Negative results on $\mathbb{Q}_p$

(1930's) Artin conjectured that any form f of degree d in n variables with coefficients in a p-adic field $\mathbb{Q}_p$ must have a non-trivial zero in that field if $n > d^2$

i.e. $\mathbb{Q}_p$ is C_2

Motivation: $\mathbb{F}_p((t))$ is C_2

But $\mathbb{F}_p((t)) \ncong \mathbb{Q}_p$ in fact $\mathrm{char}(\mathbb{F}_p((t))) = p \neq 0 = \mathrm{char}(\mathbb{Q}_p)$

Def

Let d and i be two positive integers and let K be a field.
Suppose that any form with coefficients in K of degree d in more than d^i variables has a non-trivial solution in K. Then K is said to have the property $C_i(d)$

Remark

K is C_i if it has property $C_i(d)$ $\forall d > 0$

Theorem (Hasse 1924)

$\mathbb{Q}_p$ has property $C_2(2)$ $\forall$ prime p

Theorem (Demyanov 1950 ($p \neq 3$), Lewis 1952 ($\forall p$))

$\mathbb{Q}_p$ has property $C_2(3)$ $\forall$ prime p

But in (1966) Terjanian found a counter-example in degree 4:
He constructed a form h of 18 variables of degree 4 s.t. h does not have a non-trivial solution in $\mathbb{Q}_2$

$\Rightarrow$ $\mathbb{Q}_2$ is not C_2

Construction:

$$f(X_1,X_2,X_3) = X_1^4 + X_2^4 + X_3^4 - X_1^2X_2^2 - X_1^2X_3^2 - X_2^2X_3^2 - X_1^2X_2X_3 - X_2^2X_1X_3 - X_3^2X_2X_1$$

$$g(X_1,\dots,X_9) = f(X_1,X_2,X_3) + f(X_4,X_5,X_6) + f(X_7,X_8,X_9)$$

$$h(X_1,\dots,X_{18}) = g(X_1,\dots,X_9) + 4\cdot g(X_{10},\dots,X_{18})$$

Remark

Since h is an hom. polynomial $\Rightarrow$ it suffices to prove that we cannot find a primitive solution in $\mathbb{Z}_2^{18}$

$\hookrightarrow$ $\underline{x} = (x_1,\dots,x_{18})$ is primitive if at least one of the x_i's is a unit

Recall: $a \in \mathbb{Z}_p \Rightarrow a = a_0 + a_1 p + a_2 p^2 + \dots$ where $a_i \in \{0,\dots,p-1\}$

a is a unit $\Leftrightarrow$ $a_0 \neq 0$

Claim 1: if $\underline{x}$ is a primitive vector $\Rightarrow$ $f(\underline{x}) \equiv 1 \mod 4$

proof

$$f(X_1,X_2,X_3) = X_1^4 + X_2^4 + X_3^4 - X_1^2X_2^2 - X_1^2X_3^2 - X_2^2X_3^2 - X_1^2X_2X_3 - X_2^2X_1X_3 - X_3^2X_1X_2$$

$f(x_1,x_2,x_3) = x_1^4 + x_2^4 + x_3^4 - x_1^2x_2^2 - x_1^2x_3^2 - x_2^2x_3^2 - x_1^2x_2x_3 - x_2^2x_1x_3 - x_3^2x_1x_2$

$\frac{\partial f}{\partial x_1} \equiv -x_2^2x_3 - x_2x_3^2 \bmod 2$

If $\alpha \in \mathbb{Z}_2 \Rightarrow \alpha^2 \equiv \alpha \bmod 2 \Rightarrow$ for any $x = (x_1,x_2,x_3)$ $\frac{\partial f}{\partial x_1}(x) \equiv 0 \bmod 2$

f symmetric $\Rightarrow \frac{\partial f}{\partial x_2} \equiv \frac{\partial f}{\partial x_3} \equiv 0 \bmod 2$

