TERNARY QUADRATIC FORMS: LAGRANGE AND LEGENDRE

This writeup is drawn from André Weil's book *Number Theory: An approach through history, From Hammurapi to Legendre,* from Borevich and Shafarevich's *Number Theory,* and from Ireland and Rosen's *A Classical Introduction to Modern Number Theory.*

Consider a class of nondegenerate ternary quadratic equations, in which a, b are nonzero squarefree integers, not both negative,

$$aX^2 + bY^2 = Z^2.$$

This equation *has solutions* if there exist nonzero triples $(x, y, z) \in \mathbb{Q}^3$ such that $ax^2 + by^2 = z^2$. *Throughout this writeup it is understood, with or without comment, that* $(0, 0, 0)$ *is not considered a solution of a homogeneous equation.* Any solution can be scaled to an integer solution, but a naïve search for integer solutions is not an algorithm. The first section of this writeup discusses *Lagrange's descent method* of seeking solutions of such an equation that satisfies a condition necessary for solutions to exist.

The second section of this writeup discusses *Legendre's theorem* about related ternary quadratic equations, in which a, b, c are nonzero squarefree pairwise coprime integers, not all of the same sign,

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

Legendre gave a condition necessary and sufficient for solutions. More importantly, he showed that solutions exist in $\mathbb{Z}$ if and only if solutions exist modulo n for all odd positive integers n. For this, it suffices by the Sun Ze theorem to establish solutions modulo all odd prime powers. Let $\mathbb{Q}_p$ denote the field of p-adic numbers, and view $\mathbb{R}$ as $\mathbb{Q}_p$ for a non-Archimedean prime p. Legendre's theorem points toward the *Hasse–Minkowski principle* that a quadratic form over $\mathbb{Q}$ in m variables has solutions in $\mathbb{Q}^m$ if and only if it has solutions in $\mathbb{Q}_p^m$ for every prime p. This writeup proves Legendre's theorem in this spirit. The reader who wants only to see a quick, elementary such proof of Legendre's theorem can go straight to section 2 and read into section 2.1. This writeup also gives a second elementary proof of Legendre's theorem, motivated by Lagrange's descent method.

Contents

1. Lagrange's descent method

Consider a class of nondegenerate ternary quadratic equations, in which a, b are nonzero squarefree integers, not both negative,

$$aX^2 + bY^2 = Z^2. \tag{Q}$$

Any solution $(x, y, z) \in \mathbb{Q}^3$ of (Q), understood to be nonzero, can be scaled to an integer solution, but a naïve search for integer solutions is not an algorithm.

A necessary condition for (Q) to have solutions is

$$a, b \text{ are squares modulo } b, a. \tag{C}$$

Indeed, assume that a nonzero solution of (Q) exists, scale it to a primitive integer solution (x, y, z), meaning that $\gcd(x, y, z) = 1$, and make some observations.

- The relation $ax^2 + by^2 = z^2$ shows that x, y, z are pairwise coprime because, for example, if $p \mid x, z$ then $p^2 \mid by^2$ while $p \nmid y$ and so $p^2 \mid b$, contradicting that b is squarefree.
- Consequently x and b are coprime because if $p \mid x, b$ then $p \mid z^2$ and so $p \mid z$, contradicting that x and z are coprime. Now reduce the equality modulo b to get $ax^2 \equiv_b z^2$ with x multiplicatively invertible, and so a is a square modulo b.
- Symmetrically, b is a square modulo a.

Whether condition (C) holds can be determined efficiently by quadratic reciprocity. We explain Lagrange's descent method of seeking solutions of an equation (Q) that satisfies condition (C).

1.1. **Reducing the equation.** Again with a, b nonzero squarefree integers, not both negative, consider an equation that satisfies a necessary condition for solutions to exist,

$$aX^2 + bY^2 = Z^2, \qquad |a| \le |b|, \quad a \text{ is a square modulo } b. \tag{QC}$$

Define the *size* of such an equation, an integer at least 2,

$$|(\mathrm{QC})| = |a| + |b|.$$

If $a = 1$ then the solution $(1, 0, 1)$ is obvious, and similarly if $|(\mathrm{QC})| = 2$ because the only other possibility for this is $-X^2 + Y^2 = Z^2$, with solution $(0, 1, 1)$. Thus we take $a \neq 1$ and $|b| \ge 2$ because otherwise we have a solution.

Using the conditions that a is a square modulo b, that $a \neq 1$, and that a is squarefree, write

$$a = a_o^2 - b\tilde{b}c^2, \quad 0 \le a_o \le \tfrac{1}{2}|b|, \ \tilde{b} \text{ squarefree, } \tilde{b} \text{ and } c \text{ nonzero.} \tag{$a_o\tilde{b}c$}$$

