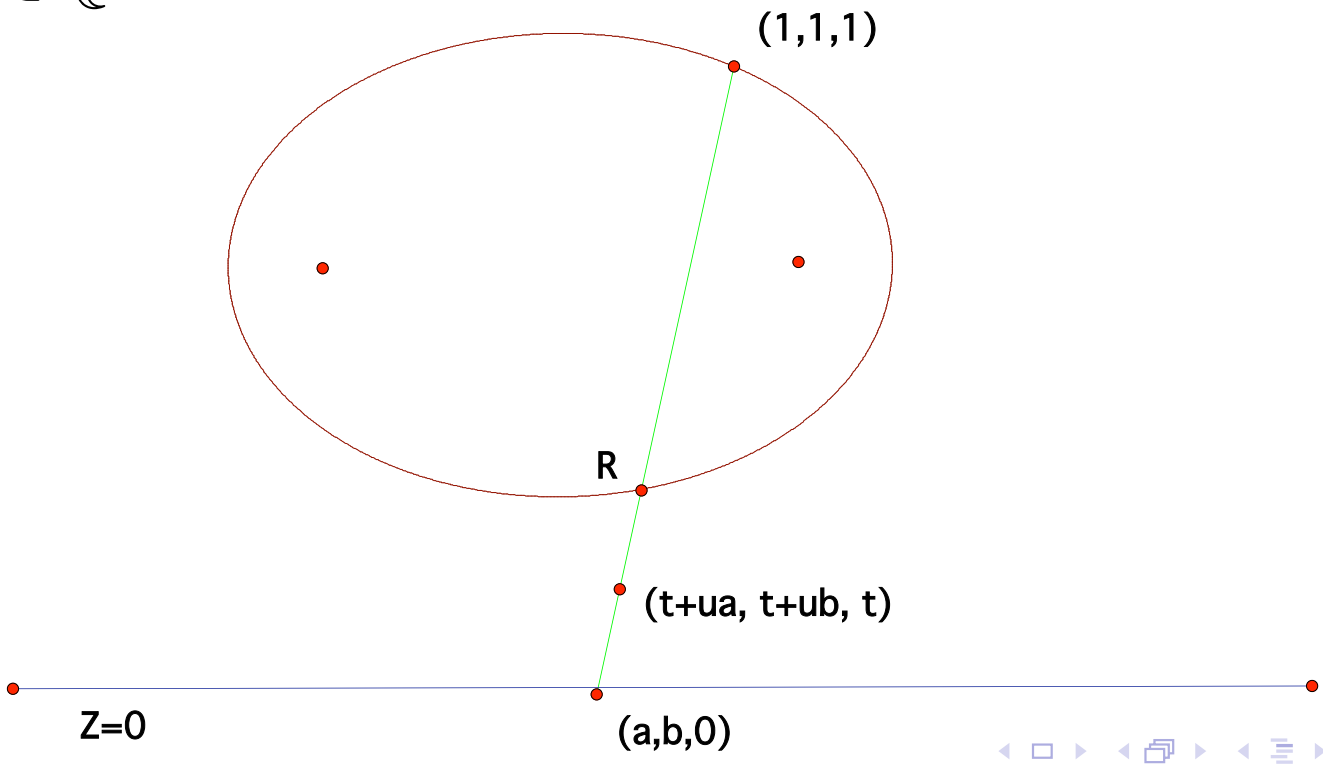
A rational point on this conic is an integer triple (x, y, z) satisfying $Q = 0$. To avoid ambiguity, one can insist that x, y, and z be relatively prime, and that the the one with greatest absolute value be positive. Each equivalence class of integer triples contains a unique such (x, y, z).

Example: $2x^2 + 3y^2 = 5z^2$

There is an obvious solution $(1, 1, 1)$. To find any other rational point R on this conic, note that the line joining R to $(1, 1, 1)$ intersects the conic in just the two points R and $(1, 1, 1)$. Any line through $(1, 1, 1)$ and another point with integer coordinates has the parametric form

$$X = t + ua, \;\; Y = t + ub, \;\; Z = t. \qquad (*)$$

with $a, b \in \mathbb{Q}$.



To find the intersections, plug the parametric equations $(*)$ into $2x^2 + 3y^2 = 5z^2$ to get a quadratic equation for u/t, one of whose roots is 0, giving the intersection $(1, 1, 1)$, and the other of which is

$$\frac{u}{t} = \frac{-4a - 6b}{2a^2 + 3b^2},$$

where, after multiplying through by a common denominator, and factoring out any common factor, we may assume a and b to be relatively prime integers. Setting $u = -4a - 6b$, $t = 2a^2 + 3b^2$ in $(*)$, get

$$R = (x, y, z) = (-2a^2 - 6ab + 3b^2,\ 2a^2 - 4ab - 3b^2,\ 2a^2 - 3b^2).$$

This is a general formula for all solutions.

