p-adic Zeros of Systems of Quadratic Forms

Roger Heath-Brown

Oxford University

The problem: Let K be a field, and let $r \in \mathbb{N}$. Define $\beta(r;K)$ as the largest integer n for which there exist quadratic forms $q^{(i)}(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ $(1 \le i \le r)$ having only the trivial common zero over K.

$\beta(1;\mathbb{R}) = \infty$ $(x_1^2 + \cdots + x_n^2$ has no non-trivial zero over $\mathbb{R}$, $\forall n)$

$\beta(1;\mathbb{C}) = 1$ $(x_1^2 = 0 \Rightarrow x_1 = 0)$

$\beta(r;\mathbb{C}) = r$ $\forall r \in \mathbb{N}$

Primarily interested in $K = \mathbb{Q}_p$:

$\beta(1;\mathbb{Q}_p) = 4$ (eg $p = 3$ $x_1^2 + x_2^2 + 3(x_3^2 + x_4^2)$ has no zero, but 5 variables suffice).

What can one say about $\beta(r;\mathbb{Q}_p)$?

Why should one care?

Local-to-Global principles. The circle method sometimes will provide a solution of $q^{(1)}(\underline{x}) = \cdots = q^{(r)}(\underline{x}) = 0$ over $\mathbb{Z}$, given that there are solutions locally.

(But note that i) we also need to handle solvability over $\mathbb{R}$; and ii) the circle method requires non-singular local solutions.)

Systems of quadratics are important – we can reduce general Diophantine equations to systems of quadratics.

A p-adic quartic form in n variables has a zero if $p \neq 2$, and n variables suffice for any system of 16 linear forms and 8 quadratic forms.

What might we expect?

Artin's Conjecture: A p-adic form of degree d in $>d^2$ variables has a non-trivial zero.

$$\Rightarrow \quad \beta(r;\mathbb{Q}_p) \le 4r$$

and if $q(x_1,\ldots,x_4)$ has only the trivial zero, the system $q_1 = q(x_1,\ldots,x_4)$, $q_2 = q(x_5,\ldots,x_8)$, $q_3 = q(x_9,\ldots,x_{12})$ .... has $4r$ variables, and only the trivial zero.

Hence $\beta(r;\mathbb{Q}_p) \geq 4r$.

Conjecture: $\beta(r;\mathbb{Q}_p) = 4r$.

However Artin's conjecture is known to be false.

None the less the above conjecture remains open.

Ax-Kochen (1965). Artin's Conjecture holds for $p \geq p(d)$.

$\Rightarrow \forall r \ \exists\, p(r)$ s.t. $\beta(r; \mathbb{Q}_p) = 4r \quad \forall p \geq p(r)$.

—

$r = 1$: $\beta(1; \mathbb{Q}_p) = 4$ (? 19^{th} century, Hasse 1924)

$r = 2$: $\beta(2; \mathbb{Q}_p) = 8$ (Demyanov, 1956)

$r = 3$: $\beta(3; \mathbb{Q}_p) = 12$ for $p \geq 11$

(Schuur, 1980 ; Birch & Lewis 1965)

—

Open Question : $\beta(3; \mathbb{Q}_p) = 12 \quad \forall p$?

—

1st line of attack:- Birch, Lewis & Murphy 1962, Birch & Lewis 1965, Schmidt 1980

WLOG $q^{(i)}(\underline{x}) \in \mathbb{Z}_p[\underline{x}]$. Reduce to $\mathbb{F}_p$,

$q^{(i)}(\underline{x}) \rightarrow Q^{(i)}(\underline{x}) \in \mathbb{F}_p[\underline{x}]$.

If the system $Q^{(1)}, \ldots, Q^{(r)}$ has a non-singular zero over $\mathbb{F}_p$, then $q^{(1)}, \ldots, q^{(r)}$ will have a non-singular zero over $\mathbb{Q}_p$, by Hensel's Lemma.

By the Chevalley-Warning Theorem there will be a non-trivial zero over $\mathbb{F}_p$ if $n > 2r$. So the key issue is non-singularity.

Not every system $Q^{(1)}, \ldots, Q^{(r)}$ has a smooth zero e.g if all the $Q^{(i)}$ vanish identically

We need a good model over $\mathbb{Z}_p$, with excess

We may make linear changes of variable on $\underline{x}$ without changing the problem ("Does $q^{(1)}, \ldots, q^{(r)}$ have a simultaneous zero")

Similarly we can make linear changes amongst the $q^{(i)}$.