This will require a search for a_o if one doesn't see it by other means, but the search space is finite, half the size of the larger equation coefficient, and if $|b|$ is composite then the search can be facilitated by the Sun Ze theorem. Thus $a, \tilde{b}$ are nonzero squarefree integers, not both negative. Because $|a| \le |b|$ and $|b| \ge 2$,

$$|\tilde{b}| = \left|\frac{a_o^2 - a}{bc^2}\right| \le \left|\frac{a_o^2 - a}{b}\right| \le \frac{|b|}{4} + 1 < |b|$$

and so $|a| + |\tilde{b}| < |a| + |b|$. That is, the quadratic equation

$$aX^2 + \tilde{b}Y^2 = Z^2 \tag{q}$$

is such that $|(\mathrm{q})| < |(\mathrm{Q})|$. Define

$$(a', b') = \begin{cases} (a, \tilde{b}) & \text{if } |a| \le |\tilde{b}| \\ (\tilde{b}, a) & \text{if } |\tilde{b}| < |a|, \end{cases}$$

and now the smaller quadratic equation is

$$a'X^2 + b'Y^2 = Z^2, \qquad |a'| \le |b'|. \tag{q}$$

If $a' = 1$ or $|(\mathrm{q})| = 2$ then this has solutions. If a' is not a square modulo b' then it does not; because a is a square modulo $\tilde{b}$ by $(a_o\tilde{b}c)$, this is possible only if the new absolutely smaller coefficient a' is $\tilde{b}$ rather than a. Otherwise we have a smaller version (qC) of (QC).

1.2. **Simplest binary quadratic form composition law.** A result known in various forms across different cultures since ancient times is now mechanical for us to express and prove by basic algebra,

$$(x^2 + Dy^2)(z^2 + Dw^2) = (xz \pm Dyw)^2 + D(yz \mp xw)^2. \tag{CL}$$

Indeed,

$$\begin{aligned} &(x^2 + Dy^2)(z^2 + Dw^2) \\ &\qquad = (x + \sqrt{-D}y)(x - \sqrt{-D}y)(z \mp \sqrt{-D}w)(z \pm \sqrt{-D}w) \\ &\qquad = (x + \sqrt{-D}y)(z \mp \sqrt{-D}w)(x - \sqrt{-D}y)(z \pm \sqrt{-D}w) \\ &\qquad = \big(xz \pm Dyw + \sqrt{-D}(yz \mp xw)\big)\big(xz \pm Dyw - \sqrt{-D}(yz \mp xw)\big) \\ &\qquad = (xz \pm Dyw)^2 + D(yz \mp xw)^2. \end{aligned}$$

To rephrase this result, if $F(x, y) = x^2 + Dy^2$ then the product of two F-values is another,

$$F(x_1, y_1)F(x_2, y_2) = F(x_3, y_3), \qquad \begin{pmatrix} x_3 = x_1x_2 \pm Dy_1y_2 \\ y_3 = y_1x_2 \mp x_1y_2 \end{pmatrix},$$

or, more concisely,

$$F \cdot F = F.$$

This is the first, most basic *composition law* of binary quadratic forms, hence its designation (CL).

1.3. **Lowering and raising solutions.** Again consider a (QC) equation that could have solutions but isn't known to do so,

$$aX^2 + bY^2 = Z^2, \qquad |a| \le |b|, \quad a \text{ is a square modulo } b, \tag{QC}$$

with $a \ne 1$ and $|a| + |b| \ge 3$. As explained above, a finite search gives rise to a smaller equation (q)

$$ax^2 + \tilde{b}Y^2 = Z^2, \qquad a = a_o^2 - b\tilde{b}c^2, \quad c \ne 0. \tag{q}$$

Now suppose a solution (x, y, z) of the larger equation (QC). Here $y \ne 0$ because $a \ne 1$ and a is squarefree. Compute, using the previous display and the relation $ax^2 + by^2 = z^2$ for the second equality to follow, and using the composition law (CL) with $x, y, w, d = a_o, -1, x, -a$ for the third,

$$\tilde{b}(bcy)^2 = b\tilde{b}c^2 \cdot by^2 = (a_o^2 - a)(z^2 - ax^2) = (a_oz \mp ax)^2 - a(z \mp a_ox)^2.$$

That is,

$$a(z \mp a_o x)^2 + \tilde{b}(bcy)^2 = (a_o z \mp ax)^2.$$

and we have a solution of the smaller equation (q),

$$(\tilde{x}, \tilde{y}, \tilde{z}) = (z \mp a_o x, bcy, a_o z \mp ax),$$

nonzero because $bcy \neq 0$.

Conversely, suppose a solution $(\tilde{x}, \tilde{y}, \tilde{z})$ of (q), freely scaled to an integer solution such that $a - a_o^2$ divides $\tilde{x}$ and $\tilde{z}$ while bc divides $\tilde{y}$. Inverting the relations from lowering a solution, define

$$(x, y, z) = \left(\frac{\tilde{z} - a_o \tilde{x}}{a - a_o^2}, \frac{\tilde{y}}{bc}, \frac{a\tilde{x} - a_o \tilde{z}}{a - a_o^2} \right).$$

Inevitably (x, y, z) solves (QC) but we confirm this,

$$\begin{aligned} ax^2 + by^2 &= a\frac{(\tilde{z} - a_o\tilde{x})^2}{(a - a_o^2)^2} + \frac{\tilde{y}^2}{bc^2} = \frac{a(\tilde{z} - a_o\tilde{x})^2}{(a - a_o^2)^2} - \frac{b'\tilde{y}^2}{a - a_o^2} \\ &= \frac{a(\tilde{z} - a_o\tilde{x})^2 + (a - a_o^2)(a\tilde{x}^2 - \tilde{z}^2)}{(a - a_o^2)^2} \\ &= \frac{-2aa_o\tilde{z}\tilde{x} + a^2\tilde{x}^2 + a_o^2\tilde{z}^2}{(a - a_o^2)^2} = \frac{(a\tilde{x} - a_o\tilde{z})^2}{(a - a_o^2)^2} \\ &= z^2. \end{aligned}$$

1.4. **Solving an equation $aX^2 + bY^2 = Z^2$.** Overall, the situation is as follows.

