The Minkowski – Hasse Theorem (local-to-global principle)

See: J.-P. Serre, Cours d'arithmétique
J.W.S. Cassels, Local Fields
—— " ——, Rational Quadratic Forms

$\mathcal{P} = \{\text{primes } p\}$, $\mathbb{Q}_\infty = \mathbb{R}$

f, g non-degenerate quadratic forms over $\mathbb{Q}$, $\dim(f) = \dim(g) = n$

Theorem (Minkowski–Hasse)

(1) (Strong form) f is isotropic over $\mathbb{Q} \iff \forall r \in \mathcal{P} \cup \{\infty\}$ f is isotropic over $\mathbb{Q}_r$.
$f = 0$ has a solution in $\mathbb{Q}^n \setminus \{0\}$

(2) (Weak form) $f \sim g$ over $\mathbb{Q} \iff \forall r \in \mathcal{P} \cup \{\infty\}$ $f \sim g$ over $\mathbb{Q}_r$.

If $n \le 3$, one can replace in both (1) and (2) the set $\mathcal{P} \cup \{\infty\}$ by $(\mathcal{P} \cup \{\infty\}) \setminus \{r_0\}$, for any $r_0 \in \mathcal{P} \cup \{\infty\}$.

Cor. The equivalence class of $f \sim \langle a_1, \dots, a_n \rangle$ over $\mathbb{Q}$ is determined by the following invariants: $n = \dim(f)$, $d(f) = \overline{a_1 \cdots a_n} \in \mathbb{Q}^*/\mathbb{Q}^{*2}$, $\forall r \in \mathcal{P} \cup \{\infty\}$ $c_r(f) = \prod_{i<j} (a_i, a_j)_r \in \{\pm 1\}$, and the signature at ∞
They satisfy: • $c_r(f) = 1$ for $r \notin$ finite set
• $\prod_r c_r(f) = 1$
• $\forall r$ $\exists$ g_r over $\mathbb{Q}_r$ such that $\dim(g_r) = n$, $d(g_r) = d(f) \mathbb{Q}_r^{*2} \in \mathbb{Q}_r^*/\mathbb{Q}_r^{*2}$, $c(g_r) = c_r(f)$

Pf of [(1) $\Rightarrow$ (2)]: Assume $f \sim g$ over $\mathbb{Q}_r$ $\forall r \in \mathcal{P} \cup \{\infty\}$ ($r \ne r_0$ if $n \le 3$). Consider $h = \langle f \rangle \perp \langle -g \rangle$, $\dim(h) = 2n$. $\forall r$ ($\ne r_0$) h is isotropic over $\mathbb{Q}_r \overset{(1)}{\Rightarrow}$ also over $\mathbb{Q}$
$\Rightarrow$ $\exists a \in \mathbb{Q}$ represented by both f and g; if $a = 0 \Rightarrow$ f, g represent all elements of $\mathbb{Q}$, so we can take $a \in \mathbb{Q}^*$. Then $f \sim \langle a \rangle \perp f'$, $g \sim \langle a \rangle \perp g'$. Witt's thm $\Rightarrow$ $f' \sim g'$ over $\mathbb{Q}_r$ for all r ($\ne r_0$). Induction: $f' \sim g'$ over $\mathbb{Q} \Rightarrow f \sim g$ over $\mathbb{Q}$.
[If $n \le 3$, $d(f)\mathbb{Q}_r^{*2} = d(g)\mathbb{Q}_r^{*2} \in \mathbb{Q}_r^*/\mathbb{Q}_r^{*2}$ $\forall r \ne r_0 \Rightarrow d(f) = d(g) \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ (see $n=2$ below)
$c_r(f) = c_r(g)$ $\forall r \ne r_0 \Rightarrow c_{r_0}(f) = \prod_{r \ne r_0} c_r(f) = \prod_{r \ne r_0} c_r(g) = c_{r_0}(g)$
$\Rightarrow$ $f \sim g$ over $\mathbb{Q}_{r_0}$, even if $r_0 = \infty$]