Let $M^{(i)}$ be symmetric matrices$/\mathbb{Q}_p$ representing $q^{(i)}$

$$F(X_1, \ldots, X_r) := \mathrm{Det}(X_1 M^{(1)} + \cdots + X_r M^{(r)})$$

$$P(q^{(1)}, \ldots, q^{(r)}) := \mathrm{Res}\left(\frac{\partial F}{\partial X_1}, \frac{\partial F}{\partial X_2}, \ldots, \frac{\partial F}{\partial X_r}\right)$$

It suffices to consider systems with $P \neq 0$

Any such system has a "Minimal model", in which $q^{(i)}(\underline{x}) \in \mathbb{Z}_p[\underline{x}]$, and $|P(q^{(1)}, \ldots, q^{(r)})|_p$ is maximal.

Assume $n > 4r$

For a minimal model, $Q^{(1)}(0,0,x_3,x_4,\dots,x_n) \in \mathbb{F}_p(x_1 \dots x_n)$ cannot vanish identically;

Set $q^{(1)\prime} = p^{-1} q^{(1)}(px_1, px_2, x_3, x_4 \dots x_n)$ and

$q^{(i)\prime} = q^{(i)}(px_1, px_2, x_3 \dots x_n)$ for $2 \le i \le r$.

Then $|P(q^{(1)\prime}, q^{(2)\prime}, \dots q^{(r)\prime})|_p > |P(q^{(1)}, \dots, q^{(r)})|$ ※

Similarly $Q^{(1)}(0,0,0,0,x_5,x_6,\dots)$ and $Q^{(2)}(0,0,0,0,x_5,x_6\dots)$ cannot both vanish identically,

Or any j of the forms, with $x_1 = \dots = x_{2j} = 0$,

Even after making $SL_n(\mathbb{F}_p)$ transforms on the x_i, or $SL_r(\mathbb{F}_p)$ transforms among the $Q^{(i)}$

eg $r=1$, $p \neq 2$, Diagonalize $Q^{(1)}$ as

$a_1 x_1^2 + \dots + a_m x_m^2 + 0 . x_{m+1}^2 + \dots + 0 . x_n^2$, $a_1 a_2 \dots a_m \neq 0$.

Then $m \geq 3$. Chevalley - Warning gives $(x_1, x_2, x_3) \neq \underline{0}$ with $a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 = 0$, a non-singular zero.

$r=1$: easily cover $p=2$ too

$r=2$: Can show that $q^{(1)}, q^{(2)}$ minimal, $n \geq 9$ (i.e. $n > 4r$) $\Rightarrow$ $Q^{(1)}, Q^{(2)}$ has a non-singular zero$/\mathbb{F}_p$ $\Rightarrow$ $q^{(1)}, q^{(2)}$ has a common non-trivial zero. (Demyanov; Birch, Lewis & Murphy)

$r=3$: Similarly, if $p \geq 11$ (Schuur) — harder, many cases to consider.

<u>But</u> one cannot handle all primes this way.

$p=2$:

$$Q^{(1)} = x_1x_2 + x_3^2 + x_3x_4 + x_4^2$$

$$Q^{(2)} = x_5x_6 + x_7^2 + x_7x_8 + x_8^2$$

$$Q^{(3)} = x_1^2 + x_1x_2 + x_2^2 + x_5x_7 + x_6x_8 + x_7^2 + x_8^2$$

Satisfies the minimality condition

e.g. no linear combination vanishes when we set two variables to zero.

And : (over $\mathbb{F}_2$)

$Q^{(1)} = 0 \Rightarrow (x_1, \dots, x_4) = (0000)$ or $x_1^2 + x_1x_2 + x_2^2 = 1$

$Q^{(2)} = 0 \Rightarrow x_5x_7 + x_6x_8 + x_7^2 + x_8^2 = 0$

So $Q^{(1)} = Q^{(2)} = Q^{(3)} = 0 \Rightarrow x_1 = x_2 = x_3 = x_4 = 0$

$\Rightarrow \nabla Q^{(1)} = 0$ $\quad \therefore$ singular zero.

Conclusion: This line of attack cannot prove

$\beta(r; \mathbb{Q}_p) = 4r \quad \forall p$, if $r \geq 3$.

