Some estimates for diagonal equations over $p$-adic fields

by

M. M. Dodson (Heslington, York)

Let $K_p$ be a $p$-adic field with ring of integers $\mathcal{O}$ and prime ideal $p = (a_p)$, where $\pi$ is an algebraic integer. Let the rational prime above $p$ be $p$ and the ramification index be $e$ so that $p^e = (\pi^e) = (p)$. Let the residue class field $k = \mathcal{O}/p$ have $p^e$ elements, so that $\mathcal{N}p = p^{e-1}$. Let the degree $[K_p: \mathcal{O}_p]$ of $K_p$ over $\mathcal{O}_p$, the rational $p$-adic field, be $n$, so that $n = e$. Finally let $p^e$ exactly divide $d$ and denote by $m_0$ the highest common factor $(d, p^e-1)$ of $d$ and $p^e-1$.

Denote by $G(d)$ the least $s$ for which the equation

$$a_1^s + \ldots + a_d^s = 0,$$

where $a_1, \ldots, a_d$ are arbitrary non-zero $p$-adic integers and $d$ a positive integer, has a non-trivial solution.

It was shown by Brauer ([4], Theorem C) that if $G(d)$ depends only on $d$, then there exists a number $I(d)$ also depending only on $d$, such that every general form of degree $d$ in at least $I(d)$ variables over a $p$-adic field represents zero non-trivially, although the number of variables required to effect the reduction to the diagonal case is very large. A decade earlier Artin had conjectured that $I(d) = d^2 + 1$ but in 1966 Terjanian [20] produced a form of degree $d$ in 18 variables which did not represent zero non-trivially in $\mathcal{O}_p$. Subsequently other authors disproved the conjecture for every $p$-adic field $\mathcal{O}_p$. For example Browkin [5] showed that there exist forms of degree $d$ in $n$ variables over $\mathcal{O}_p$ which have no non-trivial zeros and with $\log p$ arbitrarily close to 3. Terjanian [21] extended this result to finite extensions of $\mathcal{O}_p$ and so in particular to $K_p$. Nonetheless, Artin's conjecture holds for all but a finite number of primes $p$ in $\mathcal{N}$ since Ax and Kochen [3] have proved that the conjecture holds when the order of the residue class field exceeds a bound depending only on $d$. Their methods, which are model-theoretic in nature, are not effective for determining this bound, although Cohen [7] has shown how a bound can be obtained in principle.
The number $G(d)$ was investigated by Peck [18] who showed that
\[ G(d) \leq 4d^{2n+1} + 1, \]
an estimate which evidently depends very much on the degree $n$. Subsequently Birch [2] eliminated at the cost of introducing an "inordinately large number of variables" the dependence on $n$, the degree of the field, and proved that
\[ G(d) \leq (2n^2 + 3)d^2 + 1. \]
In view of Ax and Kochen's result Birch's estimate appears to be far from best possible though the possibility when $p$ is ramified of $G(d)$ being very large cannot be excluded. There are much better estimates available for $G(d)$ in special cases. Siegel [17] proved that $G(2) = 5$ and Lewis [15] that $G(3) = 7$. More generally Gray [13] showed that when $d$ is an odd prime
\[ G(d) \leq (d-1)d + 1. \]
Chevalley [6] proved Artin's conjecture for finite fields and it follows from this and Hensel's lemma that if the rational prime $p$ does not divide $d$, then
\[ G(d) \leq d^3 + 1. \]
In the $p$-adic case, where $K_p = Q_p$, Davenport and Lewis [8] showed that $G(d) \leq d^3 + 1$ and that there is equality whenever $d + 1$ is prime. When $d + 1$ is composite
\[ G(d) \leq (1 + 2(1 + \sqrt{1 + 4d}))d + 1, \]
where there is equality when $d = p(p-1)$ for some odd prime $p$ ([9], [3]). If $p-1$ does not divide the exponent $d$, the estimate for $G(d)$ can be much reduced [11] and for sufficiently large $d$,
\[ G(d) < d^{2n+1}. \]
When $d$ is odd, $G(d)$ is much smaller and Tietzvärinen [29] has obtained the best possible estimate
\[ G(d) < (1 + \varepsilon)\log_2 d \cdot d \]
for sufficiently large odd $d$.

The purpose of this note is to show that in the $p$-adic case
\[ G(d) \leq 16n^2(\log d)^2d^2, \]
where $n = [K_p : Q]$. Although it depends on $n$ and hence on the ramification index $e$ and so, in view of Birch's uniform estimate, is of limited interest the above estimate is simple to prove and represents a big improvement on Peck's original estimate. In addition, when $p$ is unramified the estimate is not far from best possible and indeed can be quite effective when $d$ has the appropriate arithmetic character.