Pf of (1). $n = 2$: $f \sim \langle a_1, a_2 \rangle$ is isotropic over $K \supset \mathbb{Q} \iff \underbrace{-a_1 a_2}_{b \in \mathbb{Q}^*} \in K^{*2}$.
If $\forall p \in \mathcal{P} \setminus \{p_0\}$ $b \in \mathbb{Q}_p^{*2} \Rightarrow \forall p \ne p_0$ $2 \mid v_p(b) \Rightarrow \exists b' \in \mathbb{Q}^*$ $b/b'^2 \in \{\pm 1, \pm p_0\}$; but $-1 \notin \mathbb{Q}_3^{*2}, \mathbb{Q}_7^{*2}$.
Fix $\varepsilon = \pm 1$; the Jacobi symbol $\left(\frac{\varepsilon p_0}{a}\right) = (-1)^{\frac{a-1}{2}\frac{\varepsilon-1}{2}} \left(\frac{a}{p_0}\right)$ can be made $= -1$ for some $a > 1$, $\gcd(a, 2p_0) = 1$; then $\exists$ prime $q \mid a$ such that $\left(\frac{\varepsilon p_0}{q}\right) = -1 \Rightarrow \varepsilon p_0 \notin \mathbb{Q}_q^{*2}$. Therefore $b = b'^2 \in \mathbb{Q}^{*2}$.

Rmk: In fact, $b \in \mathbb{Q}^*$ satisfies $b \in \mathbb{Q}^{*2} \iff b \in \mathbb{Q}_p^{*2}$ for "many" (more than 50%) $p \in \mathcal{P}$.

$n=3$: a non-zero multiple of f is equivalent to $\langle a_1,a_2,a_3\rangle$, $a_i\in\mathbb{Z}\setminus\{0\}$, $a_1a_2a_3$ squarefree.

f is isotropic over $\mathbb{Q}_v \iff \left(-\frac{a_1}{a_3},-\frac{a_2}{a_3}\right)_v = 1$. As $\prod_v (a,b)_v = 1$,

—"— $\forall v\neq v_0 \Rightarrow$ also for $v=v_0$. So we can assume that

—"— $\forall v\in P \Longrightarrow$ f is isotropic over $\mathbb{Q}$.

Legendre's thm (in our version)

$n=4$: The argument for $n=4$ will use Dirichlet's thm on primes in arithmetic progressions. There is another proof, which avoids Dirichlet's thm: one first proves the weak version (2) by a direct algebraic argument (showing that the map of Witt rings $W(\mathbb{Q}) \longrightarrow \prod_v W(\mathbb{Q}_v)$ is injective). If f is isotropic over each $\mathbb{Q}_v$, then $f \sim \langle 1,-1\rangle \perp g_v$ for some g_v over $\mathbb{Q}_v$, $\dim(g_v)=2$.
Gauss's theory of genera $\Rightarrow \exists$ g over $\mathbb{Q}$ with $d(g)=-d(f)$ and $c_v(g)=c(g_v)$
$\forall v \Rightarrow g\sim g_v$ over $\mathbb{Q}_v$ $\forall v \Rightarrow h = f\perp(-g) \sim 3\langle 1,-1\rangle$ over all $\mathbb{Q}_v \overset{(2)}{\Rightarrow}$ over $\mathbb{Q}$
$\Rightarrow$ f isotropic.

Pf: We can again assume $f=\langle a_1,a_2,a_3,a_4\rangle$, $a_i\in\mathbb{Z}\setminus\{0\}$ squarefree; let $P_0=\{p\in P \mid p\mid 2\prod a_i\}$
f isotropic over all $\mathbb{Q}_v$ $\qquad v=\infty$: can assume $a_1>0>a_4$
Let $g=\langle a_1,a_2\rangle$, $h=\langle -a_3,-a_4\rangle$.
$\forall p\in P_0$ $\exists b_p\in\mathbb{Q}_p$ represented by both g and h (over $\mathbb{Q}_p$); again, we can assume $b_p\in\mathbb{Q}_p^*$, even $b_p\in\mathbb{Z}_p\setminus\{0\}$. Let $\lambda_p=\begin{cases}3 & p=2\\ 1 & p\neq 2\end{cases}$, $\mu_p=v_p(b_p)\geq 0$, $m=\prod_{p\in P_0} p^{\lambda_p+\mu_p}$

