On solvability of diophantine equations in p-adic numbers

Yuri Nesterenko
Moscow State University

Arithmetic as Geometry: Parshin Fest
Moscow, Russia, November 26–29, 2012

$\mathbb{Q}$, $|\ |_p$, $|p|_p = p^{-1}$, $\mathbb{Q}_p$ — the completion of $\mathbb{Q}$.
p-adic numbers were first described by Kurt Hensel in 1897.

$\mathbb{Q},\ \ |\ \ |_p,\ |p|_p = p^{-1},\ \mathbb{Q}_p$ — the completion of $\mathbb{Q}$.
p-adic numbers were first described by Kurt Hensel in 1897.

- $$F_i(x_1, \dots, x_n) = 0, \qquad 1 \le i \le m,$$
  $$F_i \in \mathbb{Z}[x_1, \dots, x_n], \qquad \text{solubility in} \quad \mathbb{Q}_p.$$

Parameters: $p,\ n,\ d = \max_i \deg F_i,\ h = \max_i h(F_i),\ m.$

$\mathbb{Q}, \ \ | \ \ |_p, \ |p|_p = p^{-1}, \ \mathbb{Q}_p$ — the completion of $\mathbb{Q}$.
p-adic numbers were first described by Kurt Hensel in 1897.

$$\bullet \qquad F_i(x_1, \dots, x_n) = 0, \qquad 1 \le i \le m,$$
$$F_i \in \mathbb{Z}[x_1, \dots, x_n], \qquad \text{solubility in} \quad \mathbb{Q}_p.$$

Parameters: $p, \ n, \ d = \max_i \deg F_i, \ h = \max_i h(F_i), \ m$.

• **K. Hensel**: Let $F = F(x_1, \dots, x_n)$ be a homogeneous polynomial with coefficients in $\mathbb{Z}_p$. Let $\overline{a} \in \mathbb{Z}^n$ be a vector such that

$$F(\overline{a}) \equiv 0 \pmod{p}, \qquad \exists \ i \quad \frac{\partial F}{\partial x_i}(\overline{a}) \not\equiv 0 \pmod{p}.$$

Then the equation $F(\overline{x}) = 0$ has a nontrivial solution in $\mathbb{Q}_p$.

$p >> n, d$

- **C. Chevalley-E. Warning, 1936**: *If $n > d$, where d is the total degree of F, and the polynomial has no constant term, then the equation $F(x_1, \ldots, x_n) = 0$ has a nontrivial solution in $GF(p)$.*

$p >> n, d$

• **C. Chevalley-E. Warning, 1936**: *If $n > d$, where d is the total degree of F, and the polynomial has no constant term, then the equation $F(x_1, \ldots, x_n) = 0$ has a nontrivial solution in $GF(p)$.*

• The consequence of **A. Weil's** theorem about number of points on algebraic curves over finite fields,
S.Lang and A.Weil, L.B.Nisnevich, 1954:
Let $F = F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be an absolutely irreducible polynomial. Then $N(F, p)$ the number of solutions of

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

satisfies

$$|N(F, p) - p^{n-1}| < C(F) p^{n-3/2},$$

where the positive constant $C(F)$ depends only on the polynomial.

$n >> d$

- $d = 2$, **A. Meyer, 1884**: An indefinite quadratic form in five or more variables over the field of rational numbers nontrivially represents zero in $\mathbb{Q}$.

$n >> d$

- $d = 2$, **A. Meyer, 1884**: An indefinite quadratic form in five or more variables over the field of rational numbers nontrivially represents zero in $\mathbb{Q}$.

H. Hasse, 1923: Every quadratic form in five or more variables with coefficients in $\mathbb{Q}_p$ nontrivially represents zero in $\mathbb{Q}_p$ for all p.

$n >> d$

- $d = 2$, **A. Meyer, 1884**: An indefinite quadratic form in five or more variables over the field of rational numbers nontrivially represents zero in $\mathbb{Q}$.

H. Hasse, 1923: Every quadratic form in five or more variables with coefficients in $\mathbb{Q}_p$ nontrivially represents zero in $\mathbb{Q}_p$ for all p.

