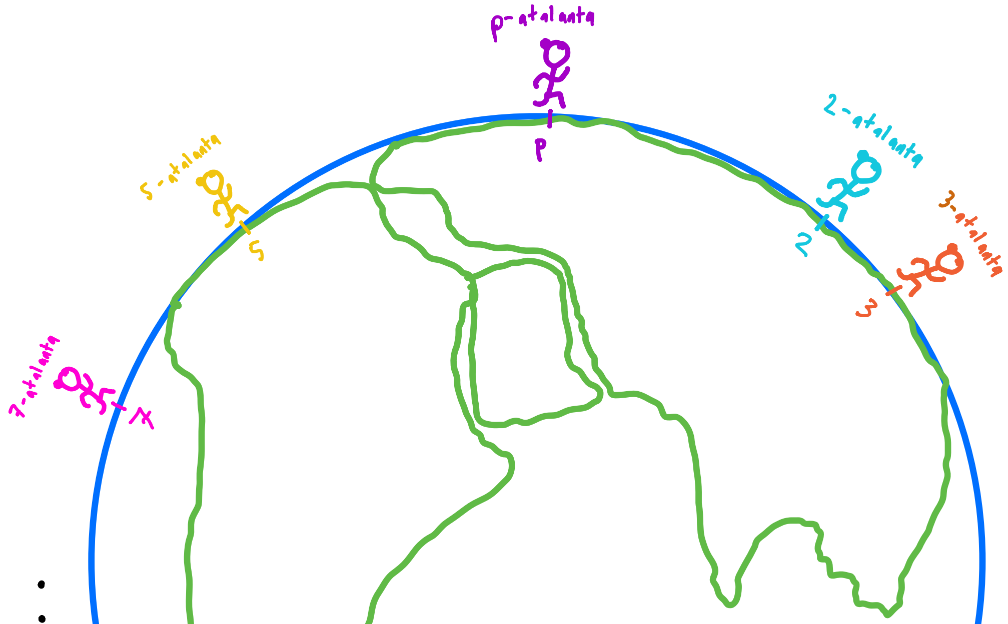
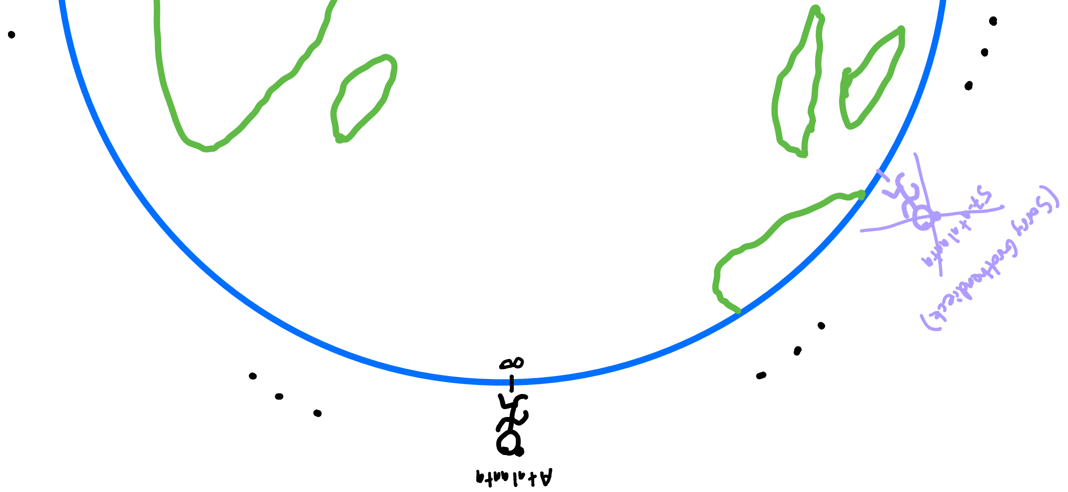
2021

Arizona Winter School

p-adic Lecture 4: Local-to-Global

Expanding Our Horizons





4.1 Hensel's Analogy: Prime and Space

$\mathbb{C}[x]$ = functions on…	$\mathbb{Z}$ = functions on…
the curve $\mathbb{A}^1_{\mathbb{C}}$	$\{p : p \text{ prime}\}$
 	
Evaluating $f \in \mathbb{C}[x]$ at $x=c$: $\pi_c : \mathbb{C}[x] \to \mathbb{C}[x]/(x-c) \cong \mathbb{C}$ $f \mapsto \pi_c(f) = f(c)$ "evaluation at $x=c$"	**Evaluating** $n \in \mathbb{Z}$ at p: $\pi_p : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ $n \mapsto \pi_p(n) = \bar{n} \pmod p$ "evaluation at p"
Examples: $f = x^3 - 2x^2 - 4x + 8$ $b=1$ $c=2$ - $\overline{x^3 - 2x^2 - 4x + 8} \in \mathbb{C}[x]/x-b$	Examples: $n = 12$ $p=2$ $m = -25$ $q=3$ - $\pi(12) = 12 \bmod 2 = \bar{0} \in \mathbb{F}_2$