Examples. $a = -3$ and $b = 2$ gives $(30, 30, 30) \equiv (1, 1, 1)$; $a = 2, b = -3$ gives $(55, 5, 35) \equiv (11, 1, 7)$; $a = 5, b = 7$ gives $(-113, -237, 197)$.

One gets relatively prime integers unless $a \equiv 0 \pmod 3$, $b \equiv 0 \pmod 2$, or $a \equiv b \pmod 5$. So some further, elementary, tweaking of the formula is needed to get only relatively prime positive triples.

But having brought out the main point, we stop here.

When is there any solution?

When does $aX^2 + bY^2 + cZ^2 = 0$ have any rational point at all?

First reduction:

Lemma (Gauss, Disquisitiones, article 298.)

Write $bc = \alpha^2 s$, $ac = \beta^2 t$, $ab = \gamma^2 u$ with s, t and u square free. Then

$$A = \frac{a\alpha}{\beta\gamma}, \quad B = \frac{b\beta}{\alpha\gamma}, \quad C = \frac{c\gamma}{\alpha\beta}$$

are squarefree integers, pairwise relatively prime; and $aX^2 + bY^2 + cZ^2 = 0$ has a rational point if and only if so does $AX^2 + BY^2 + CZ^2 = 0$.

The *proof*, elementary but requiring some thinking, is left as an exercise.

So assume: (#): a, b and c are squarefree and *pairwise* relatively prime.

Recall that a is a quadratic residue of b is there is an integer x such that $a \equiv x^2 \pmod{b}$, i.e., a is a square in $\mathbb{Z}/b\mathbb{Z}$.

Theorem (Legendre, 1785.)

Assume $abc \neq 0$ and (#). Then $aX^2 + bY^2 + cZ^2 = 0$ has a rational point iff a, b, c don't all have the same sign, and $-bc$, $-ac$ and $-ab$ are quadratic residues of a, b and c respectively.

This reduces the determination of whether $aX^2 + bY^2 + cZ^2 = 0$ has a rational point to the determination of when one integer is a quadratic residue of another. (More below.)

The *necessity* of a, b, c not all having the same sign is obvious.

Further, if (x, y, z) is a nonzero solution, then, e.g., the gcd $(y, a) = 1$, since any prime p dividing y and a would divide cz^2 but not c (since $(a, c) = 1$), whence $p|z$ and p^2 divides $-by^2 - cz^2 = ax^2$, and so, a being square free, $p|x$ as well as y and z, contradiction.

But then $\exists w$ with $yw \equiv 1 \pmod{a}$, so, since $-by^2 \equiv cz^2 \pmod{a}$, therefore $-bc \equiv -bcy^2w^2 \equiv (wcz)^2$, and $-bc$ is a quadratic residue of a.

Similarly, $-ac$ and $-ab$ are quadratic residues of b and c respectively.

Sufficiency of Legendre's conditions is proved classically, e.g., in his book **Théorie des nombres**, see **http://gallica.bnf.fr/ark:/12148/bpt6k426107/f116.chemindefer**.

A different treatment is in Gauss's **Disquisitiones Arithmeticae,** articles 294 *ff.* (Available in translation.) Moreover, Gauss's proofs are (as always) *constructive,* i.e., he gives a method for finding a solution.

If you don't believe in reading the masters, you can also look, e.g., in Ireland and Rosen's **Classical introduction to Modern Number Theory,** chapter 17, §3.

We will outline an approach which is more modern in spirit.

But first:

Quadratic reciprocity (brief remarks).

Deciding whether a is a quadratic residue of b (in brief, $a\mathrm{R}b$) is a finite question: just square all the natural numbers $\leq b$, take the remainders on division by b, and compare with the remainder of a.
This is extremely inefficient in practice.
Quadratic reciprocity provides a close relation (not specified here, but see any book on number theory) between the conditions $a\mathrm{R}b$ and $b\mathrm{R}a$. Hence we can decide one condition by reference to the other.

For example, is $5\mathrm{R}149$? Quadratic reciprocity tells us that this is so if and only if $149\mathrm{R}5$. But $149 \equiv 4 \pmod 5$, so the latter holds iff $4\mathrm{R}5$, which is clearly true. And indeed, $5 \equiv 68^2 \pmod{149}$. (Compare this way of discovering that $5\mathrm{R}149$ with squaring 1–68!)

