11.1 Quadratic forms over $\mathbb{Q}_p$

The Hasse-Minkowski theorem reduces the problem of determining whether a quadratic form f over $\mathbb{Q}$ represents 0 to the problem of determining whether f represents zero over $\mathbb{Q}_p$ for all $p \leq \infty$. At first glance this might not seem like progress, since there are infinitely many p to check, but in fact we only need to check $p = 2$, $p = \infty$ and a finite set of odd primes.

Theorem 11.1. *Let p be an odd prime and let f be a diagonal quadratic form of dimension $n > 2$ with coefficients $a_1, \dots, a_n \in \mathbb{Z}_p^\times$. Then f represents 0 over $\mathbb{Q}_p$.*

Proof. The equation $f(x_1, \dots, x_n) \equiv 0 \bmod p$ is a homogeneous equation of degree 2 in $n > 2$ variables over $\mathbb{F}_p$. It follows from the Chevalley-Warning theorem that it has a non-trivial solution $(y_1, \dots, y_n)$ over $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$. Assume without loss of generality that $y_1 \neq 0$ and let $g(z)$ be the univariate polynomial $g(y) = f(y, y_2, \dots, y_n)$ over $\mathbb{Z}_p$. Then $g(y_1) \equiv 0 \bmod p$ and $g'(y_1) = 2a_1y_1 \not\equiv 0 \bmod p$, so by Hensel's lemma there is a root z_1 of $g(y)$ over $\mathbb{Z}_p$. We then have $f(z_1, y_2, \dots, y_n) = g(z_1) = 0$, so f represents 0 over $\mathbb{Q}_p$. □

Corollary 11.2. *Every quadratic form of dimension $n > 2$ over $\mathbb{Q}$ represents 0 over $\mathbb{Q}_p$ for all but finitely many primes p.*

Proof. In diagonal form the coefficients $a_1, \dots, a_n$ lie in $\mathbb{Z}_p^\times$ for all odd $p \nmid a_1 \cdots a_n$. □

For quadratic forms of dimension $n \leq 2$, we note that a nondegenerate unary form never represents 0, and the nondegenerate form $ax^2 + by^2$ represents 0 if and only if $-ab$ is square (this holds over any field). But when $-ab$ is not square it may still be the case that $ax^2 + by^2$ represents a given nonzero element t, and having a criterion for identifying such t will be useful in our proof of the Hasse-Minkowski theorem.

Lemma 11.3. *The nondegenerate quadratic form $ax^2 + by^2$ over $\mathbb{Q}_p$ represents $t \in \mathbb{Q}_p^*$ if and only if $(a, b)_p = (t, -ab)_p$.*

Proof. Since $t \neq 0$, the equation $ax^2 + by^2 = t$ has a non-trivial solution in $\mathbb{Q}_p$ if and only if $(a/t)x^2 + (b/t)y^2 = 1$ has a solution, which is equivalent to $(a/t, b/t)_p = 1$. We have

$$\begin{aligned}(a/t, b/t)_p &= (at, bt)_p = (a, bt)_p(t, bt)_p = (a, b)_p(a, t)_p(t, bt) = (a, b)_p(t, abt)_p \\ &= (a, b)_p(t, abt)_p(t, -t)_p = (a, b)_p(t, -ab)_p,\end{aligned}$$

where we have used that the Hilbert symbol is symmetric, bilinear, invariant on square classes, and satisfies $(x, -x)_p = 1$. Thus $(a/t, b/t)_p = 1$ if and only if $(a, b)_p(t, -ab)_p = 1$, which is equivalent to $(a, b)_p = (t, -ab)_p$ since both are ± 1. □

Corollary 11.4. *The nondegenerate form $ax^2 + by^2 + cz^2$ over $\mathbb{Q}_p$ represents 0 if and only if $(a, b)_p = (-c, -ab)_p$*

Proof. By the lemma, if suffices to show that $ax^2 + by^2 + cz^2$ represents 0 if and only if the binary form $ax^2 + by^2$ represents $-c$. The reverse implication is clear (set $z = 1$). For the forward implication, if $ax_0^2 + by_0^2 + cz_0^2 = 0$ then either $z_0 \neq 0$, in which case $a(x_0/z_0^2) + b(y_0/z_0)^2 = -c$ or $z_0 = 0$ in which case $ax^2 + by^2$ represents 0 and therefore every element of $\mathbb{Q}_p$, including $-c$. □