- The equation (QC) with coefficients a, b has been reduced to a smaller equation (q) with coefficients $a, \tilde{b}$, and these have been renamed a', b' with $|a'| \leq |b'|$.
- Solutions of (QC) give solutions of (q) by lowering. Thus, if (q) has no solutions then neither does (QC).
- Solutions of (q) give solutions of (QC) by raising.

In light of these facts, consider an equation (QC). Lagrange's descent method is as follows.

- If $a' = 1$ or $|(\text{q})| = 2$ then we know solutions of (q), and they give solutions of (QC).
- If a' is not a square modulo b' then (q) has no solutions, and so neither does (QC) by the second bullet just above.
- Otherwise we have a smaller problem (qC) of the same sort that we started with, and if it has solutions then they give solutions of (QC) by the third bullet just above.

Legendre's theorem, discussed in the second section of this writeup, shows that a little more care with condition (C) ensures that the second possibility just listed can never occur, and so Lagrange's descent method will always find a solution.

For example, take $a = 101$ and $b = 211$, the first primes after 100 and 200. To study

$$(*) \qquad 101X^2 + 211Y^2 = Z^2,$$

compute by quadratic reciprocity that $(101/211) = (211/101) = (9/101) = 1$, and then search to find

$$101 = 34^2 - 211 \cdot 5 \cdot 1^2, \qquad \text{so } a_o, \tilde{b}, c = 34, 5, 1,$$

and the resulting quadratic equation is

$$5X^2 + 101Y^2 = Z^2. \tag{$**$}$$

By quadratic reciprocity, $(5/101) = (101/5) = (1/5) = 1$, and then another search gives

$$5 = 45^2 - 101 \cdot 5 \cdot 2^2, \qquad \text{so } a_o, \tilde{b}, c = 45, 5, 2,$$

and now the resulting equation is

$$5X^2 + 5Y^2 = Z^2.$$

Because $2^2 + 1^2 = 5$ this has solution $(2, 1, 5)$,

$$5 \cdot 2^2 + 5 \cdot 1^2 = 5^2.$$

Raising gives a solution $(17, 2, 43)$ of $(**)$,

$$5 \cdot 17^2 + 101 \cdot 2^2 = 43^2,$$

and raising again gives a solution $(5, 17, 252)$ of $(*)$,

$$101 \cdot 5^2 + 211 \cdot 17^2 = 252^2.$$

2. Legendre's theorem

A convenient abbreviation will be in effect for the rest of this writeup: for any two integers d, n,

$$d \,\mathrm{S}\, n \text{ means that } d \text{ is a square modulo } n\mathbb{Z}.$$

Here d could be 0 modulo n. Although the conditions $d \,\mathrm{S}\, n$ and $d \,\mathrm{S}\, -n$ are equivalent, the conditions $d \,\mathrm{S}\, n$ and $-d \,\mathrm{S}\, n$ need not be. The relation $d \,\mathrm{S}\, n$ is not the same as $(d/n) \geq 0$ with the Legendre–Jacobi–Kronecker symbol; for example, -1 is not a square modulo 21 even though $(-1/21) = 1$, and 3 is a square modulo 2 even though $(3/2) = -1$, We make an observation for future reference:

$$(\mathrm{S}\, km) \qquad \text{Let } k \text{ and } m \text{ be coprime. If } d \,\mathrm{S}\, k \text{ and } d \,\mathrm{S}\, m \text{ then } d \,\mathrm{S}\, km.$$

Indeed, given d such that $d \equiv_k a^2$ and $d \equiv_m b^2$, the existence statement in the Sun Ze theorem gives some c such that $c \equiv_k a$ and $c \equiv_m b$; thus $d \equiv_k c^2$ and $d \equiv_m c^2$, so the uniqueness statement in the Sun Ze theorem says that $d \equiv_{km} c^2$ as desired. The converse of $(\mathrm{S}\, km)$, that if $d \,\mathrm{S}\, km$ then $d \,\mathrm{S}\, k$ and $d \,\mathrm{S}\, m$, is immediate, not even requiring k and m to be coprime.

Legendre studied nondegenerate ternary quadratic equations over $\mathbb{Q}$. These can be reduced to the diagonal case with coefficients a, b, c that are nonzero squarefree pairwise coprime integers, not all of the same sign,

$$aX^2 + bY^2 + cZ^2 = 0. \tag{Q Le}$$

Legendre's famous result can be phrased in two ways: (Q Le) has solutions in $\mathbb{Z}^3$ if and only if

$$-bc \,\mathrm{S}\, a, \ -ca \,\mathrm{S}\, b, \ -ab \,\mathrm{S}\, c \tag{C Le}$$

or

(C′ Le) (Q Le) has compatible solutions modulo all odd positive integers n.

Here *compatible* means that if $n \mid m$ then the solutions (x_n, y_n, z_n) modulo n and (x_m, y_m, z_m) modulo m satisfy $(x_m, y_m, z_m) \equiv_n (x_n, y_n, z_n)$.