Similarly, for any $a < b$, the question whether $a\mathrm{R}b$ can be transformed into the question of whether $\bar{b}\mathrm{R}a$, where $\bar{b}$ is the remainder of division of b by a. Since $\bar{b} + a < b + a$, we have a simplification in the sense of "total size;" and by repetition of the process, we can reduce the question to one involving small enough numbers that it becomes easy to answer.

Quadratic reciprocity was first adumbrated by Euler (mid 18th century).

Legendre thought he could prove it with his theorem.

For example, if a and b are relatively prime and both are $\equiv 3 \pmod 4$, and $a\mathrm{R}b$, then $b\mathrm{R}a$ fails, since otherwise $-aX^2 - bY^2 + Z^2$ would have a solution (x, y, z) with at least one coordinate odd; but that's impossible because $x^2 + y^2 + z^2 \not\equiv 0 \pmod 4$.

Similarly, if b and c are relatively prime, $b \equiv 1 \pmod 4$, $c \equiv 3 \pmod 4$, and $c\mathrm{R}b$, then $-b\mathrm{R}c$ fails, since otherwise $X^2 + bY^2 - cZ^2 = 0$ would have a solution (x, y, z) as above.

But there are a number of other possibilities, to handle which Legendre made some unwarranted—at the time—assumptions (like the infinitude of primes in an arithmetic progression).

The first complete proof of quadratic reciprocity was due to Gauss. There is a keen analysis of Legendre's gaps in Disquisitiones, articles 296 and 297.

Reinterpreting Legendre's conditions

Lemma

In Legendre's theorem, the conditions $-abRc$, $-acRb$ and $-bcRa$ are equivalent, together, to the following condition:
For every odd prime p, the equation $aX^2 + bY^2 + cZ^2 = 0$ has a nontrivial p-adic solution, that is, for every positive integer m there exists $(x, y, z) \not\equiv (0, 0, 0)$ with $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p^m}$.

Proof. (Sketch.) First one shows that it suffices to deal with the case $m = 1$. This is by a form of Hensel's lemma, which uses Newton's method of solving equations via a first-order Taylor expansion, see e.g. Theorem 1 on page 14 in J.P. Serre's **A Course in Arithmetic.**

(This is where we need p to be odd.)

For $m = 1$, if, say, $p \nmid abc$, we can divide through by a and assume the equation (mod p) to be of the form $X^2 = eY^2 + fZ^2$, where neither e nor f vanishes. Substituting 1 for Z and letting Y run through $\mathbb{Z}/p\mathbb{Z}$, we get $(p+1)/2$ distinct values on the right side, and these can't all be nonresidues. Thus there is a nontrivial solution (mod p).

Finally, if, say $p|c$, whence $p \nmid ab$, the equation (mod p) is $X^2 = -ab(Y/a)^2$, which has a solution with $Y = a$, since $-ab\mathrm{R}c$.

Conversely, if the equation has a nontrivial solution (mod p) for every p dividing c, then similar reasoning shows that $-ab\mathrm{R}p$ for all such p, and (trivially) for $p = 2$ as well, whence, since c is squarefree, the Chinese Remainder Theorem gives that $-ab\mathrm{R}c$.
In this argument, a, b, c can be permuted at will. Q.E.D.

Hasse-Minkowski Theorem

Thus Legendre's theorem becomes a consequence of the case $n = 3$ of:

Theorem

Let

$$Q(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$$

be homogeneous of degree 2. In order that $Q = 0$ have a nontrivial integer solution $(x_1, \ldots, x_n)$ it is necessary and sufficient that the same be true p-adically for all primes p, and also over $\mathbf{R}$.

A proof can be found in Serre's **A Course in Arithmetic,** Chapter IV. The general case involves an important notion called the Hilbert symbol, but the elementary case $n = 3$ doesn't need that.

Local and Global

Number-theoretic phenomena which hold p-adically for all p and also over $\mathbf{R}$ are said to hold locally. Those which hold over $\mathbb{Q}$ (in particular, over $\mathbb{Z}$) are said to hold globally.

The idea here is that arithmetic in local situations is much easier than in global ones. So any time you can reduce a global problem to a local one, you have a much better chance of solving it. This is a fundamental principle of modern Number Theory.

Example. A class of Diophantine equations which have global solutions whenever they have local solutions is said to satisfy the Hasse Principle.

So quadratic forms satisfy this principle, and there are a few other nice examples.

However, for cubics the principle doesn't hold in general. There is a counterexample due to Selmer:

the equation $3X^3 + 4Y^3 + 5Z^3 = 0$ is solvable locally, but not globally.

The arithmetic of cubic curves (or elliptic curves) is a huge part of number theory. For such curves, the failure of the Hasse principle is measured by a group called the Tate-Shafarevich group. It remains an open question whether this group is always finite.

Homework. Google "Hasse principle" and "Tate-Shafarevich."