Example: $Q = x_1^2 + x_2^2 - p(x_3^2 + x_4^2)$, $p \equiv 3 \pmod 4$ does not represent zero in $\mathbb{Q}_p$.

$n >> d$

- $d = 2$, **A. Meyer, 1884**: An indefinite quadratic form in five or more variables over the field of rational numbers nontrivially represents zero in $\mathbb{Q}$.

H. Hasse, 1923: Every quadratic form in five or more variables with coefficients in $\mathbb{Q}_p$ nontrivially represents zero in $\mathbb{Q}_p$ for all p.

Example: $Q = x_1^2 + x_2^2 - p(x_3^2 + x_4^2)$, $p \equiv 3 \pmod 4$ does not represent zero in $\mathbb{Q}_p$.

- $d = 3$, **Demianov, 1951,($p \neq 3$), D.J. Lewis, 1952**: Every cubic homogeneous polynomial equation in $n \geq 10$ variables with coefficients in $\mathbb{Q}_p$ has a non-trivial zero in $\mathbb{Q}_p$.

- **H. Davenport, D.J. Lewis, 1963**: An equation

$$F = c_1 x_1^d + \ldots + c_n x_n^d = 0, \qquad n > d^2, \qquad c_j \in \mathbb{Q}_p,$$

has a non-trivial zero in $\mathbb{Q}_p$.

• **H. Davenport, D.J. Lewis, 1963**: An equation

$$F = c_1 x_1^d + \ldots + c_n x_n^d = 0, \qquad n > d^2, \qquad c_j \in \mathbb{Q}_p,$$

has a non-trivial zero in $\mathbb{Q}_p$.

Simple case ($p \nmid d$):

• By an obvious substitution of the form $x_i' = p^{\lambda_i} x_i$ we can ensure that $\nu_p(c_i) < d$.

• **H. Davenport, D.J. Lewis, 1963**: An equation

$$F = c_1 x_1^d + \ldots + c_n x_n^d = 0, \qquad n > d^2, \qquad c_j \in \mathbb{Q}_p,$$

has a non-trivial zero in $\mathbb{Q}_p$.

Simple case ($p \nmid d$):

• By an obvious substitution of the form $x_i' = p^{\lambda_i} x_i$ we can ensure that $\nu_p(c_i) < d$. Then $F = G_0 + pG_1 + \ldots + p^{d-1} G_{d-1}$, where G_k are diagonal forms of degree d with coefficients not divisible by p and with own set of variables.

• **H. Davenport, D.J. Lewis, 1963**: An equation

$$F = c_1 x_1^d + \ldots + c_n x_n^d = 0, \qquad n > d^2, \qquad c_j \in \mathbb{Q}_p,$$

has a non-trivial zero in $\mathbb{Q}_p$.

Simple case ($p \nmid d$):

• By an obvious substitution of the form $x_i' = p^{\lambda_i} x_i$ we can ensure that $\nu_p(c_i) < d$. Then $F = G_0 + pG_1 + \ldots + p^{d-1} G_{d-1}$, where G_k are diagonal forms of degree d with coefficients not divisible by p and with own set of variables.

• If G_0 depends on more than d variables, one can apply Chevalley's lemma to G_0 and Hensel's lemma to the form F.

• **H. Davenport, D.J. Lewis, 1963**: An equation

$$F = c_1 x_1^d + \ldots + c_n x_n^d = 0, \qquad n > d^2, \qquad c_j \in \mathbb{Q}_p,$$

has a non-trivial zero in $\mathbb{Q}_p$.

Simple case ($p \nmid d$):

• By an obvious substitution of the form $x_i' = p^{\lambda_i} x_i$ we can ensure that $\nu_p(c_i) < d$. Then $F = G_0 + pG_1 + \ldots + p^{d-1} G_{d-1}$, where G_k are diagonal forms of degree d with coefficients not divisible by p and with own set of variables.

• If G_0 depends on more than d variables, one can apply Chevalley's lemma to G_0 and Hensel's lemma to the form F.