The necessity of (C Le) is easy to show. If $ax^2+by^2+cz^2 = 0$ with x, y, z coprime integers, not all zero, then they are pairwise coprime because, for example, with p prime, if $p \mid x, y$ then $p^2 \mid cz^2$ and so $p^2 \mid c$, impossible because c is squarefree; it follows that y and a are coprime because if $p \mid y, a$ then $p \mid z^2$ and therefore $p \mid z$, impossible because y and z are coprime. Multiply $ax^2 + by^2 + cz^2 = 0$ by $-c$ and reduce modulo a to get $-bcy^2 \equiv_a c^2z^2$, and so $-bc \,\mathrm{S}\, a$ because y^2 is invertible modulo a. The rest of (C Le) follows symmetrically.

The necessity of (C′ Le) is immediate from a primitive integral root of $F(X, Y, Z)$.

We prove Legendre's theorem by showing the sufficiency of (C Le). After the proof we show that (C Le) and (C′ Le) are equivalent.

2.1. **Proof of Legendre's theorem.** Again with a, b, c nonzero squarefree pairwise coprime integers, not all of the same sign, assume now that also $-bc \,\mathrm{S}\, a$, $-ca \,\mathrm{S}\, b$, and $-ab \,\mathrm{S}\, c$. Define

$$F(X, Y, Z) = aX^2 + bY^2 + cZ^2.$$

Legendre's theorem is that $F(X, Y, Z)$ has nonzero integral roots (x, y, z).

If any two of $|a|, |b|, |c|$ are 1 then such a root of $F(X, Y, Z)$ is immediate because

- $\pm 1 \mp 1 = 0$
- if $a = b = 1$ and $c < 0$ then the condition $-ab \,\mathrm{S}\, c$ is $-1 \,\mathrm{S}\, -c$; this makes $-c$ a product of distinct primes $p = 2$ or $p \equiv_4 1$, each a sum of two squares, and so $-c$ is a sum of squares by the composition law (CL) with $D = 1$ on page 3, $x^2 + y^2 + c = 0$.

Thus, to prove Legendre's theorem we may freely assume that none of $|bc|, |ca|, |ab|$ is a perfect square, and so none of $\sqrt{|bc|}, \sqrt{|ca|}, \sqrt{|ab|}$ is an integer.

The coming proof of the theorem uses a fact about the values taken by F, so we establish it in advance. A small composition law for binary quadratic forms comes from using basic algebra to cancel two cross terms,

$$a(X + bY)^2 + b(Y - aX)^2 = (1 + ab)(aX^2 + bY^2).$$

Add $c(1 + ab)^2$ to both sides to get

$$a(X + bY)^2 + b(Y - aX)^2 + c(1 + ab)^2 = (1 + ab)(aX^2 + bY^2 + c + abc),$$

and then homogenize this to a quintic relation in a, b, c, X, Y, Z,

$$F(XZ + bY, YZ - aX, Z^2 + ab) = (Z^2 + ab)(F(X, Y, Z) + abc).$$

Freely assuming that a and b have the same sign, so that $Z^2 + ab$ is never 0, this shows:

If F takes the value $-abc$ then F takes the value 0.

The previous displayed equality homogenizes to a quartic relation in X, Y, Z, W, but we have no need for it. Now we prove Legendre's theorem.

Proof. From the condition $-bc \,\mathrm{S}\, a$ there exists y_o such that $-bc \equiv_a y_o^2$. Compute, taking c^{-1} modulo a in the next display,

$$F(X, Y, Z) \equiv_a bY^2 + cZ^2 \equiv_a -c^{-1}(y_oY + cZ)(y_oY - cZ).$$

(Consequently $F(0, \pm y_o, b) \equiv_a 0$, but we do not even need this.) That is, for two integral linear forms $L_a(X, Y, Z)$ and $L'_a(X, Y, Z)$, in which X incidentally does not appear,

$$F(X, Y, Z) \equiv_a L_a(X, Y, Z)L'_a(X, Y, Z).$$

Similarly for b and c. Now the Sun Ze theorem gives integral linear forms $L(X,Y,Z)$ and $L'(X,Y,Z)$ such that

$$F(X,Y,Z) \equiv_{abc} L(X,Y,Z)L'(X,Y,Z).$$

Consider a set of finitely many integer triples,

$$I = \{(x,y,z) \in \mathbb{Z}^3 : 0 \le x \le \lfloor\sqrt{|bc|}\rfloor,\ 0 \le y \le \lfloor\sqrt{|ca|}\rfloor,\ 0 \le z \le \lfloor\sqrt{|ab|}\rfloor\}.$$

As noted, we may assume that none of these square roots is an integer. Thus,

$$|I| = (\lfloor\sqrt{|bc|}\rfloor + 1)(\lfloor\sqrt{|ca|}\rfloor + 1)(\lfloor\sqrt{|ab|}\rfloor + 1) > \sqrt{|bc|}\sqrt{|ca|}\sqrt{|ab|} = |abc|.$$

This says that there exist two distinct triples (x_1,y_1,z_1) and (x_2,y_2,z_2) in I such that $L(x_1,y_1,z_1) \equiv_{abc} L(x_2,y_2,z_2)$. So with $x = x_1 - x_2$, $y = y_1 - y_2$, and $z = z_1 - z_2$ a nonzero triple in $\mathbb{Z}^3$, the linearity of L gives

$$L(x,y,z) \equiv_{abc} 0, \qquad |x| < \sqrt{|bc|},\ |y| < \sqrt{|ca|},\ |z| < \sqrt{|ab|}.$$