$\parallel$

$\overline{1^3-2\cdot1^2-4\cdot1+8} \leadsto f(1)=3$

- $\overline{(x+2)(x-2)^2} \in \mathbb{C}[x]/x-2$

$\parallel$

$\overline{0} \leadsto f(2)=0$

$\pi_2(-25) = \overline{1} \text{ mod } 2 = \overline{1} \in \mathbb{F}_2$

- $\pi(12) = \overline{12} \text{ mod } 3 = \overline{0} \in \mathbb{F}_3$

$\pi(-25) = \overline{-1} \text{ mod } 3 = \overline{2} \in \mathbb{F}_3$

Rational functions

$\mathbb{C}(x) =$ quotients $\frac{f}{g}$

$f, g \in \mathbb{C}[x] \quad g \neq 0$

Rational numbers

$\mathbb{Q} =$ quotients $\frac{n}{m}$

$n, m \in \mathbb{Z} \quad m \neq 0$

Expansion around a point c

- $\mathbb{C}((x-c))$ Laurent series:

$$\sum_{i=n_0}^{\infty} c_i (x-c)^i$$

↖ can be negative

- Laurent/Taylor series expansion of a function ⇝ map

$T : \mathbb{C}(x) \longrightarrow \mathbb{C}((x-c))$

$h := \frac{f}{g} \longmapsto \sum_{i=n_0}^{\infty} c_i (x-c)^i$

reduced ↗

- $\mathbb{C}[[x-c]]$ power series

$x-c \nmid g$

$\Updownarrow$

c is not a "pole" of h

(h is defined at c)

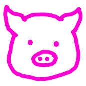
Expansion around a prime p

- $\mathbb{Q}_p$ field of p-adic #s:

$$\sum_{i=n_0}^{\infty} b_i p^i$$

↖ can be negative

- Expansion into pigits: of a rational # ⇝ map

 $: \mathbb{Q} \longrightarrow \mathbb{Q}_p$

$a = \frac{n}{m} \longmapsto \sum_{i=n_0}^{\infty} b_i p^i$

reduced ↗

- $\mathbb{Z}_p$ p-adic integers

$p \nmid m$

$\Updownarrow$

a "exists in" $\mathbb{Z}/p\mathbb{Z}$

$\Updownarrow$

$h \in \mathbb{C}[\![x-c]\!]$

$$T(h) = \overbrace{\underbrace{\overbrace{h(c)}^{\text{const.}} + h'(c)(x-c)}_{\text{lin. approx}} + \frac{h''(c)}{2!}(x-c)^2}^{\text{quadratic approx}} + \dots$$

$(\exists$ sol'n to $mx = n \pmod{p})$

$\Updownarrow$ Hensel's lemma!!

$a \in \mathbb{Z}_p$

$$🐷(a) = \overbrace{\underbrace{\overbrace{b_0}^{a_0 \text{ mod } p} + b_1 p}_{a_1 \text{ approx mod } p^2} + b_2 p^2}^{a_2 \text{ approx mod } p^3} + b_3 p^3 + \dots$$

Vanishing for $\mathbb{C}[\![x-c]\!]$

- If $h = \sum_{i=n_0}^{\infty} c_i (x-c)^i \in \mathbb{C}[\![x-c]\!]$ and $c_{n_0} \neq 0$, we say h vanishes at c with order n_0

ex: $\frac{x^2}{x-1}$ at $x=0$:

$= 0 + 0x + x^2 + x^3 + \cdots$

order 2 zero at $x=0$.

Vanishing for $\mathbb{Z}_p$

- If $a = \sum_{i=n_0}^{\infty} b_i p^i \in \mathbb{Z}_p$ and $b_{n_0} \neq 0$, then $v_p(a) = n_0$ is "order of vanishing of a at p"

ex: $\frac{25}{3}$ at $p=5$:

$= 0 + 0 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \dots$

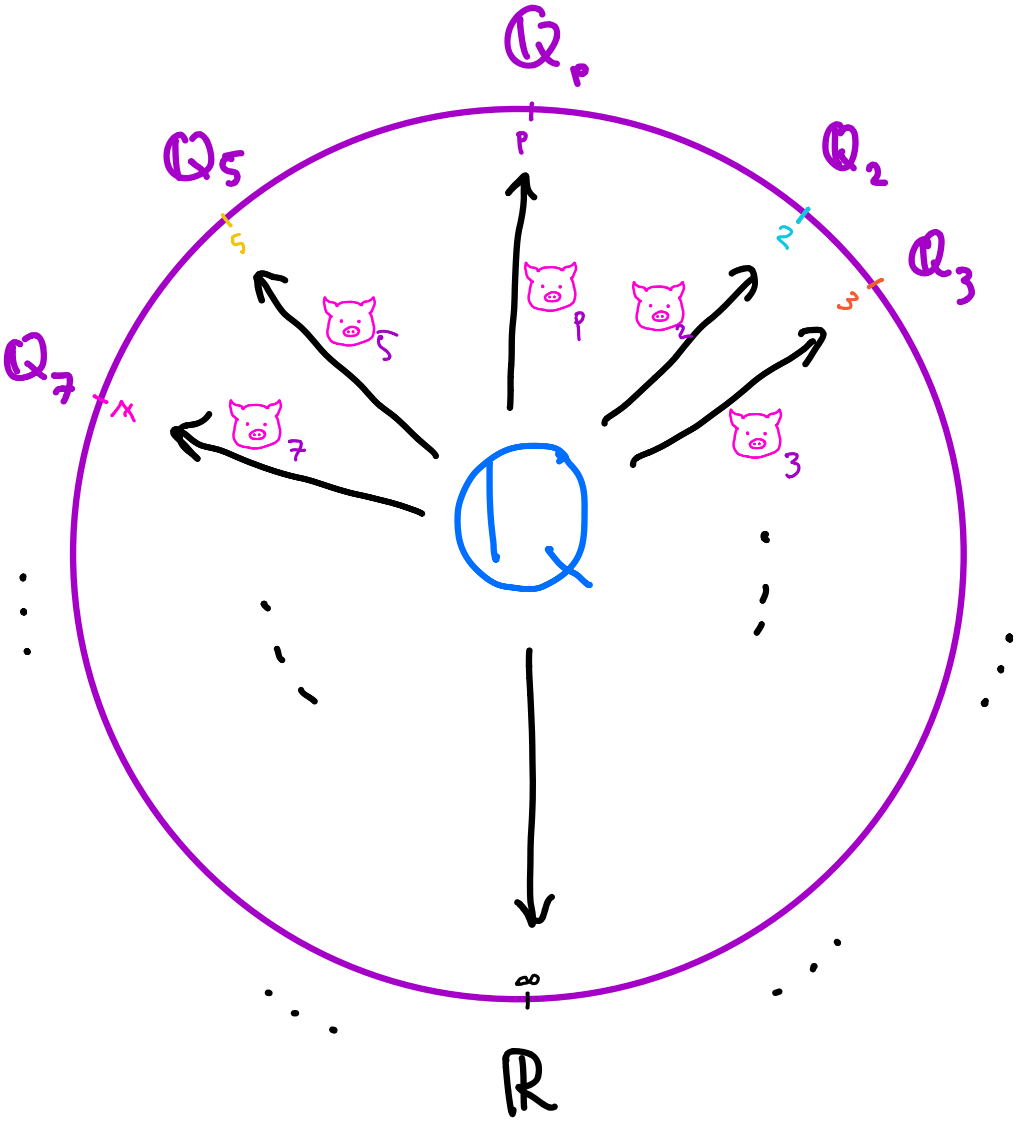
vanishes w/ order 2 at $p=5$

4.2 Local to Global Principle

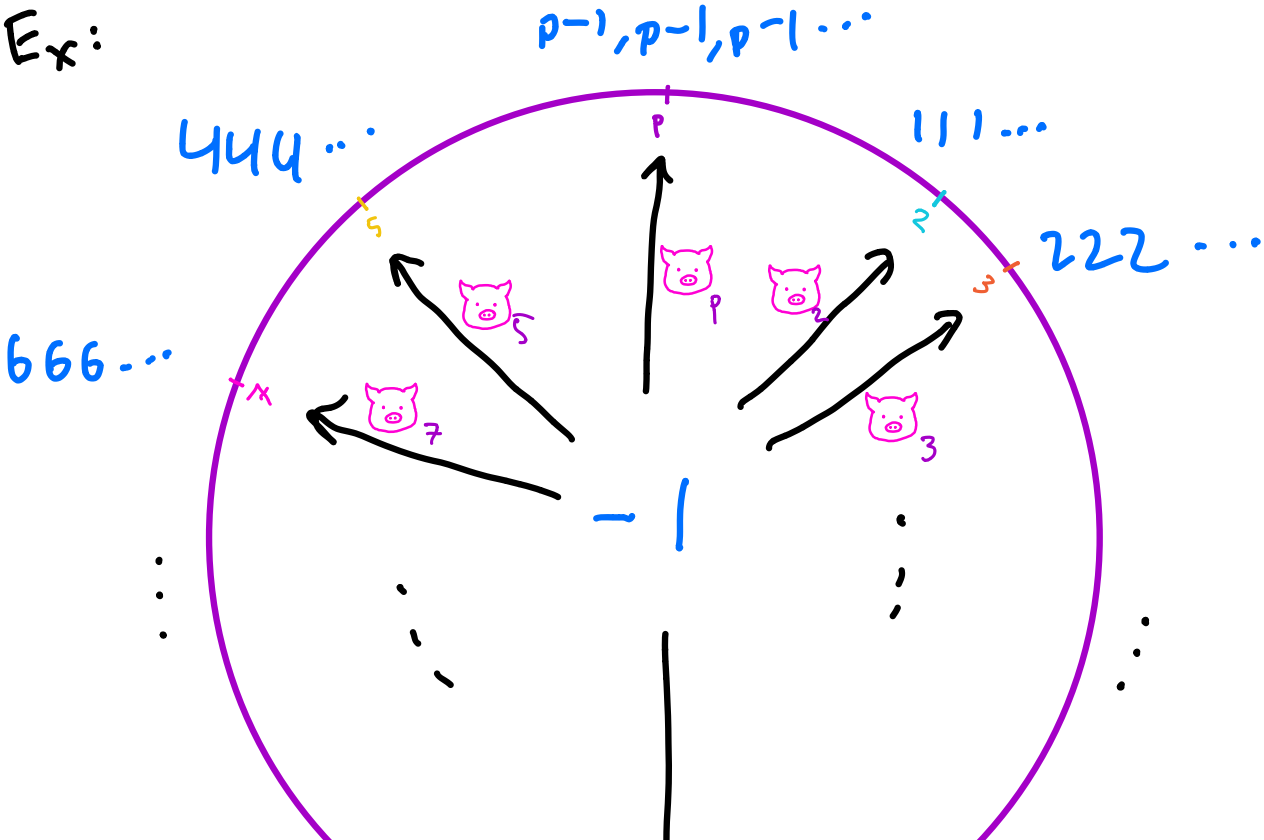
- Along these lines, we can think of the natural map

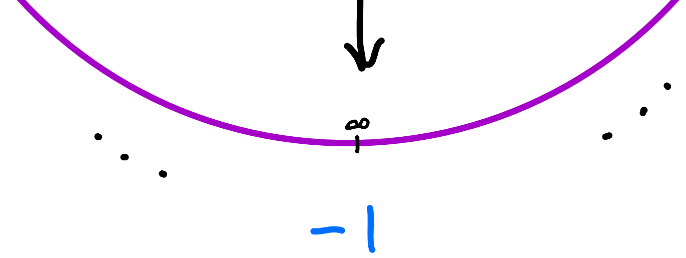