• In general case one can effect a cyclic permutation of $G_0, \ldots, G_{d-1}$ by putting $x_i = p\tilde{x}_i$ for all the variables in G_0 and then dividing throughout by p. Since the total number of variables is $n > d^2$, we can choose a cyclic permutation which will ensure that the number of terms in G_0 became larger then d.

$n >> d$

• **R. Brauer, 1945**: There exists a positive function $\psi(d)$ such that any system

$$F_i(x_1, \ldots, x_n) = 0, \qquad F_i \in \mathbb{Z}[x_1, \ldots, x_n], \qquad 1 \le i \le m,$$

with $n > \psi(d)$ is soluble in $\mathbb{Q}_p$.

$n >> d$

• **R. Brauer, 1945**: There exists a positive function $\psi(d)$ such that any system

$$F_i(x_1, \ldots, x_n) = 0, \qquad F_i \in \mathbb{Z}[x_1, \ldots, x_n], \qquad 1 \le i \le m,$$

with $n > \psi(d)$ is soluble in $\mathbb{Q}_p$.

Best upper bounds for $\psi(d)$ are

• **W. Schmidt, 1984**: $\log \psi(d) = o(2^d d!)$

• **T. Wooley, 1998**: $\log \psi(d) \le 2^d \log d$.

$n >> d$

• **R. Brauer, 1945**: There exists a positive function $\psi(d)$ such that any system

$$F_i(x_1, \ldots, x_n) = 0, \qquad F_i \in \mathbb{Z}[x_1, \ldots, x_n], \qquad 1 \leq i \leq m,$$

with $n > \psi(d)$ is soluble in $\mathbb{Q}_p$.

Best upper bounds for $\psi(d)$ are

• **W. Schmidt, 1984**: $\log \psi(d) = o(2^d d!)$

• **T. Wooley, 1998**: $\log \psi(d) \leq 2^d \log d$.

• **J. Ax, S. Kochen, 1965**: For every d there is a number $p(d)$ such that every form with $n > d^2$ variables and $p > p(d)$ has a nontrivial p-adic zero.

$n >> d$

- **Conjecture (attributed to E. Artin, 1933-1935)**: A form $F(\overline{x}) \in \mathbb{Q}_p[x_1, \ldots, x_n]$ of degree d should have a non-trivial p-adic zero as soon as $n > d^2$, i.e. $\psi(d) = d^2$ independently on p.

$n >> d$

- **Conjecture (attributed to E. Artin, 1933-1935)**: A form $F(\overline{x}) \in \mathbb{Q}_p[x_1, \ldots, x_n]$ of degree d should have a non-trivial p-adic zero as soon as $n > d^2$, i.e. $\psi(d) = d^2$ independently on p.

- **Counter-examples**:

G. Terjanian, 1966: $p = 2, d = 4, n = 18$.

$n >> d$

- **Conjecture (attributed to E. Artin, 1933-1935)**: A form $F(\overline{x}) \in \mathbb{Q}_p[x_1, \ldots, x_n]$ of degree d should have a non-trivial p-adic zero as soon as $n > d^2$, i.e. $\psi(d) = d^2$ independently on p.

- **Counter-examples**:

G. Terjanian, 1966: $p = 2, d = 4, n = 18$.
J. Browkin, 1966: For every prime p we have $\psi(d) \geq d^{3-\varepsilon}$. For any $\varepsilon > 0$ there exist infinitely many forms F of degree d such that $n > d^{3-\varepsilon}$ and F has only trivial zeros in $\mathbb{Q}_p$.

$n >> d$

• **Conjecture (attributed to E. Artin, 1933-1935)**: A form $F(\overline{x}) \in \mathbb{Q}_p[x_1, \ldots, x_n]$ of degree d should have a non-trivial p-adic zero as soon as $n > d^2$, i.e. $\psi(d) = d^2$ independently on p.