Corollary 11.5. *A ternary quadratic form over $\mathbb{Q}$ that represents 0 over all but at most one completion of $\mathbb{Q}$ represents 0 over every completion of $\mathbb{Q}$.*

Proof. The corollary is trivially true if the form is degenerate and otherwise it follows from the product formula for Hilbert symbols and the corollary above. □

11.2 Approximation

We now prove two *approximation theorems* that we will need to prove the Hasse-Minkowski theorem for $\mathbb{Q}$. These are quite general theorems that have many applications, but we will state them in a particularly simple form that suffices for our purposes here. Before proving them we first note/recall that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ and $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

Theorem 11.6. *Let $p \le \infty$ be any prime of $\mathbb{Q}$. Under the metric $d(x,y) = |x-y|_p$, the set $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ and the set $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.*

Proof. We know that $\mathbb{Q}_\infty = \mathbb{R}$ is the completion of $\mathbb{Q}$ and we proved that $\mathbb{Q}_p$ is (isomorphic to) the completion of $\mathbb{Q}$ for $p < \infty$, and any field is dense in its completion (this follows immediately from the definition). We note that the completion $\mathbb{Z}_\infty = \mathbb{Z}$ (any Cauchy sequence of integers must be eventually constant), and for $p < \infty$ the we can apply the fact that $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \le 1\}$ and $\mathbb{Z} = \{x \in \mathbb{Q} : |x|_p \le 1\}$. □

Theorem 11.7 (Weak approximation)**.** *Let S be a finite set of primes $p \le \infty$, and for each $p \in S$ let $x_p \in \mathbb{Q}_p$ be given. Then for every $\epsilon > 0$ there exists $x \in \mathbb{Q}$ such that*

$$|x - x_p|_p < \epsilon$$

for all $p \in S$. Equivalently, the image of $\mathbb{Q}$ in $\prod_{p\in S} \mathbb{Q}_p$ dense under the product topology.

Proof. If S has cardinality 1 we can apply Theorem 11.6, so we assume S contains at least 2 primes. For any particular prime $p \in S$, we claim that there is a $y_p \in \mathbb{Q}$ such that $|y_p|_p > 1$ and $|y_p|_q < 1$ for $q \in S - \{p\}$. Indeed, let P be the product of the finite primes in S, and for each $p < \infty$ choose $r \in \mathbb{Z}_{>0}$ so that $p^{-r}P < 1$. Then define

$$y_p = \begin{cases} P & \text{if } p = \infty, \\ p^{-r}P & \text{otherwise.} \end{cases}$$

We now note that for any $q \in S$,

$$\lim_{n\to\infty} |y_p|_q = \begin{cases} \infty & \text{if } q = p, \\ 0 & \text{if } q \ne p. \end{cases}$$

It follows that for each $q \in S$

$$\lim_{n\to\infty} \frac{y_p^n}{1+y_p^n} = \begin{cases} 1 \text{ with respect to } |\ |_q \text{ for } q = p, \\ 0 \text{ with respect to } |\ |_q \text{ for } q \ne p, \end{cases}$$

since $\lim_{n\to\infty} |1 - y_p^n/(1+y_p^n)|_p = \lim_{n\to\infty} |1/(1+y_p^n)|_p = 0$ and $\lim_{n\to\infty} |y_p^n/(1+y_p^n)|_q = 0$ for $q \ne p$. For each $n \in \mathbb{Z}_{>0}$ define

$$z_n = \sum_{p\in S} \frac{x_p y_p^n}{1+y_p^n}.$$

Then $\lim_{n\to\infty} z_n = x_p$ with respect to $|\ |_p$ for each $p \in S$. So for any $\epsilon > 0$ there is an n for which $x = z_n$ satisfies $|x - x_p|_p < \epsilon$ for all $p \in S$. □

Theorem 11.8 (Strong approximation)**.** *Let S be a finite set of primes $p < \infty$, and for each $p \in S$ let $x_p \in \mathbb{Z}_p$ be given. Then for every $\epsilon > 0$ there exists $x \in \mathbb{Z}$ such that*

$$|x - x_p|_p < \epsilon$$

for all $p \in S$. Equivalently, the image of $\mathbb{Z}$ in $\prod_{p\in S} \mathbb{Z}_p$ is dense under the product topology.