Because $F(X,Y,Z)$ is a multiple of $L(X,Y,Z)$ modulo abc, and because we may freely take a,b to be negative and c positive in $F(X,Y,Z) = aX^2 + bY^2 + cZ^2$,

$$F(x,y,z) \equiv_{abc} 0, \qquad -2|abc| < F(x,y,z) < |abc|.$$

There are only two possibilities,

$$F(x,y,z) = 0 \quad \text{or} \quad F(x,y,z) = -abc.$$

As shown above, if the second holds then $F(x',y',z') = 0$ for some (x',y',z') with $z' \neq 0$. So either way, the proof is complete. □

With Legendre's theorem proven, we know that each of its alternative hypothesized conditions (C Le) and (C′ Le) implies the other, but we show these implications directly. First assume (C Le), i.e., $-bc \,\square\, a$, $-ca \,\square\, b$, and $-ab \,\square\, c$. We show that $F(X,Y,Z)$ has compatible nonzero roots modulo all powers of all odd primes; compatible nonzero roots modulo all odd positive integers follow by the Sun Ze theorem.

For an odd prime divisor p of a, the proof of Legendre's theorem showd that $F(0,\pm y_o,b) \equiv_p 0$ for some y_o. Further, $\mathrm{D}_3F(0,\pm y_o,b) = 2bc \not\equiv_p 0$ because p is odd along with being coprime to bc, so Hensel's lemma gives compatible roots $(x,y,z) \equiv_p (0,\pm y_o,b)$ of $F(X,Y,Z)$ modulo all powers of p. And symmetrically for an odd prime divisor of b or c.

Now consider an odd prime $p \nmid abc$. Following Euler, define two functions from $\mathbb{F}_p$ to $\mathbb{F}_p$,

$$t \longmapsto at^2, \qquad t \longmapsto -bt^2 - c.$$

Because t^2 runs through $\frac{p+1}{2}$ outputs, these being 0 and the nonzero squares, each function has $\frac{p+1}{2}$ outputs, and so the two functions share an output. That is, there exist integers x_o, y_o such that $F(x_0,y_o,1) \equiv_p 0$. Here x_o, y_o cannot both be 0 modulo p because c is not, so at least one of $\mathrm{D}_1F(x_o,y_o,1) = 2ax_o$ and $\mathrm{D}_2F(x_o,y_o,1) = 2by_o$ is nonzero modulo p, and again Hensel's lemma gives compatible roots $(x,y,z) \equiv_p (x_o,y_o,1)$ of $F(X,Y,Z)$ modulo all powers of p.

Conversely, (C′ Le) implies (C Le) as follows. Let p be an odd prime divisor of a. Consider a nonzero root (x,y,z) of $F(X,Y,Z)$ modulo p from (C′ Le). Here p cannot divide both y and z because this root is compatible with a root modulo p^2; indeed if $p \mid y,z$ then $F(x+kp, y+\ell p, z+mp) \equiv_{p^2} ax(x+2kp)$, and for this to be 0 modulo p^2 requires $p \mid x$ because a is squarefree, contradicting that (x,y,z)

is nononzero modulo p. Now the relation $F(x,y,z) \equiv_p 0$ is $by^2 + cz^2 \equiv_p 0$ with y or z not divisible by p. If $p \nmid y$ then this relation is $-c^{-1}(-bcy^2 - (cz)^2) \equiv_p 0$ and so $-bc \,\mathrm{S}\, p$, and similarly if $p \nmid z$. And certainly $-bc \,\mathrm{S}\, 2$. Thus $-bc \,\mathrm{S}\, p$ for all prime divisors p of the squarefree a, including $p = 2$ if necessary, and so by the observation ($\mathrm{S}\, km$) on page 5, $-bc \,\mathrm{S}\, a$. Symmetrically, $-ca \,\mathrm{S}\, b$ and $-ab \,\mathrm{S}\, c$. This argument shows that (C′ Le) could require only that $F(X,Y,Z)$ have compatible roots modulo the first and second powers of each odd prime divisor of abc.

Although compatible roots of $F(X,Y,Z)$ modulo all odd prime powers are not needed to prove Legendre's theorem, the fact of their ready existence and their sufficiency for a root in $\mathbb{Z}^3$ is arguably the theorem's significance. It suggests the general idea of establishing *local* solutions of a problem, meaning compatible solutions modulo all prime powers p^e, which is to say roots in $\mathbb{Q}_p$ for all primes p, and then using the local roots to synthesize *global* roots in $\mathbb{Q}$. These ideas lead to general theorems about quadratic forms over arbitrary number fields and their completions.

2.2. **Second proof of Legendre's theorem.** Another elementary proof of Legendre's theorem, motivated by Lagrange's descent method, is frequent in the literature and so we give it here. This argument is a global proof by induction.

We have considered a class of nondegenerate ternary quadratic equations, those with a, b nonzero squarefree integers, not both negative, and $c = -1$,

$$aX^2 + bY^2 = Z^2, \tag{Q La}$$

Decompose a and b to separate out their overlap,

$$g = \gcd(a,b) > 0, \quad a = a'g, \quad b = b'g, \quad a', b', g \text{ pairwise coprime.}$$

This notation will be in effect throughout. We show that a necessary condition for (Q La) to have solutions is

$$a \,\mathrm{S}\, b,\ b \,\mathrm{S}\, a,\ -a'b' \,\mathrm{S}\, a,\ -a'b' \,\mathrm{S}\, b. \tag{C La}$$

The first two parts of the condition were already established at the beginning of section 1. For the third and fourth parts, multiply (Q La) by $a = a'g$ and then scale and rename the indeterminates to get $-a'b'X^2 + aY^2 = Z^2$. Because $-a'b'$ and a are nonzero squarefree integers, not both negative, we know that a solution requires $-a'b' \,\mathrm{S}\, a$, and $-a'b' \,\mathrm{S}\, b$ symmetrically.