However one can show by this method:-

Theorem (H-B, 2010)

$\forall r$ one has $\beta(r; \mathbb{Q}_p) = 4r$ if $p \geq (2r)^r$.

Indeed if K is any finite extension of $\mathbb{Q}_p$ with residue field F, then $\beta(r; K) = 4r$ if $\# F \geq (2r)^r$.

Recall: Ax-Kochen - $\beta(r; \mathbb{Q}_p) = 4r$ for $p \geq p(r)$

One can specify $\rho(r)$ - a 7-fold exponential (!)

One can apply the Ax-Kochen method to show $\beta(r;K) = 4r$ if $\chi_F \geq \rho(r; [K:\mathbb{Q}_p])$

A condition on χ_F, not $\#F$.

Idea for proof of (H-B, 2010)

Give a lower bound for the total number of zeros of $Q^{(1)} = \dots = Q^{(r)} = 0 \,/ F$, and an upper bound for the number of singular zeros, $\Rightarrow \exists$ (lots of) non-singular zeros.

Show that "few" linear combinations

$$a_1 Q^{(1)} + \dots + a_r Q^{(r)} \qquad (a_i \in F)$$

have "small" rank, using minimality conditions.

Corollary to (H-B, 2010) by Leep, to appear

Let $L = \mathbb{Q}_p(T_1, \dots, T_k)$, then

$$\beta(1; L) = 2^{2+k} \qquad \forall p.$$

Indeed one also has $\beta(2; L) = 2^{3+k} \quad \forall p.$

No restriction on p !!

Idea: Let $q(x_1, \dots, x_n) \in L(x_1, \dots, x_n)$ be given

Let L^*/L be an extension of odd degree.

By a theorem of Springer, if q has a zero over L^* it has a zero over L.

Take $L^* = K(T_1, \dots, T_k)$, $K/\mathbb{Q}_p$ odd

To solve $q = 0$ over L^* it suffices to solve a system of R quadratics in N variables, all over K ("restriction of scalars")

$N > 4R$, N, R depend on q, but <u>not</u> on K.

We can solve this system (by HB, 2010) if the residue field of K has

$\# F \geqslant (2R)^R$ ~ depending only on q.

So choose the extension $K/\mathbb{Q}_p$ accordingly.

Springer's theorem makes the constraint on $\# F$ disappear

A second route to $\beta(r;\mathbb{Q}_p)$
providing estimates $\forall p$.

Induction on r : Leep 1984, ...

Work over $\mathbb{Q}_p$, not over $\mathbb{F}_p$.

—

Suppose we can find a $\mathbb{Q}_p$-linear space, L, projective dimension $= \beta(k:\mathbb{Q}_p)$, on which $q^{(1)},\dots,q^{(r-k)}$ all vanish; then the remaining forms $q^{(r-k+1)},\dots,q^{(r)}$ must vanish on L.

Define $\beta(r;\mathbb{Q}_p,m)$ as the largest integer n for which $\exists$ quadratic forms $q^{(1)}(x_1,\dots,x_n)$, $q^{(2)},\dots,q^{(r)}$ where there is no $\mathbb{Q}_p$-linear space of projective dimension m on which all the forms vanish.

$$\beta(r;\mathbb{Q}_p) \le \beta(r-k;\mathbb{Q}_p,\beta(k))$$

Suppose $\exists$ $(m-1)$-dimensional space, L, spanned by $\underline{e}_0, \ldots, \underline{e}_{m-1}$. To find $\underline{e}_m = \underline{e}$

Let $\mathbb{Q}_p^n = L \oplus L^*$ and require $\underline{e} \in L^*$,

($\therefore$ $\underline{e}_0, \ldots, \underline{e}_m$ will be independent)

$q^{(i)}(\underline{e}_j, \underline{e}) = 0 \quad (i \leq r,\ 0 \leq j < m)$ $\quad$ rm linear constraints

and $q^{(i)}(\underline{e}) = 0 \quad (1 \leq i \leq r)$

We can find $\underline{e}$ when $\dim L^* \geq rm + \beta(r; \mathbb{Q}_p)$

i.e. when $n > (r+1)m + \beta(r; \mathbb{Q}_p)$

$$\therefore \quad \beta(r; \mathbb{Q}_p, m) \leq (r+1)m + \beta(r; \mathbb{Q}_p)$$