Fix $c\in\mathbb{Z}_{>0}$ such that $\forall p\in P_0 \quad c\equiv b_p \pmod{p^{\lambda_p+\mu_p}}$. $\qquad (*)$

Then: $\forall p\in P_0$ $c/b_p \in 1+p^{\lambda_p}\mathbb{Z}_p \subset \mathbb{Z}_p^{*2} \Rightarrow$ c is represented by both g,h over $\mathbb{Q}_p$
We want c divisible only by primes in $P_0\cup\{\text{one more prime}\}$: let $d=\gcd(c,m)$,
then $\gcd\left(\frac{c}{d},\frac{m}{d}\right)=1 \overset{\text{Dirichlet's thm}}{\Longrightarrow} \exists$ prime $q\equiv\frac{c}{d}\pmod{\frac{m}{d}} \Rightarrow c'=dq\equiv c \pmod m$,
this new value $c'\in\mathbb{Z}_{>0}$ is represented by g,h over $\mathbb{R}$ ($c'>0$), over $\mathbb{Q}_p$ for all $p\in P_0$ (c' satisfies $(*)$) and over all $\mathbb{Q}_{p'}$ for $p'\notin P_0\cup\{2\}$ ($v_{p'}(a_i)=0\ \forall i$ $\Rightarrow v_{p'}(c')=0$, $p'\neq 2$).
The case $n=3$ for $g\perp\langle -c'\rangle$, $h\perp\langle -c'\rangle$ and $v_0=2$ tells us that c' is represented by g and h over $\mathbb{Q} \Rightarrow f=g\perp(-h)$ is isotropic over $\mathbb{Q}$.

$n \geq 5$: Again, $f = \langle a_1, \dots, a_n \rangle$, $a_i \in \mathbb{Z} \setminus \{0\}$ square-free, $P_0 = \{p \in P \mid p \mid 2\prod a_i\}$

f isotropic over all $\mathbb{Q}_v \Rightarrow$ can assume $a_1 > 0 > a_3$

Let $g = \langle a_1, a_2 \rangle$, $h = \langle -a_3, \dots, -a_n \rangle$. Again, $f = g \perp (-h)$ and
$\forall\, p \in P_0 \;\; \exists\, c_p \in \mathbb{Z}_p \setminus \{0\}$ represented by both g and h over $\mathbb{Q}_p$.
We can assume that $\forall p \in P_0 \;\; \exists\, b_{1,p}, b_{2,p} \in \mathbb{Z}_p \quad c_p = a_1 b_{1,p}^2 + a_2 b_{2,p}^2$
(after multiplying c_p by some power of p^2).

There exist $b_1, b_2 \in \mathbb{Z}$ such that

$\forall i = 1,2 \;\; \forall p \in P_0 \quad b_i \equiv b_{i,p} \pmod{p^{\blacktriangle b_{i,p}}}$ if $b_{i,p} \neq 0$

$b_i \equiv 0 \pmod{p^2 b_{3-i,p}}$ if $b_{i,p} = 0$

If $b_1 \gg 0$, then $c = a_1 b_1^2 + a_2 b_2^2 \in \mathbb{Z}$ and $c > 0$.

By construction,

$\forall p \in P_0 \quad c_p / c \in 1 + p^{\lambda_p} \mathbb{Z}_p \subset \mathbb{Z}_p^{*2} \quad \left(\lambda_p = \begin{cases} 1 & p \neq 2 \\ 3 & p = 2 \end{cases}\right)$

$\Rightarrow \forall v \in P_0 \cup \{\infty\}$ c is represented by h over $\mathbb{Q}_v$

$\Rightarrow$ —— " —— $f' = \langle a_3, \dots, a_n \rangle \perp \langle c \rangle$ is isotropic over $\mathbb{Q}_v$.

$\forall\, q \notin P_0 \cup \{\infty\} \quad q \neq 2$, $a_3, a_4, a_5 \in \mathbb{Z}_q^* \Rightarrow \langle a_3, a_4, a_5 \rangle$ isotropic over $\mathbb{Q}_q$.

So f' is isotropic over all $\mathbb{Q}_v \Longrightarrow$ the case $\dim = n-1$ implies that
$\dim(f') = n-1$ f' is isotropic over $\mathbb{Q}$.

therefore c is represented by h over $\mathbb{Q}$
c —— " —— g —" —
$\Big\} \Rightarrow f$ is isotropic over $\mathbb{Q}$.