The proof makes use of a generalization due to Erdős and Rado [12] of a box argument, which is purely combinatorial, and which permits the coefficients in (1) to be taken to be equal at a small (but non-uniform) cost. This idea has already been used in the $p$-adic case to get better estimates for $G(d)$ when $p-1$ does not divide the exponent $d$ ([9], §3.3; [11]) and the arguments in the algebraic case are similar.

In their work on Waring's problem in algebraic number fields, Körner [14], Stemann [18] and Tatsuzawa [19] showed that every element in the ring $\mathcal{J}_K$ generated by $d$th powers of integers in $K$ can be represented as a sum of $4d$ $d$th powers of integers. As in the rational case, Waring's problem and diagonal equations over $p$-adic fields have some similar features but the methods employed by Körner, Stemann and Tatsuzawa do not appear to extend to diagonal equations.

It has been assumed tacitly that $d > 1$ and since $G(2)$ and $G(3)$ have been determined, $d$ will be taken to be greater than 3 throughout. Also, in view of (2), it will be assumed that unless otherwise stated, $p$ divides $d$, i.e. that $\tau > 0$, so that $p \leq d$, and for each $d$, there are only a finite number of primes $p$ in $K$ under consideration.

By absorbing $d$th powers of $\pi$ into the variables and by multiplying by the appropriate power of $\pi$ where necessary, it follows from a box argument that the number of coefficients in the form on the left-hand side of (1) which are prime to $\pi$ can be taken to be at least $s(d)$. For simplicity we shall assume that the coefficients $a_1, \ldots, a_s$ are prime to $\pi$ and recover the general case by taking $d$ times as many variables. More precisely, we define $H(d)$ to be the least $s$ such that the equation (1), where $a_1, \ldots, a_s$ are prime to $\pi$, has a non-trivial solution, so that
\[ G(d) \leq dH(d). \]

As is well known, Hensel's lemma implies that the non-trivial solubility of equation (1) follows from the congruence
\[ a_1d_1^d + \ldots + a_sd_s^d = 0 \pmod{\pi^n}, \tag{3} \]
where $p^{n-1}$ exactly divides $2d$ and where $a_1, \ldots, a_s$ are prime to $\pi$, having a primitive solution (i.e. a solution with not all the variables $x_1, \ldots, x_s$ divisible by $\pi$). Consider the \( \binom{s}{r} \) sets of \( a_i, \ldots, a_r \) of $r$ coefficients where \( i_1, \ldots, i_r \) are chosen from $1, \ldots, s$. The sets of suffices are of course distinct though not generally disjoint. At least
\[ (\mathcal{N}^{\pi^n})^{-1}\binom{s}{r} = p^{-\text{vol}(\mathcal{S}_r)} \]
have the same sum \((\text{mod } p^m)\) or equivalently \((\text{mod } \pi^m)\). Erdős and Rado [12] proved that if

\[
2^{-m} \left( \frac{r}{v(r-1)} \right) > \frac{1}{2} \left( \frac{r-1}{r} \right)^{v(r-1)} \cdot \ldots \cdot \frac{r-1}{r} \cdot \ldots \cdot \frac{r-1}{r} \cdot \ldots \cdot \frac{r-1}{r}
\]

then there are at least \(v\) sets of the coefficients whose sums are all congruent \((\text{mod } \pi^m)\) and which are such that the common part of any two of the sets is the same. The inequality (4) is satisfied if

\[
s - r + 1 > 2^{m} \cdot \left( \frac{r}{v} \right)^{2^m - 1}
\]

and so is satisfied if

\[
s - r + 1 > 2^{m} \cdot \left( \frac{r}{v} \right)^{2^m - 1}
\]

Put

\[
r = \left[ \frac{\log p}{\log d} \right] + 2,
\]

where \([x]\) denotes the integer part of the real number \(x\), so that

\[
(2p^{m}v)^{1/2} < 4.
\]

Then (4) is satisfied if \(s > r^2 + v - 1\). Hence if \(s\) satisfies this last inequality there exist \(v\) sets

\[
a_{i_1}, \ldots, a_{i_v}; \quad a_{j_1}, \ldots, a_{j_v}; \quad \ldots; \quad a_{m_1}, \ldots, a_{m_v},
\]

of \(r\) coefficients (where the distinct sets \(\{i_1, \ldots, i_v\}, \{j_1, \ldots, j_v\}, \ldots, \{m_1, \ldots, m_v\}\) of suffices are not necessarily disjoint) such that the sum of each set of coefficients is congruent to a \((\text{mod } \pi^m)\) and such that the common part of any two sets of suffices is the same. We put the variables corresponding to the coefficients in the common part \(\{i_1, \ldots, i_v\} \cap \{j_1, \ldots, j_v\} \cap \ldots \cap \{m_1, \ldots, m_v\}\) of the sets of the suffices to 0 and so get with suitable labelling the \(v\) disjoint sets