• **Counter-examples**:
G. Terjanian, 1966: $p = 2, d = 4, n = 18$.
J. Browkin, 1966: For every prime p we have $\psi(d) \geq d^{3-\varepsilon}$. For any $\varepsilon > 0$ there exist infinitely many forms F of degree d such that $n > d^{3-\varepsilon}$ and F has only trivial zeros in $\mathbb{Q}_p$.
G. Arhipov, A. Karacuba, 1981:

$$\psi(d) > p^{\frac{d}{\log^2 d \log\log^3 d}}$$

for every p.
Improvements: G. Arhipov, A. Karacuba, 1982 (the best); Lewis and Montgomery (1983), D. Brownawell (1984).

Main steps of the proof. p is odd.

Main steps of the proof. p is odd.

Construction of a sequence of forms F_r, only trivially representing zero in $\mathbb{Q}_p$ and such that

$$n_{r+1} > p^{n_r}, \qquad d_{r+1} < c d_r n_r, \qquad (c = 6p^2),$$

where n_r is the number of variables in F_r, $d_r = \deg F_r$.

Main steps of the proof. p is odd.

Construction of a sequence of forms F_r, only trivially representing zero in $\mathbb{Q}_p$ and such that

$$n_{r+1} > p^{n_r}, \qquad d_{r+1} < c d_r n_r, \qquad (c = 6p^2),$$

where n_r is the number of variables in F_r, $d_r = \deg F_r$.

• Denote $m = n_r$. Let a be a natural number, $g(x) \in \mathbb{Z}[x]$, $\deg g(x) < m$,

$$|g(u_j)| < p^{-(p-1)a}, \qquad j = 1, \ldots, m,$$

where

$$u_j = (1+p)^{r_j}, \qquad a \leq r_1 < \ldots < r_m < \frac{p+1}{2} a = b.$$

Then $|g(1)| < p^{-m}$. (Interpolation)

- *If integers $x_1, \ldots, x_n$ satisfy*

$$\sum_{j=1}^{n} x_j^{(p-1)r_i} \equiv 0 \pmod{p^{(p-1)a}}, \quad 1 \le i \le m, \quad \textit{then} \quad n > p^m.$$

$$p \nmid x_1 \cdots x_n \quad \Rightarrow \quad x_j^{p-1} \equiv (1+p)^{c_j} \pmod{p^{(p-1)a}}.$$

• *If integers* $x_1, \ldots, x_n$ *satisfy*

$$\sum_{j=1}^{n} x_j^{(p-1)r_i} \equiv 0 \pmod{p^{(p-1)a}}, \quad 1 \le i \le m, \quad \textit{then} \quad n > p^m.$$

$$p \nmid x_1 \cdots x_n \quad \Rightarrow \quad x_j^{p-1} \equiv (1+p)^{c_j} \pmod{p^{(p-1)a}}.$$

$$f(t) = t^{c_1} + \ldots + t^{c_n}, \quad \varphi(t) = (t-u_1)\cdots(t-u_m), \quad u_i = (1+p)^{r_i}$$

$$g(t) = f(t) - \varphi(t)h(t), \qquad \deg g(t) < m,$$

- *If integers* $x_1, \ldots, x_n$ *satisfy*

$$\sum_{j=1}^{n} x_j^{(p-1)r_i} \equiv 0 \pmod{p^{(p-1)a}}, \quad 1 \le i \le m, \quad \textit{then} \quad n > p^m.$$

$$p \nmid x_1 \cdots x_n \quad \Rightarrow \quad x_j^{p-1} \equiv (1+p)^{c_j} \pmod{p^{(p-1)a}}.$$

$$f(t) = t^{c_1} + \ldots + t^{c_n}, \quad \varphi(t) = (t-u_1)\cdots(t-u_m), \quad u_i = (1+p)^{r_i}$$

$$g(t) = f(t) - \varphi(t)h(t), \qquad \deg g(t) < m,$$

$$f(u_i) = \sum_{j=1}^{n}(1+p)^{r_i c_j} \equiv \sum_{j=1}^{n} x_j^{(p-1)r_i} \equiv 0 \pmod{p^{(p-1)a}}$$

$$|n| = |f(1)| \le \max(|g(1)|,\ |\varphi(1)|) \le p^{-m}.$$

$n >> d$

- $k = 1, \ldots, m$

$$H_k(\overline{x}) = \sum_{j=1}^{n} x_j^{(p-1)(a+k)} \cdot \sum_{j=1}^{n} x_j^{(p-1)(b-k)}, \qquad \deg H_k = (p-1)(a+b)$$