$$\text{loc}: \mathbb{Q} \longrightarrow \prod_{p \leq \infty} \mathbb{Q}_p$$

as recording the "local behavior" of "functions" $a \in \mathbb{Q}$ at all "points" p including $p = \infty$.


$\mathbb{Q}_p$
$\mathbb{Q}_5$
$\mathbb{Q}_2$
$\mathbb{Q}_3$
$\mathbb{Q}_7$
p
5
2
3
7
$\mathbb{Q}$
∞
$\mathbb{R}$

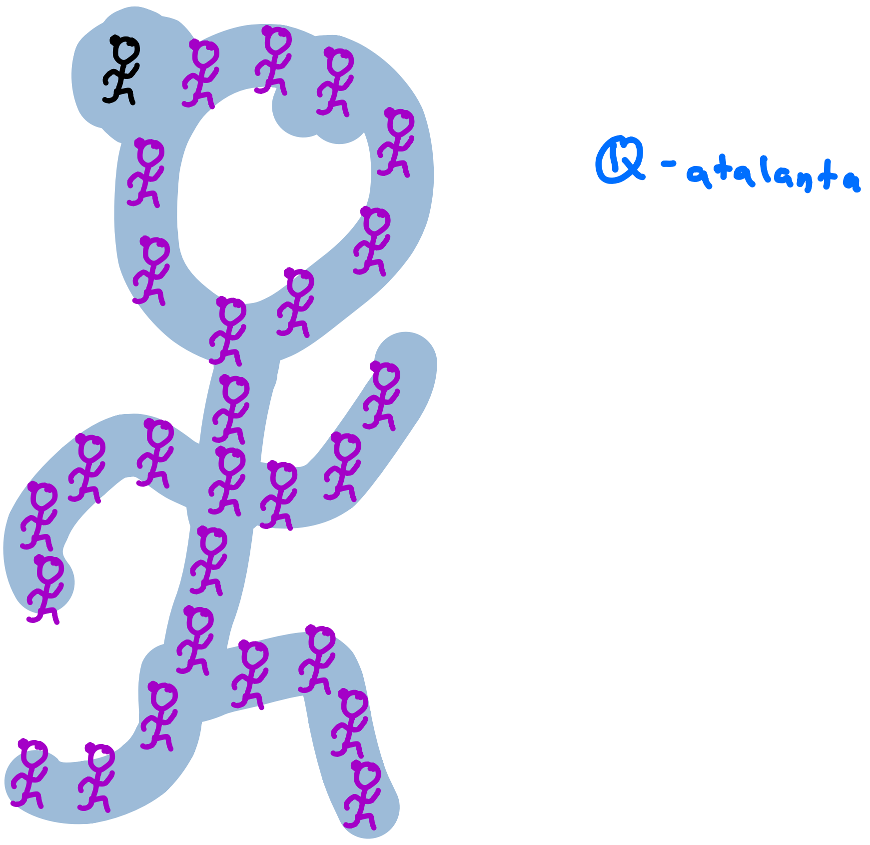
Ex:


p−1, p−1, p−1 ...
444...
111...
222...
666...
p
5
2
3
7
−1



- If $f \in \mathbb{Q}[X_1,\dots,X_n]$ and $\exists v=(x_1,\dots,x_n)\in\mathbb{Q}^n$ s.t. $f(v)=0$, then $f(v_p)=0$ $\forall p\leq\infty$, where v_p is the image of v in $\mathbb{Q}_p$
- "Global" root of f $\rightsquigarrow$ "local" roots of f.
- $\leftsquigarrow$?

Local-Global Principle:
The existence of solutions in $\mathbb{Q}$ of $f\in\mathbb{Q}[X_1,\dots,X_n]$ can be determined by studying solutions of f in $\mathbb{Q}_p$ $\forall p\leq\infty$.



- Why we would like this:
  - Over $\mathbb{R}$: tricks for determining if there's a real soln, like disc. of a quadratic, degree, sign, etc
  - Over $\mathbb{Z}_p$: Hensel's Lemma!

    ★ May need to scale f so coeffs in $\mathbb{Z}_p$

$$\begin{tikzcd}
\{\text{roots } a \in \mathbb{Z}_p \text{ of } f \in \mathbb{Z}_p[X]\} \arrow[r] \arrow[dr] \arrow[ddr] \arrow[ddd, leftrightarrow] & \text{root } a_0 \text{ in } \mathbb{Z}/p\mathbb{Z} \\
& \text{root } a_1 \text{ in } \mathbb{Z}/p^2\mathbb{Z} \\
& \text{root } a_2 \text{ in } \mathbb{Z}/p^3\mathbb{Z} \\
\left\{\begin{array}{l}\text{roots } a_0 \in \mathbb{F}_p \text{ of } \bar{f} \in \mathbb{F}_p[X] \\ \text{s.t. } \bar{f}'(a_0) \not\equiv 0 \pmod{p}\end{array}\right\} & \vdots
\end{tikzcd}$$

★
$$\begin{tikzcd}
\text{a is a unit in $\mathbb{Z}_p$} \arrow[rr, Leftrightarrow] \arrow[d, Leftrightarrow] & & \text{$a \not\equiv 0$ in $\mathbb{Z}/p\mathbb{Z}$} \arrow[d, Leftrightarrow] \\
|a|_p = 1 \arrow[dr, Leftrightarrow] & & \text{$\bar{a}$ is a unit in $\mathbb{Z}/p\mathbb{Z}$} \arrow[dl, Leftrightarrow] \\
& b_0 \neq 0 &
\end{tikzcd}$$

- But local-global principle does not hold in general ☹ (Exercise in pset)

4.3 Salvaging Local-Global

- We start by introducing a useful tool:

(Weak) Approximation Theorem

Let $V = \{p \in \mathbb{Z} : p \text{ prime}\} \cup \{\infty\}$ and let S be a finite subset of V. Then the image of $\mathbb{Q}$ in

$$\mathrm{loc}_S : \mathbb{Q} \to \prod_{p \in S} \mathbb{Q}_p$$

is dense.

That is, for any $(x_p)_{p \in S} : x_p \in \mathbb{Q}_p$,
for any $(\varepsilon_p)_{p \in S} : \varepsilon_p \in \mathbb{R}_{>0}$,
$\exists x \in \mathbb{Q} : |x - x_p|_p < \varepsilon_p \ \forall p \in S$.