\[
a_{i_1}, \ldots, a_{i_v}; \quad a_{i_{u+1}}, \ldots, a_{i_{u+v+1}}; \quad \ldots; \quad a_{i_{(v-1)u+1}}, \ldots, a_{i_{vu}}
\]

of \(u \leq r\) coefficients. Now make the following substitution:

\[
\alpha_i = \begin{cases}
\gamma_1, & 1 \leq i \leq u, \\
\gamma_1, & u + 1 \leq i \leq 2u, \\
\ldots, & \ldots, \\
\gamma_v, & (v-1)u + 1 \leq i \leq uv, \\
0, & \text{otherwise}.
\end{cases}
\]

Then the congruence (3) becomes

\[
a(\gamma_1^2 + \ldots + \gamma_v^2) = 0 \text{ (mod } \pi^m)\]

and so in order to have a primitive solution of (3) it suffices to solve the congruence

\[
y_1^2 + \ldots + y_v^2 = 0 \text{ (mod } p^m),
\]

with not all of \(y_1, \ldots, y_v\) divisible by \(\pi\), since \((\pi^m) = (p)\).

Denote by \(\theta(d)\) the least \(v\) for which the congruence (5) has a primitive solution. Then since \(p^m \leq d\),

\[
\theta(d) \leq \left( \frac{\log \pi^m \theta(d)}{\log \pi} \right)^{1/2} \cdot \theta(d) - 1 < 16n^3 (\log d)^3 \theta(d)
\]

for all \(d \geq 4\). It can be verified readily, by using the addition of residue classes \((\text{mod } p^m)\) for example, that \(\theta(d) \leq 4d\) for all \(d\), whence since \(G(d) \leq d \cdot H(d)\), we have

**Theorem 1.** For all exponents \(d\) and prime ideals \(\mathfrak{p}\) in any algebraic number field of degree \(n\) over the rationals

\[
G(d) < 16n^2 (\log d)^2 d^3.
\]

This estimate evidently has a factor \(n^2\) and so of \(d^2\) where \(e\) is the ramification index and \(p^e\) is the order of the residue class field. As a result it is of limited interest unless the \(n^2\) can be replaced by a small power of \(d\). Well ([24], p. 502) has proved that if \(d^e \leq p^e\), then the congruence

\[
a x^d + b y^d + c z^d = 0 \text{ (mod } p^m),
\]

where \(a, b, c, x, y, z\) are prime to \(\pi\), has a primitive solution. It follows by a straightforward inductive argument and Hensel's lemma that if \(d^e \leq p^e\) then

\[
H(d) \leq 3^m.
\]

Plainly if \(p\) is unramified, so that \(e = 1\), then \(H(d) \leq 3^m\) and combining this result with (6) gives a uniform estimate

\[
G(d) \leq 36 (\log d)^2 d^3.
\]

when \(p\) is unramified and \(p\) is odd. However, since it is likely that more direct arguments will yield the best possible result (2) for all unramified primes \(p\), this estimate will not be proved.

The inequality (6) provides a fairly good estimate for \(G(d)\) when \(p - 1\) does not divide \(d\) and the possibility that \(p\) might not divide \(d\) is no longer excluded.

**Theorem 2.** Let \(p\) be unramified and suppose \(p - 1\) does not divide \(d\), where \(p > 1\) is the rational prime above. Then

\[
G(d) < C(\log d)^2 d^{3/2}
\]
where \( C \) is an absolute constant, or if \( d \) is sufficiently large
\[ G(d) < d^{2+\varepsilon} \]
for any positive \( \varepsilon \).

**Proof.** If \( p - 1 \) does not divide \( d \) then
\[ \theta(d) < 18 (\log d)^{2/3} \]
([10] and [23]). Suppose first that \( p' \leq d' \). Then since \( n = f \), (6) implies that
\[ H(d) < \left( \frac{\log d' \theta(d)}{\log q} \right)^2 + 2 \theta(d) + \theta(d) - 1 < C \left( \log d \right)^{1/3} d^{2/3} , \]
where \( C \) is an absolute constant.

When \( d' < p' \) we have that
\[ H(d) < 3^s < 3p'^2 < 3d^{2/3} \]
since \( p > 7 \). As \( G(d) < dH(d) \), the theorem follows.