Proof. Fix $\epsilon > 0$. By Theorem 11.6, for each x_p we can pick $y_p \in \mathbb{Z}_{\geq 0}$ so that $|y_p - x_p|_p < \epsilon$. Let n be a positive integer such that $p^n > y_p$ for all $p \in S$. By the Chinese remainder theorem, there exists $x \in \mathbb{Z}$ such that $x \equiv y_p \bmod p^n$ for all $p \in S$, and for this x we have $|x - x_p|_p < \epsilon$ for all $p \in S$. □

Remark 11.9. In more general settings it is natural to consider the infinite product of *all* the rings of p-adic integers

$$\hat{\mathbb{Z}} = \prod_{p<\infty} \mathbb{Z}_p.$$

Recall that for infinite products, the product topology is defined using a basis of open sets that consists of sequences (U_p), where each U_p is an open subset of $\mathbb{Z}_p$, and for all but finitely many p we have $U_p = \mathbb{Z}_p$. It follows from Theorem 11.8 that the image of $\mathbb{Z}$ in $\hat{\mathbb{Z}}$ is dense.

There is another way to define $\hat{\mathbb{Z}}$, which is to consider the inverse system of rings $(\mathbb{Z}/n\mathbb{Z})$, where n ranges over all positive integers n and we have reduction maps from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ whenever $n|m$ (note that we now have an infinite acyclic graph of maps, not just a linear chain). The inverse limit

$$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$$

is called the *profinite completion* of $\mathbb{Z}$. One can show that these two definitions of $\hat{\mathbb{Z}}$ are canonically isomorphic. So a more pithy statement of Theorem 11.8 is that $\mathbb{Z}$ is dense in its profinite completion (this statement applies to profinite completions in general).

Remark 11.10. Note the difference between weak and strong approximation. With weak approximation we obtain a rational number x that is p-adically close to x_p for each p in a finite set S, but we have no control on $|x|_p$ for $p \notin S$. With strong approximation we obtain a rational number (in fact an integer) x that is p-adically close to x_p for each $p \in S$ and also satisfies $|x|_p \leq 1$ for all $p \notin S$, *except* the prime $p = \infty$; in order to apply the CRT we may need to make $|x|_\infty$ very large. More generally, we could allow $\infty \in S$ if we grant ourselves the freedom to make $|x|_{p_0}$ large for one prime $p_0 \notin S$; in this case x would be a rational number, not an integer, but its denominator would be divisible by no primes other than p_0, so that $x \in \mathbb{Z}_p$ for all $p \neq p_0$. This is characteristic of strong approximation theorems, we obtain an element whose absolute value is bounded at all but one prime.

The following lemma follows from the strong approximation theorem and Dirichlet's theorem on primes in arithmetic progressions: for any relative prime integers a and b there are infinitely many primes congruent to a mod b.

Lemma 11.11. *Let S be a finite set of primes $p \leq \infty$, and for each $p \in S$ let $x_p \in \mathbb{Q}_p^\times$ be given. Then there exists an $x \in \mathbb{Q}$ such that*

(i) *$x \in x_p \mathbb{Q}_p^{\times 2}$ for each $p \in S$.*

(ii) *$|x|_p = 1$ for all but at most one finite prime $p_0 \notin S$.*

Proof. Let $S_0 = S - \{\infty\}$, and define the rational number

$$y = \pm \prod_{p \in S_0} p^{v_p(x_p)},$$

where the sign of y is negative if $\infty \in S$ and $x_\infty < 0$, and positive otherwise. Then $|y|_p = |x_p|_p$ for all $p \in S_0$, and it follows that for each $p \in S_0$ we have $y = u_p x_p$ for some $u_p \in \mathbb{Z}_p^\times$. By the strong approximation theorem there exists an integer $z \equiv u_p \bmod p^{e_p}$, for all $p \in S_0$, where $e_p = 1$ for odd p and $e_p = 3$ for $p = 2$. It follows that $z \in u_p \mathbb{Q}_p^{\times 2}$ for all $p \in S_0$, since the square class of u_p depends only on its reduction mod p^{e_p}.