So $\beta(r; \mathbb{Q}_p) \leq \beta(r-1; \mathbb{Q}_p, \beta(1))$

$$= \beta(r-1; \mathbb{Q}_p, 4)$$

$$\leq 4r + \beta(r-1; \mathbb{Q}_p)$$

Induction $(\beta(1; \mathbb{Q}_p) = 4,\ \beta(2; \mathbb{Q}_p) = 8)$

$$\Rightarrow \beta(r; \mathbb{Q}_p) \leq \begin{cases} 2r^2 & r \text{ even} \\ 2r^2+2 & r \text{ odd} \end{cases} \quad \text{(Martin 1997)}$$

$$\beta(r;\mathbb{Q}_p,m) \leq (r+1)m + \beta(r;\mathbb{Q}_p).$$

$r = 1$: $\beta(1;\mathbb{Q}_p,m) \leq 2m + 4$

Best possible

$r = 2$? $\beta(2;\mathbb{Q}_p,m) \leq 3m + 8.$

Improvement due to Dietmann, 2005 (α refined H-B, 2010)

Theorem (Amer, 1976) Let K be any field with $\chi_K \neq 2$. Then $\beta(2;K,m) \leq \beta(1;K(x),m)$, $\forall\, m \geq 0$.

[$m=0$; $\beta(2;K) \leq \beta(1;K(x))$, Brumer, 1978]

Generally $\beta(1;F,m) \leq 2m + \beta(1;F)$

So $\beta(1;K(x),m) \leq 2m + \beta(1;K(x))$

$\therefore$ $\beta(2;\mathbb{Q}_p,m) \leq 2m + \beta(1;\mathbb{Q}_p(x))$

Recall Leep (Corollary to H-B, 2010)

$2+k$

So $\beta(1;\mathbb{Q}_p(x)) = 8$

$$\beta(2;\mathbb{Q}_p, m) \leq 2m + 8$$

(Best Possible)

Question? $\beta(3;\mathbb{Q}_p, m) \leq 2m + O(1)$?

Previously: $\beta(r;\mathbb{Q}_p) \leq \beta(r-k;\mathbb{Q}_p, \beta(k))$

$$\therefore \quad \beta(r;\mathbb{Q}_p) \leq \beta(2;\mathbb{Q}_p, \beta(r-2))$$
$$\leq 2\beta(r-2;\mathbb{Q}_p)$$

$$\therefore \quad \beta(3;\mathbb{Q}_p) \leq 2\beta(1;\mathbb{Q}_p) + 8 = 8+8 = 16$$

(Martin - $\beta(3;\mathbb{Q}_p) \leq 20$)

$$\beta(4;\mathbb{Q}_p) \leq 2\beta(2;\mathbb{Q}_p) + 8 \leq 24$$

$$\beta(5;\mathbb{Q}_p) \leq 2\beta(3;\mathbb{Q}_p) + 8 \leq 40$$

$$\beta(6;\mathbb{Q}_p) \leq 2\beta(4;\mathbb{Q}_p) + 8 \leq 56$$

Leep's induction $\Rightarrow$

$$\beta(r;\mathbb{Q}_p) \leq \begin{cases} 2r^2-14, & r \text{ odd} \geq 7 \\ 2r^2-16, & r \text{ even} \geq 8 \end{cases}$$

Improves previous bound by 16.

—

$r=3$: $12 \leq \beta(3;\mathbb{Q}_p) \leq 16$

1) $K/\mathbb{Q}_p$ finite $\# F > (2r)^r$, Can solve r equations in $\geqslant 4r+1$ variables

2) Can solve $q(x_1, \dots, x_q) = 0$, over $K(X)$, if q is defined over $\mathbb{Q}_p(X)$ and $\# F \geq c_q$

3) Can solve $q(x_1, \dots, x_q) = 0$, over $\mathbb{Q}_p(X)$

4) $\exists$ linear space of solutions of $q(x_1, \dots, x_n) = 0$, all over $\mathbb{Q}_p(X)$

5) $\exists$ linear space of solutions of $q_1(x_1, \dots, x_n) = q_2(x_1, \dots, x_n) = 0$, over $\mathbb{Q}_p$

6) $\exists$ non-trivial zero of
$$q_1(x_1, \dots, x_{17}) = q_2(x_1, \dots, x_{17}) = q_3(x_1, \dots, x_{17}) = 0$$
over $\mathbb{Q}_p$