Note : the induction $\dim = 4 \Rightarrow \dim \geq 5$ does not use

Dirichlet's thm on primes.

An alternative approach if $\dim = 4$:

Exercise. A non-degenerate f of $\dim(f) = 4$ over a field K such that $d(f) = \overline{1} \in K^*/K^{*2}$ is equivalent to $\langle 1, -a, -b, ab \rangle$. It is isotropic $\Longleftrightarrow \langle a, b, -1 \rangle$ is.

Exercise. A non-degenerate f of $\dim(f) = 4$ over a field K such that $d(f) \neq \overline{1} \in K^*/K^{*2}$ is isotropic over $K \Longleftrightarrow$ it is $\overset{\text{isotropic}}{\text{over}}$ $K(\sqrt{d(f)}) = L$
$(d(f) = \overline{1} \in L^*/L^{*2}$, then).

This reduces the Minkowski–Hasse thm over $\mathbb{Q}$ for $\dim = 4$ to the same result over the quadratic field $\mathbb{Q}(\sqrt{d(f)})$ and $\dim = 3$.

Cor. f represents $a \in \mathbb{Q}^* \iff \forall v \in P \cup \{\infty\}$ f represents a over $\mathbb{Q}_v$. Pf: take $f \perp \langle -a \rangle$.

Cor (Meyer) A non-degenerate quadratic form f over $\mathbb{Q}$ in $\dim(f) = n \geq 5$ variables is isotropic $\iff$ it is indefinite.

Pf. $n \geq 5 \Rightarrow$ f is isotropic over all $\mathbb{Q}_p$.

Cor. Let $n \in \mathbb{Z}_{>0}$.

$\exists\, x_1, x_2, x_3 \in \mathbb{Q}$ $x_1^2 + x_2^2 + x_3^2 = n \iff \forall v$ $\langle 1, 1, 1, -n \rangle$ is isotropic over $\mathbb{Q}_v$

$\Updownarrow$

$n \neq 4^a(8k+7)$

Forms of higher degree

(1) $3x^3 + 4y^3 + 5z^3 = 0$ has a solution in $\mathbb{Q}_v^3 \setminus \{0\}$ $\forall v \in P \cup \{\infty\}$, but no solution in $\mathbb{Q}^3 \setminus \{0\}$. (Selmer)

(2) $\forall d \geq 2$ $\exists$ finite set of bad primes $A(d)$ such that $\forall p \notin A(d)$ every form of degree d (= homogeneous polynomial) $\in \mathbb{Q}_p[X_1, \dots, X_{d^2+1}]$ has a (non-trivial) zero in $\mathbb{Q}_p^{d^2+1} \setminus \{0\}$. (Ax–Kochen)

(3) $A(2) = \emptyset$ (see above); $A(3) = \emptyset$ (Demyanov, Lewis)

(4) If $f \in \mathbb{Q}[X_1, \dots, X_{10}]$ is a cubic form ($\deg = 3$) such that the projective cubic hypersurface $\{f = 0\} \subset \mathbb{P}^9$ is non-singular, then $f = 0$ has a solution in $\mathbb{Q}^{10} \setminus \{0\}$; in the singular case 10 needs to be replaced by 14 (at present...) (Heath-Brown)

(5) If $f \in \mathbb{Q}[X_1, \dots, X_{41}]$ is homogeneous of $\deg(f) = 4$ and $\{f = 0\} \subset \mathbb{P}^{40}$ is non-singular, then:

$f = 0$ has a solution in $\mathbb{Q}^{41} \setminus \{0\} \iff f = 0$ has a solution in all $\mathbb{Q}_v^{41} \setminus \{0\}$ ($v \in P \cup \{\infty\}$)

(Browning – Heath-Brown)

Aubry's method – from solutions in $\mathbb{Q}^n$ to solutions in $\mathbb{Z}^n$

Thm: let $f(X) = \sum_{i,j=1}^{n} a_{ij} X_i X_j$, $a_{ij} = a_{ji} \in \frac{1}{2}\mathbb{Z}$, $a_{ii} \in \mathbb{Z}$. Assume that

