Lemma: f is non-degenerate $\iff$ C_f is non-singular.

Recall: For $g(x,y) \in k[x,y]$, the affine curve $C_g \subset \mathbb{A}^2$ (here $C_g(K) = \{(a,b) \in K^2 \mid g(a,b) = 0\}$ (for any $K \supset k$), $\mathbb{A}^2(K) = K^2$)

is non-singular at $P = (a,b) \in C_g$ provided

$$\left(\frac{\partial g}{\partial x}(P) \quad \frac{\partial g}{\partial y}(P) \right) \neq (0 \quad 0)$$

(in this case, the tangent line to C_g at P is $\frac{\partial g}{\partial x}(P)(x-a) + \frac{\partial g}{\partial y}(P)(y-b) = 0$). (compare the situation in usual calculus)

these derivatives are formally defined for polynomials (over any ring) using the usual rules $\frac{d(x^n)}{dx} = n \cdot x^{n-1}$ etc.

C_g is nonsingular if it is nonsingular at every $P \in C_g$ [when I don't specify $C_g(K)$ for a particular field K, I mean $C_g = C_g(\bar{k})$].

Example:
Think about $g(x,y) = y^2 - x^3$ at

For a projective curve

C_f, $f \in k[X_0, X_1, X_2]$

$\hookrightarrow \mathbb{P}^2$

we say C_f is non-singular if

for each i, $\mathbb{P}^2 \supset \{X_i \neq 0\}$

$\cong \mathbb{A}^2$

via $(i=0)$

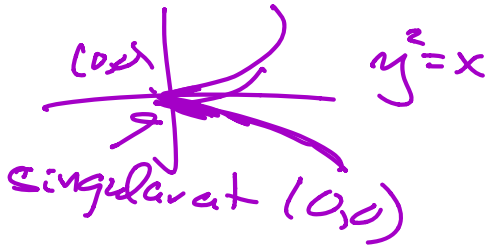
$\{X_0 \neq 0\} \xrightarrow{\sim} \mathbb{A}^2$

$[a_0, a_1, a_2] \longmapsto \left(\frac{a_1}{a_0}, \frac{a_2}{a_0}\right)$

$[1, a, b] \longleftarrow (a, b)$

$C_f \cap \{X_i \neq 0\} \subset \mathbb{A}^2$ is nonsingular (as an affine curve).

the point $(0,0)$ compared with $g(x,y) = y^2 - x$ at $(0,0)$ (say $k = \mathbb{R}$)



Pf of Lemma: Making an invertible linear change of variables, we may assume

$f(X_0, X_1, X_2) = \sum_i a_i X_i^2$ is diagonal.

f is non-degenerate $\iff a_0 a_1 a_2 \neq 0$.

On the other hand, C_f is nonsingular

$\iff \forall\, i = 0, 1, 2 \quad C_f \cap \{X_i \neq 0\} \hookrightarrow \mathbb{A}^2$

is nonsingular.

Take $i=0$: $C_f \cap \{X_0 \neq 0\} \subset \{X_0 \neq 0\} \simeq \mathbb{A}^2$

then $C_f \cap \{X_0 \neq 0\}$ identifies to the affine curve

$$a_0 + a_1 y_1^2 + a_2 y_2^2 = 0.$$

$[X_0, X_1, X_2] \mapsto \left(\frac{X_1}{X_0}, \frac{X_2}{X_0}\right)$

$\| \quad \|$

$y_1 \quad y_2$

For $P \in C_f \cap \{X_0 \neq 0\}$, P is nonsing

$$\iff (2a_1 y_1(P) \quad 2a_2 y_2(P)) \neq (0 \quad 0)$$

(and similar calc for $i=1,2$)

So assume $a_0 a_1 a_2 \neq 0$ (f nondeg).

Then a singular point $P \in C_f \cap \{X_0 \neq 0\}$ (ditto other $i=1,2$) satisfies $y_1(P)=0$, $y_2(P)=0$; but then $a_0=0$, a contradiction.

Conclude: $C_f \cap \{X_0 \neq 0\}$ is nonsingular, and the same argument shows $C_f \cap \{X_i \neq 0\}$ is nonsing $\forall i$, hence C_f is nonsingular.

Conversely, if some $a_i = 0$ (let's say $a_0=0$) then $[1,0,0] \in C_f$ is a singular point.

$\mathbb{P}^2 = \{[a_0, a_1, a_2]\} = \bigcup_{i=0}^{2} \{[a_0, a_1, a_2] \mid a_i \neq 0\}$. ∎

$\nwarrow \underline{k^3 \setminus (0,0,0)}$

Examples $k = \mathbb{F}_p, \mathbb{Q}_p, \mathbb{Q}, \ldots$ Is $C_f(k) \neq \emptyset$?