$$a \geq \frac{4m+2}{p-1} \Rightarrow H_k \text{ have no common factors.}$$

$$F_{r+1}(x_1, \ldots, x_n) = F_r(H_1, \ldots, H_m),$$
$$n_{r+1} = n > p^{n_r}, \qquad d_{r+1} = d_r(p-1)(a+b).$$

$$a \sim \frac{4m+2}{p-1} \quad \Rightarrow d_{r+1} \sim (2p+6)d_r n_r.$$

$n >> d$

Corrected Artin's conjecture (Arhipov, Karacuba, 1981): A form $F(\overline{x}) \in \mathbb{Q}_p[x_1, \ldots, x_n]$ of degree d should have a non-trivial p-adic zero as soon as $n > d^2$ and $p > d$.

$n >> d$

Corrected Artin's conjecture (Arhipov, Karacuba, 1981): A form $F(\overline{x}) \in \mathbb{Q}_p[x_1, \ldots, x_n]$ of degree d should have a non-trivial p-adic zero as soon as $n > d^2$ and $p > d$.

- **J. Ax, S. Kochen, 1965**: For every d there is a number $p(d)$ such that every form with $n > d^2$ variables and $p > p(d)$ has a nontrivial p-adic zero.

Algorithms

• **Birch, Swinnerton-Dyer, 1962,** computed (with computer) the rank of the Mordell group for many elliptic curves. In these computations they needed to decide if a given elliptic curve contains a p-adic point.

Algorithms

• **Birch, Swinnerton-Dyer, 1962,** computed (with computer) the rank of the Mordell group for many elliptic curves. In these computations they needed to decide if a given elliptic curve contains a p-adic point. An algorithm based on Hensel's lemma was used:

For any polynomial $f(x) \in \mathbb{Z}[x]$ and integer $a \in \mathbb{Z}$ such that

$$|f(a)|_p < |f'(a)|_p^2$$

there exists a p-adic zero α of $f(x)$ such that $|\alpha - a|_p < 1$.

Algorithms

• **Birch, Swinnerton-Dyer, 1962,** computed (with computer) the rank of the Mordell group for many elliptic curves. In these computations they needed to decide if a given elliptic curve contains a p-adic point. An algorithm based on Hensel's lemma was used:

For any polynomial $f(x) \in \mathbb{Z}[x]$ and integer $a \in \mathbb{Z}$ such that

$$|f(a)|_p < |f'(a)|_p^2$$

there exists a p-adic zero α of $f(x)$ such that $|\alpha - a|_p < 1$.

The set of integer a that should be checked is finite since $|f(a)|_p$ and $|f'(a)|_p$ can not be small simultaneously.

Algorithms

- **B.J. Birch, K. McCann, 1966:** *Let be* $F \in \mathbb{Z}[x_1, \ldots, x_n]$*. One can compute an integer* $D_n(F)$ *with following property. Suppose that* $|F(\overline{a})|_p < |D_n(F)|_p$ *for some* $\overline{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$*, then there is a vector* $\overline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_p^n$ *such that* $F(\overline{\alpha}) = 0$*,* $|\overline{\alpha} - \overline{a}|_p < 1$*. Moreover*

$$D_n(F) = O(e^{cd^{4^n n!}(d+h(F))}).$$

Algorithms

• **B.J. Birch, K. McCann, 1966:** *Let be* $F \in \mathbb{Z}[x_1, \dots, x_n]$*. One can compute an integer* $D_n(F)$ *with following property. Suppose that* $|F(\overline{a})|_p < |D_n(F)|_p$ *for some* $\overline{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$*, then there is a vector* $\overline{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_p^n$ *such that* $F(\overline{\alpha}) = 0$*,* $|\overline{\alpha} - \overline{a}|_p < 1$*. Moreover*

$$D_n(F) = O(e^{cd^{4^n n!}(d+h(F))}).$$

Examples:

1. $n = 1$. Let be $F(x) \in \mathbb{Z}[x]$ an irreducible polynomial, $|F(a)|_p < |R|_p^2$ then there exists $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$ and $|\alpha - a|_p < 1$. $R = Res(F, F')$

2. $n = 2$. $\qquad F(x, y) = 0$.

$$g_1(x) = Res_y(F(x,y), \frac{\partial F}{\partial y}), \qquad g_2(y) = Res_x(F(x,y), \frac{\partial F}{\partial x})$$

$$|F(a_1, a_2)|_p < |g_1(a_1)|_p^2 \quad \Rightarrow \quad \exists\ \alpha_2 \in \mathbb{Z}_p, \quad F(a_1, \alpha_2) = 0$$

$$|F(a_1, a_2)|_p < |g_2(a_2)|_p^2 \quad \Rightarrow \quad \exists\ \alpha_1 \in \mathbb{Z}_p, \quad F(\alpha_1, a_2) = 0$$

2. $n = 2$. $\qquad F(x, y) = 0$.

$$g_1(x) = Res_y(F(x,y), \frac{\partial F}{\partial y}), \qquad g_2(y) = Res_x(F(x,y), \frac{\partial F}{\partial x})$$

$$|F(a_1, a_2)|_p < |g_1(a_1)|_p^2 \quad \Rightarrow \quad \exists\ \alpha_2 \in \mathbb{Z}_p, \quad F(a_1, \alpha_2) = 0$$

$$|F(a_1, a_2)|_p < |g_2(a_2)|_p^2 \quad \Rightarrow \quad \exists\ \alpha_1 \in \mathbb{Z}_p, \quad F(\alpha_1, a_2) = 0$$

In case

$$|g_1(a_1)|_p^2 \leq |F(a_1, a_2)|_p, \quad |g_2(a_2)|_p^2 \leq |F(a_1, a_2)|_p$$
$$\Rightarrow R = Res(F(x,y), g_1(x), g_2(y)).$$

Some special cases if $g_1 \equiv 0$ or $g_2 \equiv 0$, or $R \equiv 0$.

- **A. Chistov, M. Karpinski, 1997,** : In the case of systems

$$0 < D_n(F) < 2^{d^{2^{n(1+o(1))}}} h(F)$$

- **A. Chistov, M. Karpinski, 1997,** : In the case of systems

$$0 < D_n(F) < 2^{d^{2^{n(1+o(1))}}h(F)}$$

- **Hensel :**

$$|F(a)|_p < |F'(a)|_p^2 \quad \Rightarrow \quad \exists \alpha \in \mathbb{Z}_p, \quad F(\alpha) = 0, \quad |\alpha - a|_p < 1$$

If $F(x)$ be an irreducible polynomial then $|F(x)|_p$ and $|F'(x)|_p$ can not be small simultaneously at any point.
With this idea one can prove

$$|F(a)|_p < e^{-8d(d+h)} \quad \Rightarrow \quad \exists\ \alpha \in \mathbb{Z}_p,\ F(\alpha) = 0,\ |\alpha - a| < 1.$$

Theorem 1. Let $\overline{a} = (a_0, \ldots, a_m) \in \mathbb{Z}^{m+1}$ be a primitive vector $F_i(x_0, \ldots, x_m)$, $i = 1, \ldots, n$, be homogeneous polynomials, $I = (F_1, \ldots, F_n) \subset \mathbb{Q}[x_0, \ldots, x_m]$, $\dim I = r - 1$. If

$$\ln |F_i(\overline{a})|_p \leq -c_1 \cdot d^{\,2^r(m-r+1)-1}(d + h), \qquad i = 1, \ldots, n,$$

where d, h are real numbers such that $\deg F_i \leq d$, $h(F_i) \leq h$, and c_1 is a positive constant depending only on m and r, then there exists a vector $\overline{\alpha} \in \mathbb{Z}_p^{m+1}$ such that

$$F_i(\overline{\alpha}) = 0 \qquad i = 1, \ldots, n, \qquad \text{and} \qquad |\overline{\alpha} - \overline{a}|_p < 1.$$