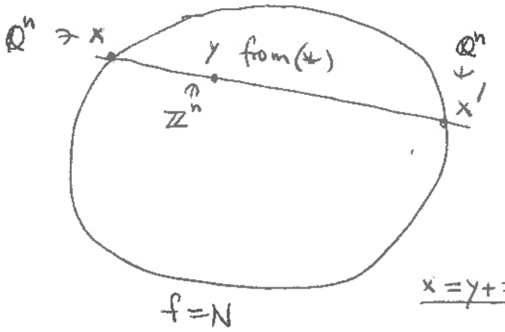
$(*)$ $\forall x \in \mathbb{R}^n \setminus \mathbb{Z}^n \quad \exists y \in \mathbb{Z}^n \quad 0 < |f(x-y)| < 1$.

Then $f(\mathbb{Q}^n) \cap \mathbb{Z} = f(\mathbb{Z}^n) \cap \mathbb{Z}$.

Ex: $f = X_1^2 + X_2^2$, $X_1^2 \pm 2X_2^2$, $X_1^2 + X_2^2 + X_3^2$, $X_1^2 + X_2^2 - 3X_3^2$, $X_1^2 - 3X_2^2$

Pf: Assume that $x \in \mathbb{Q}^n \setminus \mathbb{Z}^n$, $f(x) = N \in \mathbb{Z}$. We construct $x' \in \mathbb{Q}^n$ with $f(x') = f(x) = N$ and a smaller denominator than x as follows:

$\{x, x'\} = (\text{the line through } x \text{ and } y \text{ from } (*)) \cap \left(\begin{matrix}\text{the quadric} \\ f = N\end{matrix}\right)$



comparing the denominators:

$mx \in \mathbb{Z}^n$, $m > 1$ minimal, $f(y), f(x) \in \mathbb{Z}$, $y \in \mathbb{Z}^n$

$B : \mathbb{Z}^n \times \mathbb{Z}^n \longrightarrow \frac{1}{2}\mathbb{Z}$, $B(X, Y) = \sum_{i,j=1}^{n} a_{ij} X_i Y_j$ bilinear symmetric

$B(X, X) = f(X)$

$x = y + z$, $x' = x + tz$ $(t \neq 0)$, $\underset{f(x)}{f(x')} = f(x) + 2t\,B(x, z) + t^2 f(z)$

$\Rightarrow 2B(x, z) = -t f(z) = 2B(x, x-y) = 2f(x) - 2B(x, y) \in 2\mathbb{Z} + \frac{1}{m}\mathbb{Z} = \frac{1}{m}\mathbb{Z}$

$m' := m\,f(z) = m\,f(x-y) = m f(x) + m f(y) - 2B(mx, y) \in \mathbb{Z}$, $0 < |m'| < |m|$, by $(*)$

$m't = -2m\,B(x, z) \in \mathbb{Z} \implies m'ty \in \mathbb{Z}^n$, $x' = x + t(x-y) = (1+t)x - ty$

$1 + t = \dfrac{f(z) - 2B(x,z)}{f(z)} = \dfrac{f(x) + f(y) - 2B(x,y) + 2B(x, y-x)}{f(z)} = \dfrac{f(y) - f(x)}{f(z)}$,

$m'(1+t)x = (f(y) - f(x))\,mx \in \mathbb{Z}^n$

$\Longrightarrow$ $f(x') = N$, $m'x' \in \mathbb{Z}^n$

If $x' \notin \mathbb{Z}^n$, repeat this procedure until $m' = 1$.

Variant: for $f = X_1^2 + 3X_2^2$, $X_1^2 + X_2^2 + 2X_3^2$, $X_1^2 + X_2^2 + X_3^2 + X_4^2$ we only have

$(*')$ $\forall x \in \mathbb{R}^n \setminus \mathbb{Z}^n \quad \exists y \in \mathbb{Z}^n \quad 0 < |f(x-y)| \leq 1$. (taking y such that $\forall i$: $|x_i - y_i| \leq \frac{1}{2}$)

thm still holds for these forms: equality in $(*')$ only occurs if

$z = x - y = (\pm\frac{1}{2}, \dots, \pm\frac{1}{2})$; then $|m'| = m$, $f(z) = 1$, $t = -2B(x,z) \in \mathbb{Z} - f(z) = \mathbb{Z}$,