- $k = \mathbb{F}_q$ (finite field of odd characteristic)

we may assume $f(X_0, X_1, X_2) = a_0X_0^2 + a_1X_1^2 + a_2X_2^2$ (char $k \neq 2$). Suffices to find $x, y \in \mathbb{F}_q$ such that $a_0x^2 + a_1y^2 + a_2 = 0$.

Take $a_0a_1a_2 \neq 0$ for simplicity (degenerate cases easier)

$\{a_0x^2 \mid x \in \mathbb{F}_q\}$ $\{-a_1y^2 - a_2 \mid y \in \mathbb{F}_q\}$ $x^2 + y^2 = 1$

both have $\frac{q+1}{2}$ elements — win by pigeonhole.

So $C_f(\mathbb{F}_q) \neq \emptyset$ in all such cases!

- In fact, any homogeneous quadratic $f \in \mathbb{F}_q[X_0, X_1, X_2]$ (for any q) has a non-zero solution. ("every conic over $\mathbb{F}_q$ has an $\mathbb{F}_q$-point")

(see Serre Chpt. 1, §2)

• $k = \mathbb{Q}_p$. Recall two constructions of $\mathbb{Q}_p$:

Analytic

$\mathbb{Q}$ has its p-adic abs. value $|\cdot|_p$ given by

$$\left|p^n \cdot \frac{a}{b}\right|_p = p^{-n} \quad \text{where } (ab, p) = 1.$$

$\mathbb{Q}_p$ = completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$ (Cauchy sequences modulo ~)

eg: $\mathbb{Q}_p \ni 1 + p + p^2 + \dots$

$|\cdot|_p$ extends to $\mathbb{Q}_p$, and we define

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

(check: $\mathbb{Q}_p$ is a field. $\mathbb{Z}_p$ is a ring. $\mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Q}_p$).

Algebraic

"inverse limit"

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n$$

$$:= \{(\dots, a_n, a_{n-1}, \dots, a_1) \mid a_i \in \mathbb{Z}/p^i \text{ and } \forall i = 2, 3, \dots, a_i \equiv a_{i-1} \bmod p^{i-1}\}$$

($\mathbb{Z}/p^n \to \mathbb{Z}/p^{n-1} \to \dots \to \mathbb{Z}/p^2 \to \mathbb{Z}/p$, $a_1 \in \mathbb{Z}/p$)

- Ring under component-wise $+, \cdot$
- $\mathbb{Z}_p$ is an integral domain. Set $\mathbb{Q}_p := \mathrm{Frac}(\mathbb{Z}_p)$

p-adic valuation

group homomorphism $\mathbb{Q}_p^* \to \mathbb{Z}$

$$v_p : \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{\infty\}$$

$$0 \longmapsto \infty$$

$$(\dots a_n, a_{n-1}, \dots a_1) \longmapsto \max\{n \mid a_n = 0\}.$$

($\hat{\mathbb{Z}}_p$; $\hat{\mathbb{Z}}/p^n$)

extended to $\mathbb{Q}_p$ by defining

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

for $a, b \in \mathbb{Z}_p$ $(b \neq 0)$

The relation between $|\cdot|_p$ and v_p is

$$|x|_p = p^{-v_p(x)} \quad (\text{for any } x \in \mathbb{Q}_p).$$

Quadratic form / $\mathbb{Q}_p$ Need not have non-zero solution ($C_f(\mathbb{Q}_p) = \emptyset$).

Example: $f(X,Y,Z) = X^2 + 3Y^2 - 15Z^2 \in \mathbb{Q}_3[X,Y,Z]$

Suppose $(a_0, a_1, a_2) \in \mathbb{Q}_3^3 \setminus 0$ satisfies

$f(a_0, a_1, a_2) = 0$.

Scaling by some 3^n we may assume $(a_0, a_1, a_2) \in \mathbb{Z}_3^3$ and at least one $v_3(a_i) = 0$.

$a_0^2 = -3a_1^2 + 15a_2^2 \Rightarrow v_3(a_0) > 0$. Since v_3 is a hom, $v_3(-3a_1^2 + 15a_2^2) = v_3(a_0^2) \geq 2$

$\Rightarrow v_3(-a_1^2 + 5a_2^2) \geq 1$

Reduce mod 3: $a_1^2 \equiv 5a_2^2 \bmod 3$, which is impossible ($5 \notin ((\mathbb{Z}/3)^\times)^2$), since we've assumed some $v_3(a_i) = 0$.