With the necessity of condition (C La) for (Q La) solutions established, consider a second condition,

$$a \,\mathrm{S}\, b',\ b \,\mathrm{S}\, a',\ -a'b' \,\mathrm{S}\, g. \tag{c La}$$

Clearly (C La) implies (c La). We show that also (c La) implies (C La), so that the two conditions are equivalent. To see so, first add some trivial conditions to (c La), trivial because $a = a'g$ and $b = b'g$,

$$\text{(c La)} \quad a \,\mathrm{S}\, b',\ a \,\mathrm{S}\, g, \quad b \,\mathrm{S}\, a',\ b \,\mathrm{S}\, g, \quad -a'b' \,\mathrm{S}\, a',\ -a'b' \,\mathrm{S}\, g, \quad -a'b' \,\mathrm{S}\, b',\ -a'b' \,\mathrm{S}\, g.$$

Because a', b', g are pairwise coprime, the observation ($\mathrm{S}\, km$) on page 5 and its converse say that this augmented (c La) is

$$a \,\mathrm{S}\, b'g,\ b \,\mathrm{S}\, a'g,\ -a'b' \,\mathrm{S}\, a'g,\ -a'b' \,\mathrm{S}\, b'g, \tag{c La}$$

and because $a'g = a$ and $b'g = b$, this is (C La).

In the example $3X^2 + 3Y^2 = Z^2$, with $a', b', g = 1, 1, 3$, the condition $a \,\mathrm{S}\, b'$ is $3 \,\mathrm{S}\, 1$, which is true, making $b \,\mathrm{S}\, a'$ true as well by symmetry, but $-a'b' \,\mathrm{S}\, g$ is $-1 \,\mathrm{S}\, 3$, which is false. So the two first conditions of the first statement of (c La) above do not generally imply the third. A Lagrange descent step turns this example into $-X^2 + 3Y^2 = Z^2$, which has no solutions because -1 is not a square modulo 3. Alternatively, scale the example by 3 and then absorb 3 into X and Y and the example becomes $X^2 + Y^2 - 3Z^2 = 0$, with $a, b, c = 1, 1, -3$, which has no solutions by Legendre's theorem, again because -1 is not a square modulo 3. Either way, this example has no solutions despite satisfying $a \,\mathrm{S}\, b$ and $b \,\mathrm{S}\, a$.

Now consider two classes of ternary quadratic equations with accompanying conditions. First, with $\hat{a}, \hat{b}, \hat{c}$ nonzero squarefree pairwise coprime integers, not all positive but $\hat{c} > 0$,

$$\text{(QC Le)} \qquad \hat{a}X^2 + \hat{b}Y^2 + \hat{c}Z^2 = 0, \qquad -\hat{b}\hat{c} \,\mathrm{S}\, \hat{a},\ -\hat{c}\hat{a} \,\mathrm{S}\, \hat{b},\ -\hat{a}\hat{b} \,\mathrm{S}\, \hat{c}.$$

Second, with a, b nonzero squarefree integers, not both negative,

$$\text{(Qc La)} \qquad aX^2 + bY^2 = Z^2 \qquad a \,\mathrm{S}\, b',\ b \,\mathrm{S}\, a',\ -a'b' \,\mathrm{S}\, g.$$

We show that these two classes of equations transform to each other.

Given a (QC Le) equation, define

$$(a, b) = (-\hat{a}\hat{c}, -\hat{b}\hat{c}) \qquad (\text{so } g = \hat{c}).$$

with a, b squarefree and not both negative, and the equation is

$$-a/gX^2 - b/gY^2 + gZ^2 = 0, \qquad b \,\mathrm{S}\, a',\ a \,\mathrm{S}\, b',\ -a'b' \,\mathrm{S}\, g.$$

Multiply through by $-g$ and absorb a factor into the third indeterminate to get

$$aX^2 + bY^2 = Z^2, \qquad b \,\mathrm{S}\, a',\ a \,\mathrm{S}\, b',\ -a'b' \,\mathrm{S}\, g.$$

This is a (Qc La) equation.

Conversely, given a (Qc La) equation, define

$$(\hat{a}, \hat{b}, \hat{c}) = (-a', -b', g).$$

which are pairwise coprime and not all positive but with $\hat{c} > 0$, and the equation is

$$-\hat{a}\hat{c}X^2 - \hat{b}\hat{c}Y^2 - Z^2 = 0, \qquad -\hat{a}\hat{c} \,\mathrm{S}\, \hat{b},\ -\hat{b}\hat{c} \,\mathrm{S}\, \hat{a},\ -\hat{a}\hat{b} \,\mathrm{S}\, \hat{c}.$$

Multiply through by $-\hat{c}$ and absorb scale factors into the first two indeterminates to get

$$\hat{a}X^2 + \hat{b}Y^2 + \hat{c}Z^2 = 0, \qquad -\hat{a}\hat{c} \,\mathrm{S}\, \hat{b},\ -\hat{b}\hat{c} \,\mathrm{S}\, \hat{a},\ -\hat{a}\hat{b} \,\mathrm{S}\, \hat{c}.$$

This is a (QC Le) equation.