The integers z and $m = \prod_{p \in S_0} p^{e_p}$ are relatively prime, so it follows from Dirichlet's theorem that there are infinitely many primes congruent to $z \bmod m$. Let p_0 be the least such prime. Then $p_0 \in z\mathbb{Q}_p^{\times 2}$ for all $p \in S_0$, and $x = p_0 y$ satisfies both (i) and (ii). □

11.3 Proof of the Hasse-Minkowski theorem

Before proving the Hasse-Minkowski theorem for $\mathbb{Q}$ we make one final remark. The definition of the Hilbert symbol we gave in the last lecture makes sense over any field, in particular $\mathbb{Q}$, and the proofs of Lemma 10.2 and Corollary 10.3 still apply. In the proof below we use (a, b) to denote the Hilbert symbol of $a, b \in \mathbb{Q}^\times$.

Theorem 11.12 (Hasse-Minkowski)**.** *A quadratic form over $\mathbb{Q}$ represents 0 if and only if it represents 0 over every completion of $\mathbb{Q}$.*

Proof. The forward implication is clear, we only need to prove the reverse implication. So let f be a quadratic form over $\mathbb{Q}$ that represents 0 over every completion of $\mathbb{Q}$. We may assume without loss of generality that f is a diagonal form $a_1 x_1^2 + \cdots + a_n x_n^2$, which we may denote $\langle a_1, \ldots, a_n \rangle$. We write $\langle a_1, \ldots, a_n \rangle_p$ to denote the same form over $\mathbb{Q}_p$. If any $a_i = 0$, then f clearly represents 0 over $\mathbb{Q}$ (set $x_i = 1$ and $x_j = 0$ for $i \neq j$), so we assume f is nondegenerate and proceed by induction on its dimension n.

Case $n = 1$: The theorem holds trivially (f cannot represent 0 over any $\mathbb{Q}_p$).

Case $n = 2$: The form $\langle a, b \rangle_p$ represents 0 if and only if $-ab$ is square in $\mathbb{Q}_p$. Thus $v_p(-ab) \equiv 0 \bmod 2$ for all $p < \infty$ and $-ab > 0$. It follows that $-ab$ is square in $\mathbb{Q}$, and therefore $\langle a, b \rangle$ represents 0.

Case $n = 3$: Let $f(x, y, z) = z^2 - ax^2 - by^2$, where a and b are nonzero square-free integers with $|a| \leq |b|$. We know $(a, b)_p = 1$ for all $p \leq \infty$ and wish to show $(a, b) = 1$. We proceed by induction on $m = |a| + |b|$. The base case $m = 2$ has $a = \pm 1$ and $b = \pm 1$, in which case $(a, b)_\infty = 1$ implies that either a or b is 1 and therefore $(a, b) = 1$.

We now suppose $m \geq 3$, and that the result has been proven for all smaller m. For each prime $p|b$ there is a primitive solution $(x_0, y_0, z_0) \in \mathbb{Z}_p^3$ to $z^2 - ax^2 - by^2 = 0$. We must have $p|(z_0^2 - ax_0^2)$, since $p|b$, but we cannot have $p|x_0$ since then we would have $p|z_0$, contradicting primitivity. So $x_0 \in \mathbb{Z}_p^\times$ and $a = (z_0/x_0)^2$ is a square modulo p. This holds for every prime $p|b$, and b is square-free, so a is a square modulo b.

It follows that $a + bb' = t^2$ for some $t, b' \in \mathbb{Z}$ with $t \leq |b/2|$. This implies $(a, bb') = 1$, since $bb' = t^2 - a$ is the norm of $t + \sqrt{a}$ in $\mathbb{Q}(\sqrt{a})$. Therefore

$$(a, b) = (a, b)(a, bb') = (a, b^2 b') = (a, b').$$

We also have $(a, bb')_p = 1$, and therefore $(a, b')_p = (a, b)_p = 1$, for all $p \leq \infty$. But

$$|b'| = \left| \frac{t^2 - a}{b} \right| \leq \left| \frac{t^2}{b} \right| + \left| \frac{a}{b} \right| \leq \frac{|b|}{4} + 1 < |b|,$$

so $|a|+|b'| < m$ and the inductive hypothesis implies $(a, b') = 1$. Thus $(a, b) = 1$, as desired.