Proof: suppose $S = \{\infty, p_1, \ldots, p_n\}$, p_i distinct, and let $(x_\infty, x_1, \ldots, x_n) \in \mathbb{R} \times \mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_n}$.

- Can assume $x_i \in \mathbb{Z}_{p_i}$ for $1 \le i \le n$ (mult. by an integer)
- WTS $\forall \varepsilon > 0, \forall N \in \mathbb{N}, \exists x \in \mathbb{Q}$:

$$|x - x_\infty| \le \varepsilon \quad \text{and} \quad v_{p_i}(x - x_i) \ge N \text{ for } 1 \le i \le n.$$

- By ~~Chinese~~ Sun Tzu Remainder Theorem, $\exists \tilde{x} \in \mathbb{Z}$:
  $\tilde{x} \equiv \overline{x}_i \pmod{p_i^N} \ \forall 1 \le i \le n$.
- Let $q \in \mathbb{Z}_{>0} : p_i \nmid q \ \forall 1 \le i \le n$. Choose $a, m \in \mathbb{Z}$:

$$|\tilde{x} - x_\infty + \frac{a}{q^m} p_1^N \cdots p_n^N| < \varepsilon$$

$$|\tilde{x} - x_\infty + \frac{a}{q^m} p_1 \cdots p_n|_\infty < \varepsilon$$

and let $x = \tilde{x} + \frac{a}{q^m} p_1^N \cdots p_n^N$. $\blacksquare$

- Example: $x_\infty = \pi$, $\varepsilon_\infty =$

$$\begin{cases} x_7 = \sqrt{2} = 3 + 1 \cdot 7 + 2 \cdot 7^2 + \dots \in \mathbb{Q}_7, & \varepsilon_7 = \frac{1}{5} \\ x_3 = -1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots \in \mathbb{Q}_3, & \varepsilon_3 = \frac{1}{8} \end{cases}$$

$\rightsquigarrow \tilde{x} = 17 \quad (17 \equiv 8 \ (3^2), \quad 17 \equiv 3 \ (7))$

$\rightsquigarrow x = 17 - \frac{224}{10^3} \cdot 7 \cdot 3^2$ works. Check it!

- Now for some great news!

Hasse–Minkowski Theorem

Let $F(X_1, X_2, \dots, X_n) \in \mathbb{Q}[X_1, X_2, \dots, X_n]$ be a quadratic form. Then

$$F(X_1, X_2, \dots, X_n) = 0$$

has solutions in $\mathbb{Q}$ iff it has solns in $\mathbb{Q}_p$ $\forall p \leq \infty$.

- Before we get into the proof, an application:

Question:

For which $a, b, c \in \mathbb{Q}$ does

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

have a nontrivial rational solution?

- Simplyfing the polynomial:
  - Let $f(X,Y,Z) = aX^2+bY^2+cZ^2$.

    Then if $d\neq 0$, $f(x,y,z)=0$ iff $df(x,y,z)=0$

    So can assume $a,b,c \in \mathbb{Z}$ with no common factors

    $\Rightarrow$ can assume pairwise rel. prime (exercise, not on a test!)
  - If $a = a_1 a_2^2$, then (x,y,z) is a root of f iff (a_2x, y, z) is a root of $a_1X^2+bY^2+cZ^2$.

    Can assume a,b,c squarefree
- By HM, equivalent to check when f has roots in $\mathbb{Q}_p$
  - $p=\infty$: real roots

    $\exists$ root in $\mathbb{R}$ $\Longleftrightarrow$ a,b,c not all same sign

  - p odd prime: $p \nmid abc$

    Lemma: Let p be an odd prime, and let $a,b,c \in \mathbb{Z}$ pairwise relatively prime and prime to p. Then $\exists\, x_0, y_0, z_0$ in $\mathbb{Z}$ not all divisible by p s.t.

    $$ax_0^2+by_0^2+cz_0^2 \equiv 0 \pmod{p}.$$

    Proof: We will find a solution with $z_0 \equiv 1$, so a soln to $ax_0^2+by_0^2+c \equiv 0 \ (p)$.

    $$\Updownarrow$$

    $$ax_0^2 \equiv -c-by_0^2 \ (p)$$

    - Since there are $\frac{p+1}{2}$ squares mod p and a is invertible mod p, there are $\frac{p+1}{2}$ possible #s that can occur on the left by choosing different x_0's

- Similarly, there are $(p+1)/2$ #s that can occur on the right
- Hence there must be some overlap, proving Lemma.

- WLOG $x_0 \not\equiv 0 \bmod p$. Let

$$g(X) = aX^2 + by_0^2 + cz_0^2.$$

- Hensel's Lemma ⇝ $x \in \mathbb{Z}_p : g(x) = 0$
  $\Rightarrow (x, y_0, z_0)$ is a root of f.