The transformation from (QC Le) to (Qc La) and back, with $g = \hat{c}$ after the first step, is

$$(\hat{a}, \hat{b}, \hat{c}) \longmapsto (-\hat{a}\hat{c}, -\hat{b}\hat{c}) \longmapsto (-(-\hat{a}\hat{c})/\hat{c}, -(-\hat{b}\hat{c})/\hat{c}, \hat{c}) = (\hat{a}, \hat{b}, \hat{c}),$$

and similarly from (Qc La) to (QC Le) and back,

$$(a, b) \longmapsto (-a', -b', g) \longmapsto (-(-a')g, -(-b')g) = (a, b).$$

Thus the question of whether an equation (Q Le) satisfying condition (C Le) has solutions is the same question for an equation (Q La) satisfying condition (c La). And we have established that condition (c La) is equivalent to condition (C La).

Again with a and b nonzero squarefree integers, not both negative, consider equations

$$\text{(QC La)} \qquad aX^2 + bY^2 = Z^2, \qquad a \,\mathrm{S}\, b,\ b \,\mathrm{S}\, a,\ -a'b' \,\mathrm{S}\, a,\ -a'b' \,\mathrm{S}\, b.$$

Legendre's theorem is that all equations (QC La) have solutions, meaning nonzero solutions in $\mathbb{Q}^3$. Recall the notation $g = \gcd(a, b)$, $a = a'g$, $b = b'g$, and recall that the fourfold condition (C La) accompanying the equation is equivalent to the threefold condition $a \,\mathrm{S}\, b'$, $b \,\mathrm{S}\, a'$, $-a'b' \,\mathrm{S}\, g$, denoted (c La), and recall that the size of a (QC La) equation is an integer, $|(\text{QC La})| = |a| + |b| \geq 2$. Define the set of sizes where our desired conclusion holds,

$$S = \{n \in \mathbb{Z}_{\geq 2} : \text{all equations (QC La) of size } n \text{ have solutions}\}.$$

We show by induction that S is all of $\mathbb{Z}_{\geq 2}$.

Proof. Every equation (QC La) of size 2 has $a = 1$ or $b = 1$ or both (in fact these are all the equations (Q La) of size 2). Thus the base case $2 \in S$ of the induction holds.

For the induction step of the argument, consider some $n \in \mathbb{Z}_{\geq 2}$ and suppose that $\{2, \ldots, n\} \subset S$. We need to show that consequently $n+1 \in S$. Consider a (QC La) equation $aX^2 + bY^2 = Z^2$ of size $n + 1$. Take $|a| \leq |b|$ without loss of generality. If $a = 1$ then this equation has solutions, so take $a \neq 1$. Use the condition $a \,\mathrm{S}\, b$ to write as in Lagrange's descent method

$$(a_o\tilde{b}c) \qquad a = a_o^2 - b\tilde{b}c^2, \quad 0 \leq a_o \leq \tfrac{1}{2}|b|,\ \tilde{b} \text{ squarefree}.$$

As explained already, $a \neq a_o^2$ and so $\tilde{b} \neq 0$ and $c \neq 0$, and the size of $aX^2 + \tilde{b}Y^2 = Z^2$ is less than the size $n+1$ of $aX^2 + bY^2 = Z^2$. Thus the smaller size lies in $\{2, \ldots, n\}$ and therefore in S. Note for future reference that $(a_o\tilde{b}c)$ gives $\gcd(c, a) = 1$. Indeed, if $p \mid c, a$ with p prime then $(a_o\tilde{b}c)$ says that $p \mid a_o^2$, and so $p \mid a_o$ and then $p^2 \mid a_o^2$, and now $(a_o\tilde{b}c)$ says that $p^2 \mid a$, contradicting that a is squarefree. Thus $\gcd(c, a) = 1$ as asserted.

We show that the equation $aX^2 + \tilde{b}Y^2 = Z^2$ again satisfies (C La). As discussed above, we need to show only that it satisfies (c La). Our bigger equation is (QC La), and we use part of its (C La) condition beyond (c La),

$$a \,\mathrm{S}\, b,\ b \,\mathrm{S}\, a,\ -a'b' \,\mathrm{S}\, g.$$

Similarly to the earlier definitions $g = \gcd(a, b)$, $a = a'g$, $b = b'g$, now define

$$\tilde{g} = \gcd(a, \tilde{b}), \qquad a = \tilde{a}'\tilde{g}, \qquad \tilde{b} = \tilde{b}'\tilde{g},$$

with $\tilde{a}', \tilde{b}', \tilde{g}$ squarefree and pairwise coprime. What we need to show is

$$a \,\mathrm{S}\, \tilde{b}',\ \tilde{b} \,\mathrm{S}\, \tilde{a}',\ -\tilde{a}'\tilde{b}' \,\mathrm{S}\, \tilde{g}.$$

The $(a_o\tilde{b}c)$ equality $a = a_o^2 - b\tilde{b}c^2$ immediately gives $a \,\mathrm{S}\, \tilde{b}$, and $a \,\mathrm{S}\, \tilde{b}'$ follows.