Remarks: (1) In particular, $C_f(\mathbb{Q}) = \emptyset$: the easiest way to show an equation has no $\mathbb{Q}$ solutions is to show it has no $\mathbb{Q}_p$ (for some p) solutions or no $\mathbb{R}$ solutions

(2) The issue in this example was that while C_f is nonsingular, $C_{f \bmod p}$ is singular.

If we avoid this, we'll get solutions in $\mathbb{Q}_p$ "lifting" solutions in $\mathbb{F}_p$, as we'll see next.

Hensel's Lemma

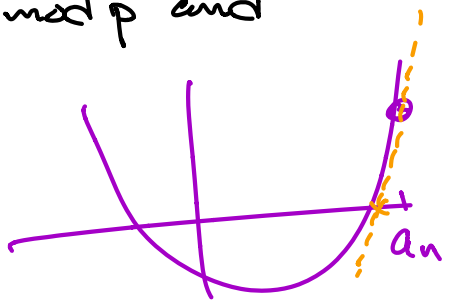
Version 1: (one variable) Let $f(x) \in \mathbb{Z}_p[x]$

Let $a \in \mathbb{Z}_p$ such that $f(a) \equiv 0 \bmod p$

and $f'(a) \not\equiv 0 \bmod p$

Then $\exists!$ $a' \in \mathbb{Z}_p$ such that $a' \equiv a \bmod p$ and $f(a') = 0$. (in $\mathbb{Z}_p$).

(on the 1st year sets) Newton's method!



Recursively define $a_1 = a$

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$

show that $\lim_{n\to\infty} a_n = a'$ works.

Refined version: (on problem set)

Assume $f(a) \equiv 0 \bmod p^n$ and that

$v_p(f'(a)) = k$ where $n > 2k$.

Then there is a unique $a' \in \mathbb{Z}_p$ such that

$f(a') = 0$ and $a' \equiv a \bmod p^{n-k}$.

Example: $p=2$. $f(x)=x^2+7 \in \mathbb{Z}_2[x]$.

Take $a=1$. $f(1)\equiv 0 \bmod 2^3$ and $v_2(f'(1))=1$

$3>2\cdot 1$, so refined Hensel shows $\exists!\ a' \in \mathbb{Z}_2$ such that $(a')^2=-7$ and $a'\equiv 1 \bmod 4$.

Version 2: Let $f(\underline{X}) \in \mathbb{Z}_p[X_0,\dots,X_n]$, and suppose there exists $a=(a_0,\dots,a_n)\in \mathbb{Z}_p^{n+1}$ and j, $0\le j\le n$, such that $v_p(f(a)) > 2\cdot v_p\left(\frac{\partial f}{\partial x_j}(a)\right)$.

Then $\exists\ a' \in \mathbb{Z}_p^{n+1}$ such that $f(a')=0$ and

$a' \equiv a \bmod p^{v_p(f(a)) - v_p\left(\frac{\partial f}{\partial x_j}(a)\right)}$

Pf: The case $n=0$ is literally the last result.

In general, we just vary a_j: $f(a_0,a_1,\dots,a_{j-1},X_j,a_{j+1},\dots,a_n) \in \mathbb{Z}_p[X_j]$ satisfies the hypotheses of the previous version, so $\exists\ a_j' \in \mathbb{Z}_p$: $a_j' \equiv a_j \bmod p^{v_p(f(a)) - v_p\left(\frac{\partial f}{\partial x_j}(a)\right)}$ such that $f(a_0,\dots,a_{j-1},a_j',a_{j+1},\dots,a_n)=0$. ✓

Cor Let $f(\underline{X}) \in \mathbb{Z}_p[X_0,\dots,X_n]$. Suppose $\bar{a} \in \mathbb{F}_p^{n+1}$ is a simple zero of $f(X) \bmod p \in \mathbb{F}_p[X_0,\dots,X_n]$: that is, $\frac{\partial f}{\partial x_j}(\bar{a}) \neq 0$ for at least one j.

Then $\bar{a}$ lifts to a zero $a \in \mathbb{Z}_p^{n+1}$ of f.

(Special case of Version 2).

↖ note this hypothesis says that the affine hypersurface over $\mathbb{F}_p$ $\{f \bmod p = 0\} \hookrightarrow \mathbb{A}^{n+1}$ is non-singular at $\bar{a}$.