$m = 2$ (since $x \in \mathbb{Z}^n + (\frac{1}{2}, \dots, \frac{1}{2})$). Inspection shows that, given $x \in \mathbb{Z}^n + (\frac{1}{2}, \dots, \frac{1}{2})$ with $f(x) \in \mathbb{Z}$, one can always choose a combination of signs $z = (\pm\frac{1}{2}, \dots, \pm\frac{1}{2})$ so that $-t \in 2B(x, z) \in 1 + 2\mathbb{Z}$; then $x' \in \mathbb{Z}^n$.

Cor: $\mathbb{Z} \cap \{x_1^2 + x_2^2 + x_3^2 \mid x_i \in \mathbb{Z}\} = \underbrace{\mathbb{Z} \cap \{x_1^2 + x_2^2 + x_3^2 \mid x_i \in \mathbb{Q}\}}_{\{n \geq 0 \mid n \neq 4^a(8k+7)\}}$
(Gauss)

Cor (Lagrange) Every $n \in \mathbb{Z}_{\geq 0}$ is of the form $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ $(x_i \in \mathbb{Z})$

Pf: If $n \neq 4^a(8k+7)$ we can even take $x_4 = 0$. If $n = 4^a(8k+7)$, then

$n = (2^a)^2 + n'$, $n' \neq 4^{a'}(8k'+7) \Rightarrow n' = x_1^2 + x_2^2 + x_3^2$.

Failure of the Hasse principle for $2y^2 = x^4 - 17$

Thm (Lind 1940, Reichardt 1942). The curve $C: 2y^2 = x^4 - 17$ satisfies $C(\mathbb{Q}) = \emptyset$, $\forall v \in Pl(\mathbb{Q})$ $C(\mathbb{Q}_v) \neq \emptyset$.

Pfs of $C(\mathbb{Q}) = \emptyset$: (1) Elementary version: assume $(x,y) \in C(\mathbb{Q})$, [redacted]

If $v_p(x) < 0 \Rightarrow v_p(2y^2) = v_p(x^4) \Rightarrow p \neq 2 \wedge v_p(y) = 2v_p(x)$, hence $x = \frac{a}{c}$, $y = \frac{b}{c^2}$, $a, b, c \in \mathbb{N}_+$, $(a,c) = (b,c) = 1$, $2 \nmid c$, $\boxed{2b^2 = a^4 - 17c^4} \Rightarrow (a,b) = 1$, $2 \nmid ac$, $17 \nmid ab$

If $p \neq 2$ is a prime, $p \mid b \Rightarrow a^4 \equiv 17c^4 \pmod p \Rightarrow \left(\frac{17}{p}\right) = 1 \overset{QRL}{\Rightarrow} \left(\frac{p}{17}\right) = 1$.

As $\left(\frac{-1}{17}\right) = \left(\frac{2}{17}\right) = 1 \Rightarrow \left(\frac{b}{17}\right) = 1 \Rightarrow b \equiv z^2 \pmod{17} \Rightarrow 2z^4 \equiv a^4 \pmod{17}$.

But $2^{\frac{17-1}{4}} = 2^4 \not\equiv 1 \pmod{17} \Rightarrow 2 \not\equiv t^4 \pmod{17}$ — contradiction.

---

(2) More scientific version:

Prop. If $v \in Pl(\mathbb{Q})$ and $(x_v, y_v) \in C(\mathbb{Q}_v)$, $y_v \neq 0 \Rightarrow (y_v, 17)_v = \begin{cases} 1 & v \neq 17 \\ -1 & v = 17 \end{cases}$

($\Rightarrow$ if $(x,y) \in C(\mathbb{Q})$, then $y \neq 0$, $\prod_v (y, 17)_v = -1$, contradiction with QRL).