To show that $\tilde{b} \,\mathrm{S}\, \tilde{a}'$, we will show that $\tilde{b} \,\mathrm{S}\, g$ and $\tilde{b} \,\mathrm{S}\, a'$, so that $\tilde{b} \,\mathrm{S}\, a$. Substitute $a = a'g$, $b = b'g$ in the $(a_o\tilde{b}c)$ equality $a = a_o^2 - b\tilde{b}c^2$ to get

$$a'g = a_o^2 - b'g\tilde{b}c^2,$$

and this gives $g \mid a_o^2$, from which $g \mid a_o$ because g is squarefree. Substitute $a_o^2 = {a_o'}^2 g^2$ and then divide through by g to get

$$a' = {a_o'}^2 g - b'\tilde{b}c^2.$$

Here $\gcd(c, g) = 1$ because $\gcd(c, a) = 1$. Reduce the previous display modulo g and multiply through by $-b'$ to get

$$b'^2\tilde{b}c^2 \equiv_g -a'b'.$$

Because $-a'b' \,\mathrm{S}\, g$ this gives $b'^2\tilde{b}c^2 \,\mathrm{S}\, g$, and so $\tilde{b} \,\mathrm{S}\, g$ because $\gcd(b'^2c^2, g) = 1$. The $(a_o\tilde{b}c)$ equality $a = a_o^2 - b\tilde{b}c^2$ also gives

$$b\tilde{b}c^2 \equiv_{a'} a_o^2.$$

Because $b \,\mathrm{S}\, a'$ and $\gcd(bc^2, a') = 1$, this gives $\tilde{b} \,\mathrm{S}\, a'$. Also $\tilde{b} \,\mathrm{S}\, g$ and $\gcd(a', g) = 1$, so the observation $(\mathrm{S}\, km)$ on page 5 gives $\tilde{b} \,\mathrm{S}\, a$, and therefore $\tilde{b} \,\mathrm{S}\, \tilde{a}'$ as desired. (Note: The equality $a = a_o^2 - b\tilde{b}c^2$ immediately gives $b\tilde{b}c^2 \,\mathrm{S}\, \tilde{a}'$, and $b\tilde{b} \,\mathrm{S}\, \tilde{a}'$ follows because $\gcd(c, \tilde{a}') = 1$, and $b \,\mathrm{S}\, \tilde{a}'$ holds because $b \,\mathrm{S}\, a$ is assumed, but it can be shown that g divides $\tilde{a}'$ along with dividing b, so this doesn't lead to the desired $\tilde{b} \,\mathrm{S}\, \tilde{a}'$. The argument in this paragraph that $\tilde{b} \,\mathrm{S}\, \tilde{a}'$ because $\tilde{b} \,\mathrm{S}\, g$ and $\tilde{b} \,\mathrm{S}\, a'$ and therefore $\tilde{b} \,\mathrm{S}\, a$ may really be necessary.)

To show that $-\tilde{a}'\tilde{b}' \,\mathrm{S}\, \tilde{g}$, substitute $a = \tilde{a}'\tilde{g}$, $\tilde{b} = \tilde{b}'\tilde{g}$ in $a = a_o^2 - b\tilde{b}c^2$ to get

$$\tilde{a}'\tilde{g} = a_o^2 - b\tilde{b}'\tilde{g}c^2,$$

and this gives $\tilde{g} \mid a_o^2$, from which $\tilde{g} \mid a_o$ because $\tilde{g}$ is squarefree. Consequently $\gcd(b, \tilde{g}) = 1$ because any common factor would divide $\tilde{a}'\tilde{g} = a$ twice, impossible because a is squarefree. In the previous display, substitute $a_o = \tilde{a}_o\tilde{g}$ and then multiply through by $\tilde{a}'$ and divide through by $\tilde{g}$ to get

$$(\tilde{a}')^2 = \tilde{a}'\tilde{a}_o^2\tilde{g} - b\tilde{a}'\tilde{b}'c^2,$$

from which

$$-b\tilde{a}'\tilde{b}'c^2 \equiv_{\tilde{g}} (\tilde{a}')^2.$$

Because $b \,\mathrm{S}\, a$ it follows that $b \,\mathrm{S}\, \tilde{g}$. This gives the desired result that $-\tilde{a}'\tilde{b}' \,\mathrm{S}\, \tilde{g}$ because $\gcd(bc^2, \tilde{g}) = 1$.

Overall, $aX^2 + \tilde{b}Y^2 = Z^2$ satisfies condition (c La) and its size lies in S, so by the inductive hypothesis it has solutions. We have seen in Lagrange's descent method that its solutions lift to solutions of the (QC La) equation $aX^2 + bY^2 = Z^2$ of size $n + 1$. Thus $n + 1 \in S$. This completes the proof by induction that S is all of $\mathbb{Z}_{\geq 2}$. □

With no reference to induction, if $a = b$ then (QC La) has solutions. Indeed, if $a = b$ then the third part $-a'b' \,\mathrm{S}\, g$ of (c La) is $-1 \,\mathrm{S}\, a$. As explained at the beginning of section 2.1, this makes a a sum of two squares. With $a = r^2 + s^2$, a solution of $aX^2 + aY^2 = Z^2$ is (r, s, a),

$$ar^2 + as^2 = a(r^2 + s^2) = a^2.$$

We saw a particular instance of this earlier for the equation $5X^2 + 5Y^2 = Z^2$.