- $p = 2$, $2 \nmid abc$:
  - If $\exists$ a soln $(x, y, z) \in \mathbb{Q}_2^3$, we can suppose $x, y, z \in \mathbb{Z}_p$ and one of x, y, z has abs.val. 1 (else scale by a suitable power of 2)
  - $0 \equiv ax^2 + by^2 + cz^2 \equiv x^2 + y^2 + z^2 \pmod 2$
    $\Rightarrow$ WLOG $y \equiv z \equiv 1 \pmod 2$, $x \equiv 0 \pmod 2$
    $\Rightarrow y^2 \equiv z^2 \equiv 1 \bmod 4$, $x^2 \equiv 0 \bmod 4$
    $\Rightarrow 0a + 1b + 1c \equiv 0 \bmod 4$
  - So, soln over $\mathbb{Q}_2 \Rightarrow$ two of a, b, c sum to $0 \bmod 4$.

Theorem

Suppose $a, b, c \in \mathbb{Z}$ are relatively prime and squarefree.

Then

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

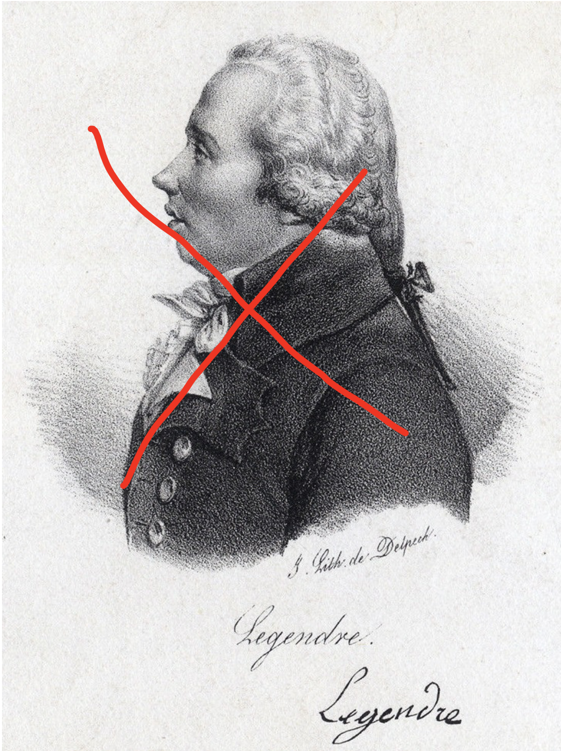
has nontrivial solns in $\mathbb{Q}$ iff all of the following hold

i) a, b, c do not all have the same sign
ii) if $p \mid a$ and $p \neq 2$, $\exists r \in \mathbb{Z} : b + r^2 c \equiv 0 \mod p$ (same for b, c)
iii) if $2 \nmid abc$, then two of $\{a, b, c\}$ sum to $0 \mod 4$
iv) if $2 \mid a$, then $8 \mid b+c$ or $8 \mid a+b+c$ (similarly for b, c)

Proof of the rest: exercise(s).

4.4 Proof of Hasse–Minkowski

- Hasse–Mi2kowski ($n=2$) — Professor Chan!
- Hasse–Mi3kowski ($n=3$): due to Legendre



2005

- Suppose $f = aX^2 + bY^2 + cZ^2$ with $a, b, c \in \mathbb{Q}^\times$ and suppose that $\forall\, p \leq \infty$, $\exists\, v_p := (x_p, y_p, z_p) \in (\mathbb{Q}_p)^3$ with $v_p \neq (0,0,0)$ and $f_p(x_p, y_p, z_p) = 0$.

- Simplifying f:

$$f_p(v_p) = 0 \text{ iff } \frac{1}{a} f_p(v_p) = 0$$

assume $a = 1$

- If $b = b_1 b_2^2$ for some $b_1, b_2 \in \mathbb{Q}$, then

$$f_p(v_p) = (x_p)^2 + b(y_p)^2 + c(z_p)^2$$

$$= (x_p)^2 + b_1(b_2 y_p)^2 + c(z_p)^2$$

- So may assume b, c squarefree integers and $|b| \leq |c|$.

- So $f = X^2 - bY^2 - cZ^2$.

We induct on $m = |b| + |c|$.

- $m = 2$: $f = X^2 \pm Y^2 \pm Z^2$

$$\hookrightarrow \begin{cases} \cancel{f = X^2 + Y^2 + Z^2} & f \text{ has real zero} \\ f = X^2 + Y^2 - Z^2 & (1, 0, 1) \\ f = X^2 - Y^2 - Z^2 & (1, 0, 1) \end{cases}$$

- $m > 2$:
  - We'll find "smaller" g s.t. g has a nontrivial 0 iff f does
    - We'll show b is a square mod c.
    - If $m > 2$, then $|c| \geq 2$, $c = \pm p_1 \cdots p_k$ distinct. let $p := p_1$.