Corollary

Let $\overline{a} = (a_0, \ldots, a_m) \in \mathbb{Z}^{m+1}$ *be a primitive vector,* $F(x_0, \ldots, x_m)$ *be a homogeneous polynomial. If*

$$\ln |F(\overline{a})| \leq -c_1 \cdot d^{\,2^m - 1}(d + h),$$

where d, h *are real numbers such that*

$$\deg F \leq d, \qquad h(F) \leq h,$$

and c_1 *is a positive constant depending only on* m*, then there exists a vector* $\overline{\alpha} \in \mathbb{Z}_p^{m+1}$ *such that*

$$F(\overline{\alpha}) = 0 \qquad \textit{and} \qquad |\overline{\alpha} - \overline{a}|_p < 1.$$

$I \subset \mathbb{Q}[\overline{x}] = \mathbb{Q}[x_0, \ldots, x_m]$, homogeneous ideal, associated prime $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ ideals, unmixed ideals: $\dim I = \dim \mathfrak{p}_j,\ 1 \leq j \leq s$. uniqueness.

$$\dim I,\ \deg I,\ h(I), |I(\overline{\alpha})|, \qquad \overline{\alpha} \in \mathbb{Q}_p^{m+1}.$$

$I \subset \mathbb{Q}[\overline{x}] = \mathbb{Q}[x_0, \ldots, x_m]$, homogeneous ideal, associated prime $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ ideals, unmixed ideals: $\dim I = \dim \mathfrak{p}_j,\ 1 \leq j \leq s$. uniqueness.

$$\dim I,\ \deg I,\ h(I), |I(\overline{\alpha})|, \qquad \overline{\alpha} \in \mathbb{Q}_p^{m+1}.$$

Theorem 2. Let $I \subset \mathbb{Q}[x_0, \ldots, x_m]$ be homogeneous unmixed ideal, $\dim I = r - 1 \geq 0$ and $\overline{a} = (a_0, \ldots, a_m) \in \mathbb{Z}^{m+1}$ be such integer vector that

$$\ln |I(\overline{a})|_p \leq -c^{2r} \cdot (\deg I)^{2^r - 1}(h(I) + \deg I),$$

where $c = c(m) > 0$ is a sufficiently large constant depending only on m. Then there exists a p-adic vector $\overline{\alpha} \in \mathbb{Z}_p^{m+1}$ that is a zero of I and $|\overline{\alpha} - \overline{a}|_p < 1$.

Theorem 2 $\Rightarrow$ Theorem 1.
Theorem 2 is proved by induction on $\dim I$. Assume that

$$\ln |I(\bar{a})|_p \leq -c^{4r} \cdot (\deg I)^{2^r-1}(h(I) + \deg I), \qquad (1)$$

where $c = c(m) > 0$ be a sufficiently large constant, $\dim I = r - 1$.

- Among $\mathfrak{p}_j$ there exists a prime $\mathfrak{p} \subset \mathbb{Q}[x_0, \dots, x_m]$, such that

$$\ln |\mathfrak{p}(\bar{a})|_p \leq -c^{4r-1} \cdot (\deg \mathfrak{p})^{2^r-1}(h(\mathfrak{p}) + \deg \mathfrak{p}). \qquad (2)$$

Let I be homogeneous unmixed ideal of the ring $\mathbb{Q}[\overline{x}]$, $\dim I \geq 0$. Let $I = I_1 \cap \ldots \cap I_s$ be irreducible primary decomposition, $\mathfrak{p}_j = \sqrt{I_j}$ be radicals and k_j be multiplicities of I_j. Let $\overline{\omega} \in \mathbb{C}_p{}^{m+1}, \overline{\omega} \neq 0$. Then

1) $\sum_{j=1}^{s} k_j \deg \mathfrak{p}_j = \deg I$;

2) $\sum_{j=1}^{s} k_j h(\mathfrak{p}_j) \leq h(I) + m^2 \deg I$;

3) $\sum_{j=1}^{s} k_j \log \mid \mathfrak{p}_j(\overline{\omega}) \mid_p = \log \mid I(\overline{\omega}) \mid_p$.