Pf of Prop: $v = \infty$ $(y_\infty, 17)_\infty = 1$; $v = p$ prime: $p = 2$ $17 \in \mathbb{Z}_2^{\times 2} \Rightarrow (y_2, 17)_2 = 1$

$p \neq 2, 17$: $(y_p, 17)_p = (p, 17)_p^{v_p(y_p)} = \left(\frac{17}{p}\right)^{v_p(y_p)}$

If $v_p(y_p) \leq 0 \overset{(1)}{\Rightarrow} 2 \mid v_p(y_p) \Rightarrow (y_p, 17)_p = 1$

If $v_p(y_p) > 0 \Rightarrow v_p(x_p) \geq 0$, $x_p^4 \equiv 17 \pmod p \Rightarrow \left(\frac{17}{p}\right) = 1 \Rightarrow (y_p, 17)_p = 1$

$p = 17$: $(1) \Rightarrow$ $v_{17}(y_{17}) = -2m$, $m \in \mathbb{N}$; $y_{17} = 17^{-2m} y'$, $y' \in \mathbb{Z}_{17}^\times$

$v_{17}(x_{17}) = -m$, $x_{17} = 17^{-m} x'$, $x' \in \mathbb{Z}_{17}^\times$

$2y'^2 = x'^4 - 17^{1+4m} \Rightarrow \left.\begin{array}{l} 2y'^2 \equiv x'^4 \pmod{17} \\ 2 \not\equiv t^4 \pmod{17} \end{array}\right\} \Rightarrow y' \not\equiv z^2 \pmod{17} \Rightarrow \left(\frac{y'}{17}\right) = -1$

But $(y_{17}, 17)_{17} = (y', 17)_{17} = \left(\frac{y'}{17}\right) = -1$.

What we see here is an example of the Brauer–Manin obstruction (to the existence of rational points) in action. In this particular instance it can also be interpreted in terms of the Cassels pairing on the Tate–Šafarevič group of the Jacobian curve of C. (the projectivisation of)

Pf of $\forall v \in P \cup \{\infty\}$ $C(\mathbb{Q}_v) \neq \emptyset$: $v = \infty$ OK; let $v = p$ prime

$p = 2$: $(3,0) \in C(\mathbb{Z}/2^5\mathbb{Z})$, $4 \cdot 3^3 \not\equiv 0 \pmod{2^3}$ $\overset{\text{Hensel}}{\Longrightarrow}$ $C(\mathbb{Z}_2) \neq \emptyset$

$p = 17$: $(6,6) \in C(\mathbb{F}_{17})$, $4 \cdot 6^3 \not\equiv 0 \pmod{17}$ $\overset{\text{Hensel}}{\Longrightarrow}$ $C(\mathbb{Z}_{17}) \neq \emptyset$

$p \neq 2, 17$: (1) enough to show $C(\mathbb{F}_p) \neq \emptyset$ ($\overset{\text{Hensel}}{\Longrightarrow} C(\mathbb{Z}_p) \neq \emptyset$), since every K-rational point $(x_0, y_0) \in C(K)$ over a field K of characteristic $\neq 2, 17$ is smooth ($4x_0^3 \neq 0 \in K$ or $4y_0 \neq 0 \in K$).

(2) If $\left(\frac{2}{p}\right) = 1$: $\left.\begin{matrix} 2 \equiv y_0^2 \pmod p \\ (3^4 - 17)/2 = 2 \cdot 4^2 \end{matrix}\right\} \Rightarrow (3, 4y_0) \in C(\mathbb{F}_p)$

(3) If $\left(\frac{3}{p}\right) = 0, 1$ and $\left(\frac{-1}{p}\right) = 1$: $\left.\begin{matrix} 3 \equiv x_0^2 \\ -1 = z_0^2 \end{matrix}\right\} \pmod p$, $\frac{3^2 - 17}{2} = (-1) \cdot 2^2 \Rightarrow (x_0, 2z_0) \in C(\mathbb{F}_p)$

(4) If $\left(\frac{-1}{p}\right) = -1$: we know that $\exists\, y_0, z_0 \in \mathbb{Z}$ $z_0^2 - 2y_0^2 \equiv 17 \pmod p$ $\Longrightarrow \mathbb{F}_p^{\times 2} = \mathbb{F}_p^{\times 4} \Rightarrow \exists\, x_0$ $z_0 \equiv x_0^2 \pmod p$ $\Rightarrow (x_0, y_0) \in C(\mathbb{F}_p)$