      Lemma: b is a square mod p.

      Pf: if $b \equiv 0 \pmod{p}$, done.

      * So suppose $b \not\equiv 0 \pmod{p}$

        $x_p^2 - b y_p^2 - c z_p^2 = 0$ in $\mathbb{Q}_p$
      * Scaling v_p by $\max\{|x_p|, |y_p|, |z_p|\}$, we can assume $x_p, y_p, z_p \in \mathbb{Z}_p$ and one of x_p, y_p, z_p has abs. val. 1.
      * $x_p^2 - b y_p^2 \equiv 0 \pmod{p}$

        If $y_p \equiv 0\ (p)$, then $x \equiv 0\ (p)$, so $c z_p^2 \equiv 0\ (p^2)$

        so $z_p \equiv 0\ (p)$, contradicting *
      * So $y_p \not\equiv 0\ (p) \rightsquigarrow b = (x_p/y_p)^2$ mod $p \Rightarrow$ lemma!
    - ~~Chinese~~ Sun Tzu Remainder Theorem

      $\Rightarrow \mathbb{Z}/c\mathbb{Z} \cong \prod_i \mathbb{Z}/p_i\mathbb{Z} \Rightarrow b$ is a square mod c.
  - $\exists\, t, \tilde{c} \in \mathbb{Z}$: $t^2 = b + \tilde{c}c$ with $|t| \leq |c|/2$

    $\Rightarrow \tilde{c}c = t^2 - b = N(t + \sqrt{b}) \Rightarrow (b, \tilde{c}c) = 1$ (Chan 3.4)
  - So $1 = (b, c) \cdot (b, \tilde{c})$ (Chan 3.4)

    so f has a nontriv. 0 in k

    $\Updownarrow$

$h := X^2 - bY^2 - \tilde{c}Z^2$ has a nontriv. 0 in k

for $k = \mathbb{Q}$ or $\mathbb{Q}_p$ for any $p \leq \infty$.

- $|\tilde{c}| = \left|\frac{t^2-b}{c}\right| \leq \frac{|c|}{4} + 1 < |c|$ since $|c| \geq 2$
- Finally, let $\tilde{c} = \gamma u^2$ with $\gamma, u \in \mathbb{Z}$, γ squarefree, and let $g = X^2 - bY^2 - \gamma Z^2$. Note: $|\gamma| < |c|$

By induction, g has a nontrivial root in $\mathbb{Q} \Rightarrow f$ has a nontrivial root in $\mathbb{Q}$. ■

- Hasse–Minkowski: $(n=4)$ Prof. Chan

- Hasse–Minkowski $(n \geq 5)$

  We proceed by induction.

  - write $f = \underbrace{a_1X^2 + a_2X_2^2}_{h} - \underbrace{(-(a_3X_3^2 + \cdots + a_nX_n^2))}_{g}$
  - Let

    $S = \{\infty\} \cup \{2\} \cup \{p \text{ prime} : |a_i|_p \neq 1 \text{ for some } i \geq 3\}$

  - By the hypothesis, $\exists\, c_p, x_{1,p}, \dots, x_{n,p} \in \mathbb{Q}_p$:

    $h(x_{1,p}, x_{2,p}) = c_p = g(x_{3,p}, \dots, x_{n,p})$.

Let $\mathbb{Q}_p^{\times 2} = \{y^2 : y \in \mathbb{Q}_p^{\times}\}$. Then $\mathbb{Q}_p^{\times 2}$ is open in $\mathbb{Q}_p$ (check!)

- By weak approximation theorem, $\exists\, x_1, x_2 \in \mathbb{Q}$: $\dfrac{h(x_1, x_2)}{c_p} \in \mathbb{Q}_p^{\times 2}$ $\forall p \in S$.

  Let $c := h(x_1, x_2)$. Then $h = c$ has a nontriv. soln in $\mathbb{Q}_p$ for $p \in S$

- Let $f_1 = cZ^2 - g$. Then $f_1 = 0$ has a nontrivial root in $\mathbb{Q}_p$ for $p \in S$

- If $p \notin S$, the coefficients of $d_p(g)$ are units so $\varepsilon_p(g) = 1$

- Hence f_1 has a nontrivial 0 in $\mathbb{Q}_p$ for <u>all</u> p !

- By induction, f_1 has a nontrivial 0 in $\mathbb{Q}$ so $g = c$ has a nontrivial soln in $\mathbb{Q}$, so $f = 0$ has nontriv. soln in $\mathbb{Q}$ ∎