- There are polynomials $Q_1, \dots, Q_t \in \mathfrak{p}$,

$$\deg Q_j \le r \deg \mathfrak{p}, \qquad h(Q_j) \le h(\mathfrak{p}) + m^2 \deg \mathfrak{p}. \tag{3}$$

Projective varieties of $\mathfrak{p}$ and $\theta(\mathfrak{p}) = (Q_1, \dots, Q_t)$ coincide. The ideal $\theta(\mathfrak{p})$ has unique isolated primary component, it equals to $\mathfrak{p}$.

• There are polynomials $Q_1, \dots, Q_t \in \mathfrak{p}$,

$$\deg Q_j \le r \deg \mathfrak{p}, \qquad h(Q_j) \le h(\mathfrak{p}) + m^2 \deg \mathfrak{p}. \tag{3}$$

Projective varieties of $\mathfrak{p}$ and $\theta(\mathfrak{p}) = (Q_1, \dots, Q_t)$ coincide. The ideal $\theta(\mathfrak{p})$ has unique isolated primary component, it equals to $\mathfrak{p}$.

• Rank of the matrix

$$\left(\frac{\partial Q_i}{\partial x_j}\right)_{1 \le i \le t,\ 0 \le j \le m}, \tag{4}$$

modulo $\mathfrak{p}$ equals $m - r + 1$.

• There are polynomials $Q_1, \dots, Q_t \in \mathfrak{p}$,

$$\deg Q_j \le r \deg \mathfrak{p}, \qquad h(Q_j) \le h(\mathfrak{p}) + m^2 \deg \mathfrak{p}. \tag{3}$$

Projective varieties of $\mathfrak{p}$ and $\theta(\mathfrak{p}) = (Q_1, \dots, Q_t)$ coincide. The ideal $\theta(\mathfrak{p})$ has unique isolated primary component, it equals to $\mathfrak{p}$.

• Rank of the matrix

$$\left(\frac{\partial Q_i}{\partial x_j}\right)_{1 \le i \le t,\ 0 \le j \le m}, \tag{4}$$

modulo $\mathfrak{p}$ equals $m - r + 1$.

$\Delta(\overline{x})$ is a minor of the size $m - r + 1$ that does not belong to $\mathfrak{p}$.

In case

$$\ln|\Delta(\bar{a})| < -c^{4r-2} \cdot (\deg \mathfrak{p})^{2^r-1}(h(\mathfrak{p}) + \deg \mathfrak{p})$$

one can construct an unmixed ideal $J \subset \mathbb{Q}[x_0, \dots, x_m]$, $\dim J = r - 2$ such that

$$\deg J \leq m^2 \deg^2 \mathfrak{p}$$

$$h(J) \leq 7m^4 \deg \mathfrak{p}(h(\mathfrak{p}) + \deg \mathfrak{p}).$$

$$\ln|J(\bar{a})| \leq -c^{4r-3} \cdot (\deg \mathfrak{p})^{2^r-1}(h(\mathfrak{p}) + \deg \mathfrak{p}) \leq$$
$$\leq -c^{4r-4} \cdot (\deg J)^{2^{r-1}-1}(h(J) + \deg J).$$

and $V(J) \subset V(\mathfrak{p})$.
Induction assumption is applied to J.

- In case

$$\ln|\Delta(\overline{a})| \geq -c^{4r-2} \cdot (\deg \mathfrak{p})^{2^r-1}(h(\mathfrak{p}) + \deg \mathfrak{p}).$$

one can use the Hensel lemma and to prove the existence of p-adic zero for $\mathfrak{p}$.

• In case

$$\ln|\Delta(\bar{a})| \geq -c^{4r-2} \cdot (\deg \mathfrak{p})^{2^r-1}(h(\mathfrak{p}) + \deg \mathfrak{p}).$$

one can use the Hensel lemma and to prove the existence of p-adic zero for $\mathfrak{p}$.
Conjecture: Right hand side of

$$\ln|F_i(\bar{a})|_p \leq -c_1 \cdot d^{2^m-1}(d+h), \qquad i = 1, \ldots, n,$$

should be improved to

$$-c_1 \cdot d^{m}(d+h)$$

.