If \( p \) is unramified and \( d \) is odd or, more generally if \( (d, p - 1) \) divides \( \frac{1}{2}(p - 1) \), so that \(-1\) is a \( d \)th power residue \( (\text{mod} p') \), then \( \theta(d) = 2 \). It can be verified readily that given any positive \( \varepsilon \),
\[ G(d) < d^{2+\varepsilon} \]
providing \( d \) is sufficiently large when \( \tau = 0 \) and \( p \) is sufficiently large \( (p > 3^m) \) when \( \tau > 0 \). Of course if \( (d, p' - 1) \) divides \( \frac{1}{2}(p' - 1) \), so that \(-1\) is a \( d \)th power residue \( (\text{mod} p') \), a simple box argument can be used. For if \( s' > N(a') = p'^2 \), the congruence (3) with \( e = 1 \), must have a primitive solution, whence
\[ H(d) < \frac{\log p' \theta(d)}{\log q} . \]

As before it follows that if \( p \) is unramified and \( (d, p' - 1) \) divides \( \frac{1}{2}(p' - 1) \) then given any positive \( \varepsilon \)
\[ G(d) < d^{2+\varepsilon} \]
for \( d \) or \( p \) sufficiently large.

Dr Peter Plesnaci has pointed out that it is not possible to improve the Brdós–Rado result sufficiently to give a uniform estimate. For let \( a_1, \ldots, a_r \) be \( p \)-adic units whose images in the residue class field \( k = GF(p') \) form a basis over \( GF(p) \). Then no two distinct subsets of the
\[ \left[ \frac{2d}{d} \left( \frac{\log p}{\log 2} \right) \right] \]
numbers of the form
\[ 2^{i-1}a_ja_{j-1} \quad 1 \leq i \leq \frac{\log p}{\log 2}, \quad 1 \leq j < f, \quad 1 \leq r \leq \gamma p/d , \]
have the same sum \( (\text{mod} n^p) \). Thus the best possible result which the methods used here can give has a non-uniform lower bound \( \frac{\gamma n}{d} \left( \frac{\log p}{\log 2} \right) \theta(d) \).

The idea used here of grouping the coefficients so that the sums of each group are all in the same residue class is in contrast to the approach of Birch who works with coefficients distributed amongst many different cosets of the subgroup of \( d \)th powers in \( k^* \). However, despite these two approaches being to some extent complementary, I can see no way exploiting this to improve Birch's estimate or even to shorten his arguments.

**Acknowledgements.** I am grateful to Dr. B. J. Birch and to Dr. M. Bhaskaran for their advice and to Dr. Peter Plesnaci for some very helpful discussions. I am also grateful to the referee for suggesting some improvements in the presentation and to Professor A. Schinzel for drawing my attention to some references.

**References**

К одной формуле Зигеля

Т. В. Вихадзе (Тбилиси)

§ 1. Пусть \( f = \sum_{1 \leq d \leq m} a_d \cdot z^d \) — целочисленная квадратичная форма с индексом инверсии \( n \), \( S(f, g) \) — соответствующая сумма Гаусса, \( d = (-1)^{[m/2]} \det(2f) \) — дискриминант формы \( f \); далее пусть \( \varepsilon \) и \( \tau \) — комплексные переменные, причем \( \Re \tau > 0 \).

Раманатхан [12] доказал, что при \( m \geq 3 \) (за исключением нулевых форм при \( m = 3 \) и нулевых форм, дискримinant которых полный квадрат, при \( m = 4 \)) функцию

\[
U_m(\tau, \varepsilon; f) = 1 + e^{\frac{n((\tau, \varepsilon))}{4} |d|^{-1/2}} \times \\
\sum_{n=1}^{\infty} \sum_{H=0}^{\infty} \sum_{(a, H) = 1} \frac{S(fH, g)}{(H, H) \cdot (\tau, \varepsilon; f)}
\]

регулярную при фиксированном \( \tau \) и \( \Re \varepsilon > 2 - m/2 \), можно аналитически продолжить в полную окрестность точки \( \varepsilon = 0 \). Далее, положив

\[
\theta_m(\tau; f) = U_m(\tau, \varepsilon; f)|_{\varepsilon = 0},
\]

доказал, что при \( m \geq 3 \) имеет место равенство

\[
F_m(\tau; f) = \theta_m(\tau; f),
\]

где \( F_m(\tau; f) \) — тета-функция рода формы \( f \) (см., напр., [12], стр. 432, формула (38)).

В случае \( m \geq 4 \) функция (2) совпадает с рядом Эйлера — Зигеля, а формула (3) — с известной формулой Зигеля ([13], теорема 3).

В упомянутой выше работе Раманахан утверждает, что в случае положительных и негладковых неопределенных бинарных квадратичных форм функцию (1) невозможно аналитически продолжить в полную окрестность точки \( \varepsilon = 0 \).

Однако, в случае положительных диагональных квадратичных форм функция (1) еще ранее была исследована Ломаде [5], который