Also $\frac{\partial^2 f}{\partial x_1^2} \equiv 0 \bmod 2$

If $x = (x_1,x_2,x_3)$ is a primitive vector $\Rightarrow x_i \equiv \varepsilon_i + 2x_i' \bmod 4$

and $\varepsilon_i = 0$ or 1 but at least one of them is 1

we compute $f(x) \bmod 4$ by the Taylor expansion at $(\varepsilon_1,\varepsilon_2,\varepsilon_3)$:

$$f(x_1,x_2,x_3) \equiv f(\varepsilon_1,\varepsilon_2,\varepsilon_3) + \sum_{i=1}^{3} \frac{\partial f}{\partial x_i}(\varepsilon_1,\varepsilon_2,\varepsilon_3)\cdot(2\cdot x_i') + \frac{1}{2}\left(\sum_{i=1}^{3} \frac{\partial^2 f}{\partial x_i^2}(\varepsilon_1,\varepsilon_2,\varepsilon_3)(2\cdot x_i')^2\right)$$

$$+ \sum_{i\neq j} \frac{\partial^2 f}{\partial x_i \partial x_j}(\varepsilon_1,\varepsilon_2,\varepsilon_3)\, 4\cdot x_i' x_j'$$

$$\equiv f(\varepsilon_1,\varepsilon_2,\varepsilon_3) \bmod 4$$

Notice $f(1,1,1) \equiv f(1,1,0) \equiv f(1,0,0) \equiv 1 \bmod 4$ $\square$

Remark

For any primitive vector $x = (x_1,\dots,x_9) \in \mathbb{Z}_2^9 \Rightarrow g(x) \equiv 1, 2$ or $3 \bmod 4$

in particular $g(x) \not\equiv 0 \bmod 4$

Claim 2: h has no primitive zero mod 16

Proof

Let $x = (x_1,\dots,x_{18})$ be such that $h(x) \equiv 0 \bmod 16$

$\Rightarrow h(x) = g(x_1,\dots,x_9) + 4\, g(x_{10},\dots,x_{18}) \equiv 0 \bmod 16$

$\Rightarrow g(x_1,\dots,x_9) \equiv 0 \bmod 4 \Rightarrow (x_1,\dots,x_9)$ is not primitive

$\Rightarrow (x_1,\dots,x_9) = 2\cdot(x_1',\dots,x_9') \Rightarrow h(x) = 16\, g(x_1',\dots,x_9') + 4g(x_{10},\dots,x_{18})$

$\Rightarrow g(x_{10},\dots,x_{18}) \equiv 0 \bmod 4 \Rightarrow (x_{10},\dots,x_{18})$ is not primitive $\square$

$\Rightarrow$ we cannot find any solution in $\mathbb{Z}_2$ $\Rightarrow$ $\mathbb{Q}_2$ does not have property C_2

Question: What about $p>2$?

Schanuel: $\mathbb{Q}_p$ does not have property $C_2(p(p-1))$

He constructed a form h of degree $d = p\cdot(p-1)$ in $p\cdot(p+1)(p-1)^2$ variables with no primitive zeros:

$f(X,Y) = \phi(X^{p-1}, Y^{p-1})$

$\phi(X,Y) = X^p + Y^p - \frac{1}{2}(X^{p-1}Y + XY^{p-1})$

any $(x,y) \in \mathbb{Z}_p^2$ primitive $\overset{\text{to prove}}{\Longrightarrow}$ $f(x,y) \equiv 1 \mod p^2$

Remark

If x and y are both units in $\mathbb{Z}_p$ $\Rightarrow$ $x^{p-1} \equiv y^{p-1} \equiv 1 \mod p$

If x say is a unit and $y = p \cdot \eta$ $\Rightarrow$ $y^{p-1} \equiv 0 \mod p^2$

Lemma

If one of x,y is congruent to $1 \mod p$ and the other one is either $\equiv 1 \mod p$ or $\equiv 0 \mod p^2$ $\Rightarrow$ $\phi(X,Y) \equiv 1 \mod p^2$

proof

$x = 1 + p\xi$ $\Rightarrow$ $x^{p-1} \equiv 1 - p\xi \mod p^2$

$x^p \equiv 1 \mod p^2$

we have two cases:

① $y = 1 + p\xi$ $\Rightarrow$ $x^p + y^p \equiv 2 \mod p^2$

$x^{p-1}y \equiv 1 + p(\eta - \xi) \mod p^2$

$xy^{p-1} \equiv 1 + p(\xi - \eta) \mod p^2$

$\Rightarrow \phi(x,y) \equiv 2 - \frac{1}{2}\cdot(2) \equiv 1 \mod p^2$

② $y = p^2\eta$ $\Rightarrow$ $y^{p-1} \equiv y^p \equiv 0 \mod p^2$ $\Rightarrow \phi(x,y) \equiv x^p \equiv 1 \mod p^2$ $\square$

We consider now $g(V) = f(V_1) + f(V_2) + \dots + f(V_{p^2-1})$

where V_i is a vector of 2 variables $1 \le i \le p^2-1$

$\Rightarrow V$ is a vector of $2 \cdot (p^2-1)$ variables

$\Rightarrow$ $\forall$ primitive vector $\underline{v}$ $\Rightarrow$ $g(\underline{v}) \not\equiv 0 \mod p^2$ (By the lemma)

we define

$h = g_0 + p^2 g_2 + p^4 g_4 + \dots + p^{d-2} g_{d-2}$ where g_i are copies of g with new variables in each copy

$\Rightarrow$ the number of variables of h is $n = \frac{p\cdot(p-1)}{2} \cdot 2 \cdot (p^2-1) = p(p+1)(p-1)^2$

$\Rightarrow$ Same argument as before $\Rightarrow$ h has no primitive zero $\mod p^d$ $\square$

since $n > d^2$ $\Rightarrow$ we have a counterexample

All these counterexamples have less than d^3 variables

All these counterexamples have less than d^3 variables

Theorem (Brauer 1945)

There is an integer $\psi(p,d) \geq d^2$ such that any form over $\mathbb{Q}_p$ of degree d in n variables with $n > \psi(p,d)$ has a non-trivial zero in $\mathbb{Q}_p$

(1982) Arhipov and Karacuba:

Taking $\psi(p,d)$ to be minimal with respect to this property they proved that $\forall p$ there are infinitely many d such that

$$\psi(p,d) > \exp_p\left(\frac{d}{(\log_p d)^2(\log_p\log_p d)^3}\right)$$

$$\Rightarrow \lim_{d\to\infty} \frac{\exp_p\left(\frac{d}{(\log_p d)^2(\log_p\log_p d)^3}\right)}{d^i} = \infty \quad \Rightarrow \quad \mathbb{Q}_p \text{ is not } C_i \text{ for all } i.$$

Theorem (Alemu 1983)

Every finite extension of the field of p-adic numbers is not C_i for any i

Theorem (Ax-Kochen 1965)

"$\mathbb{Q}_p$ is almost C_2": Given a degree d, let X_d be the set of primes p such that $\mathbb{Q}_p$ does not have the property $C_2(d)$ $\Rightarrow$ X_d is a finite set.

~ o ~

Theorem (Hasse)

$\mathbb{Q}_p$ has property $C_2(2)$ $\forall$ prime p

proof (for odd primes) (for $p=2$ there are more computations but the idea is similar)

Every quadratic form is equivalent to a diagonal form

$$f(X) = a_1X_1^2 + \dots + a_nX_n^2$$

we can assume that the coefficients a_i are divisible by at most the first power of p since if $a_i = p^{2k_i}\varepsilon_i$ or $a_i = p^{2k_i+1}\varepsilon_i$ $\Rightarrow$ we can make a change of variables $p^{k_i}x_i = y_i$

$\Rightarrow$ we can write $f = f_0(X) + pf_1(X)$

where $f_0(X) = \varepsilon_1X_1^2 + \dots + \varepsilon_r X_r^2$

$f_1(X) = \varepsilon_{r+1}X_{r+1}^2 + \dots + \varepsilon_n X_n^2$ with ε_i p-adic units

we can assume $r \geq n-r$ otherwise we can work with the form $pf = pf_0(X) + p^2f_1(X)$ that is equivalent to the form $f_1 + pf_0$

Since $n \geqslant 5 \Rightarrow$ by our normalization we have $r \geqslant 3$

$\Rightarrow f_0$ has a non-trivial zero $(y_1, \dots, y_r) \in \mathbb{Z}_p^r$ (By Chevalley's Theorem and Hensel's lemma)

$\Rightarrow (y_1, \dots, y_r, 0, \dots, 0)$ is a non-trivial zero of f $\square$