(5) If $\left(\frac{5}{p}\right) = 0, 1$: $\left.\begin{matrix} 5 \equiv x_0^2 \pmod p \\ (5^2 - 17)/2 = 2^2 \end{matrix}\right\} \Rightarrow (x_0, 2) \in C(\mathbb{F}_p)$

(6) If $\left(\frac{19}{p}\right) = 0, 1$: $\left.\begin{matrix} 19 \equiv y_0^2 \pmod p \\ (5^4 - 17)/2 = 19 \cdot 4^2 \end{matrix}\right\} \Rightarrow (5, 4y_0) \in C(\mathbb{F}_p)$

(7) Remaining case: $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{19}{p}\right) = -1$ $\Rightarrow \left(\frac{6}{p}\right) = \left(\frac{38}{p}\right) = 1$

$$\left.\begin{matrix} \left.\begin{matrix} 6 \equiv x_0^2 \\ 19 \equiv 2y_0^2 \end{matrix}\right\} \pmod p \\ \frac{6^2 - 17}{2} = 38\left(\frac{1}{2}\right)^2 \end{matrix}\right\} \Rightarrow (x_0, y_0) \in C(\mathbb{F}_p)$$

In fact, Step (4) was unnecessary.

Thm'. The curve $C'\colon y^2 = 2x^4 - 17$ also satisfies $C'(\mathbb{Q}) = \emptyset$, $\forall v \in P \cup \{\infty\}$ $C'(\mathbb{Q}_v) \neq \emptyset$.

Pf of $C'(\mathbb{Q}) = \emptyset$ $\Leftarrow$ Prop: $\forall v \in P \cup \{\infty\}$ $\left[(x_v, y_v) \in C'(\mathbb{Q}_v) \Rightarrow (y_v, 34)_v = \begin{cases} 1 & v \neq 17 \\ -1 & v = 17 \end{cases}\right]$.

Pf of Prop: $v \neq 2$ — as for the curve C

$v = 2$: $v_2(x_2), v_2(y_2) \geq 0 \Rightarrow y_2 \in \mathbb{Z}_2^\times$, $2x_2^4 \equiv 1 + 17 \equiv 2 \pmod{2^3} \Rightarrow x_2 \in \mathbb{Z}_2^\times$

$\Rightarrow y_2^2 \equiv \underbrace{2 \cdot 1 - 17}_{\equiv 1} \pmod{2^4} \Rightarrow y_2 \equiv \pm 1 \pmod{2^3} \Rightarrow (y_2, 34)_2 = \underbrace{(y_2, 17)_2}_{1\ (17 \in \mathbb{Z}_2^{\times 2})} (y_2, 2)_2 =$

$= (y_2, 2)_2 = 1$.

Pf of $C'(\mathbb{Q}_p) \neq \emptyset$: $(1,6) \in C'(\mathbb{F}_{17})$ is smooth $\Rightarrow C'(\mathbb{Z}_{17}) \neq \emptyset$

$(1,9) \in C'(\mathbb{Z}/2^5\mathbb{Z}) \overset{\text{Hensel}}{\Longrightarrow} C'(\mathbb{Z}_2) \neq \emptyset$.

$p \neq 2, 17$: $2(7/4)^4 - 17 = 2(15/16)^2 \Rightarrow C'(\mathbb{F}_p) \neq \emptyset$ if $\left(\frac{2}{p}\right) = 1$

$2(1/2)^4 - 17 = -5(3/2)^3 \Rightarrow C'(\mathbb{F}_p) \neq \emptyset$ if $\left(\frac{-5}{p}\right) = \left(\frac{6}{p}\right) = 1, 0$

$2 \cdot 3^2 - 17 = 1^2 \Rightarrow C'(\mathbb{F}_p) \neq \emptyset$ if $\left(\frac{3}{p}\right) = 1, 0$

$\left(\frac{-1}{p}\right) = -1 \Rightarrow C'(\mathbb{F}_p) \neq \emptyset$ (as for C)

Remaining case: $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{-5}{p}\right) = -\left(\frac{-1}{p}\right) = -1$ $\Rightarrow y_0^2 \equiv -15 \pmod p \Rightarrow (1, y_0) \in C'(\mathbb{F}_p)$.