Cor: $p \neq 2$. Let $f(x) = \sum_{i,j=0}^{n} a_{ij} X_i X_j \in \mathbb{Z}_p[X_0, \dots, X_n]$ with $a_{ij} = a_{ji}$ $\forall i,j$ be a quadratic form with $\det(a_{ij}) \in \mathbb{Z}_p^\times$. Fix $c \in \mathbb{Z}_p$ (e.g. $c = 0$). Suppose $\bar{a} = (a_0, \dots, a_n) \in \mathbb{Z}_p^{n+1}$ is a primitive solution to $f(x) = c \bmod p$, meaning not every a_i is divisible by p. ($\Leftrightarrow$ $a \bmod p \neq 0$). Then $\exists$ a solution $a' \in \mathbb{Z}_p^{n+1}$: $a' \equiv a \bmod p$ and $f(a') = c$

Pf: $\frac{\partial f}{\partial X_i} = 2 \sum_{j=0}^{n} a_{ij} X_j$ so if $\frac{\partial f}{\partial X_i}(\bar{a}) \equiv 0 \bmod p$ $\forall i$, then $[a_{ij}] \begin{bmatrix} a_0 \\ \vdots \\ a_n \end{bmatrix} = 0 \bmod p$, so $\det(a_{ij}) \equiv 0 \bmod p$, a contradiction. But then win by previous corollary.

Cor: $p = 2$. Let $f(x) \in \mathbb{Z}_2[X_0, \dots, X_n]$ be a quadratic form, and fix $c \in \mathbb{Z}_2$. Suppose $a \in \mathbb{Z}_p^{n+1}$ is a primitive solution to $f(x) = c \bmod 8$. Then $\exists$ $a' \equiv a \bmod 4$ such that $f(a') = c$ provided $\left(\frac{\partial f}{\partial X_j}(a) \bmod 4 \right)_j$ is not the zero vector (in particular, if $\det a_{ij} \in \mathbb{Z}_2^\times$).

(Similar to above — left to you).

Rmk: Replace $\mathbb{Q}_p$ by $\mathbb{R}$. Then the situation is clear: up to a linear change of var, every nondegenerate quadratic form in n variables is equivalent to $X_1^2 + \dots + X_r^2 - Y_1^2 - \dots - Y_s^2$ for some $0 \leq r, s \leq n$, $r+s=n$. $f(a) = 0$ has a solution in $\mathbb{R}^{n+1} \setminus 0$ (or in $\mathbb{P}^n(\mathbb{R})$) $\Leftrightarrow$ r and s are both non-zero.

Example: Checking for what p a quadratic form / $\mathbb{Q}$ has a non-zero solution in $\mathbb{Q}_p$.

Let $f(X,Y,Z) = X^2 - 13Y^2 + 17Z^2 \rightsquigarrow C_f \hookrightarrow \mathbb{P}^2$

$C_f(\mathbb{R}) \neq \emptyset$: $[\sqrt{13}, 1, 0]$. For primes p, we'll use Hensel's Lemma + analysis over $\mathbb{F}_p$.

For $p \neq 2, 13, 17$, $C_{f \bmod p}$ is non-singular, so it suffices to find a primitive solution mod p (for $p \neq 2, 13, 17$) — then Hensel forces a p-adic solution.

We've already seen (pigeonhole) that these primitive solutions exist — so $C_f(\mathbb{Q}_p) \neq \emptyset$ for $p \neq 2, 13, 17$.

$p=13$: (note $[0,1,0]$ is a singular point of $C_{f \bmod 13}$)

$f \bmod 13 = X^2 + 4Z^2$, so $[3,0,1]$ is a solution to $f \bmod 13$, and $\frac{\partial f}{\partial x}$ or $\frac{\partial f}{\partial z}$ at this point is $\neq 0$, so Hensel $\Rightarrow C_f(\mathbb{Q}_{13})$.

$p=17$: similarly $[8,1,0]$ lifts to a 17-adic solution

$p=2$: $f \bmod 8$ $f(2,1,1) \equiv 0 \bmod 8$ and $v_2\left(\frac{\partial f}{\partial y}(2,1,1)\right) = 1$, so we win again. **Conclusion:** $\forall p$, $C_f(\mathbb{Q}_p) \neq \emptyset$ and $C_f(\mathbb{R}) \neq \emptyset$.

Question: For this f, is $C_f(\mathbb{Q}) \neq \emptyset$? The 3-variable case of the Hasse-Minkowski thm says YES:

Thm Let $f \in \mathbb{Q}[X_0, \ldots, X_n]$ be a non-degenerate quadratic form. Then

$$\exists\, a \in \mathbb{Q}^{n+1} \setminus 0 : f(a) = 0 \iff \forall p, \exists\, a_p \in \mathbb{Q}_p^{n+1} \setminus 0 : f(a) = 0 \text{ and } \exists\, a_\infty \in \mathbb{R}^{n+1} \setminus 0 : f(a) = 0$$