Case $n = 4$: Let $f = \langle a_1, a_2, a_3, a_4\rangle$ and let S consist of the primes $p|2a_1a_2a_3a_4$ and ∞. Then $a_i \in \mathbb{Z}_p^\times$ for all $p \notin S$. For each $p \in S$ there exists $t_p \in \mathbb{Q}_p^\times$ such that $\langle a_1, a_2\rangle_p$ represents t_p and $\langle a_3, a_4\rangle_p$ represents $-t_p$ (we can assume $t_p \neq 0$: if 0 is represented, by both forms, so is every element of $\mathbb{Q}_p$). By Lemma 11.11, there is a rational number t and a prime $p_0 \notin S$ such that $t \in t_p\mathbb{Q}_p^{\times 2}$ for all $p \in S$ and $|t|_p = 1$ for all $p \notin S \cup \{p_0\}$.

The forms $\langle a_1, a_2, -t\rangle_p$ and $\langle a_3, a_4, t\rangle_p$ represent 0 for all $p \notin S\cup\{p_0\}$ because all such p are odd, and $a_i, \pm t \in \mathbb{Z}_p^\times$, so $(a_1, a_2)_p = 1 = (t, -a_1a_2)_p$ and $(a_3, a_4)_p = 1 = (-t, -a_3a_4)_p$, and we may apply Corollary 11.4. Since $t \in t_p\mathbb{Q}_p^{\times 2}$ for all $p \in S$, the forms $\langle a_1, a_2, -t\rangle_p$ and $\langle a_3, a_4, t\rangle_p$ also represent 0 for all $p \in S$. Thus $\langle a_1, a_2, -t\rangle_p$ and $\langle a_3, a_4, t\rangle_p$ represent 0 for all $p \neq p_0$, and by Corollary 11.5, also for $p = p_0$. By the inductive hypothesis $\langle a_1, a_2, -t\rangle$ and $\langle a_3, a_4, t\rangle$ both represent 0, therefore $\langle a_1, a_2, a_3, a_4\rangle$ represents 0.

Case $n \geq 5$: Let $f = \langle a_1, \dots, a_n\rangle$. Let S be the set of primes for which $\langle a_3, \dots, a_n\rangle_p$ does not represent 0. The set S is finite, by Corollary 11.2. If S is empty then $\langle a_3, \dots, a_n\rangle$, and therefore f, represents 0, by the inductive hypothesis, so we assume S is not empty. For each $p \in S$ pick $t_p \in \mathbb{Q}_p^\times$ represented by $\langle a_1, a_2\rangle$, say $a_1x_p^2 + a_2y_p^2 = t_p$, such that $\langle a_3, \dots, a_n\rangle_p$ represents $-t_p$ (such a t_p exists since f represents 0 over $\mathbb{Q}_p$ and, as above, we can always pick $t_p \neq 0$).

By the weak approximation theorem there exists $x, y \in \mathbb{Q}$ that are simultaneously close enough to all the $x_p, y_p \in \mathbb{Q}_p$ so that $t = a_1x^2 + a_2y^2$ is close enough to all the t_p to guarantee that $t \in t_p\mathbb{Q}_p^{\times 2}$ for all $p \in S$ (for $p < \infty$ the square class only depends on at most the first three nonzero p-adic digits, and over $\mathbb{R} = \mathbb{Q}_\infty$ we can ensure that x and y have the same signs as x_∞ and y_∞).[1] It follows that $\langle t, a_3, \dots, a_n\rangle_p$ represents 0 for all $p \in S$, and since $\langle a_3, \dots, a_n\rangle_p$ represents 0 for all $p \notin S$, so does $\langle t, a_3, \dots, a_n\rangle_p$. Thus $\langle t, a_3, \dots, a_n\rangle_p$ represents 0 for all p, and by the inductive hypothesis, $\langle t, a_3, \dots, a_n\rangle$ represents 0. Therefore $\langle a_3, \dots, a_n\rangle$ represents $-t = -a_1x^2 - a_2y^2$, hence $\langle a_1, \dots, a_n\rangle$ represents 0. □

[1] Equivalently, the set of squares $\mathbb{Q}_p^{\times 2}$ is an open subset of $\mathbb{Q}_p^\times$, hence so is every square class $t_p\mathbb{Q}_p^{\times 2}$.

18.782 Introduction to Arithmetic Geometry
Fall 2013