Conspectus materiae tomi XL, fasciculi 2

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange	Address of the Editorial Board and of the exchange	Die Adresse der Schriftleitung und des Austausches	Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-02070-9 ISSN 0065-1036

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XL (1982)

Some estimates for diagonal equations over $\mathfrak{p}$-adic fields

by

M. M. Dodson (Heslington, York)

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

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

$$a_1x_1^d + \ldots + a_sx_s^d = 0, \tag{1}$$

where $a_1, \ldots, a_s$ are arbitrary non-zero $\mathfrak{p}$-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 $\Gamma(d)$ also depending only on d, such that every general form of degree d in at least $\Gamma(d)$ variables over a $\mathfrak{p}$-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 $\Gamma(d) = d^2+1$ but in 1966 Terjanian [20] produced a form of degree 4 in 18 variables which did not represent zero non-trivially in $\boldsymbol{Q}_2$. Subsequently other authors disproved the conjecture for every p-adic field $\boldsymbol{Q}_p$. For example Browkin [5] showed that there exist forms of degree d in n variables over $\boldsymbol{Q}_p$ which have no non-trivial zeros and with $\log_d n$ arbitrarily close to 3. Terjanian [21] extended this result to finite extensions of $\boldsymbol{Q}_p$ and so in particular to $K_{\mathfrak{p}}$. Nonetheless, Artin's conjecture holds for all but a finite number of primes $\mathfrak{p}$ in K since Ax and Kochen [1] 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 [16] who showed that

$$G(d) \leqslant 4d^{2n+3}+1,$$

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

$$G(d) \leqslant (2\tau+3)^d(m_0^2 d)^{d-1}.$$

In view of Ax and Kochen's result Birch's estimate appears to be far from best possible though the possibility when $\mathfrak{p}$ 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

$$G(d) \leqslant (d-1)d+1.$$

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

$$G(d) \leqslant d^2+1. \tag{2}$$

In the p-adic case, where $K_{\mathfrak{p}} = Q_p$, Davenport and Lewis [8] showed that $G(d) \leqslant d^2+1$ and that there is equality whenever $d+1$ is prime. When $d+1$ is composite

$$G(d) \leqslant \tfrac{1}{2}\{1+2/(1+\sqrt{1+4d}\,)\}d^2+1,$$

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,

$$G(d) < d^{3/2+\varepsilon}.$$

When d is odd, $G(d)$ is much smaller and Tietäväinen [22] 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 $\mathfrak{p}$-adic case

$$G(d) < 16n^2(\log d)^2 d^2,$$

where $n = [K_{\mathfrak{p}}\colon Q_p]$. 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 $\mathfrak{p}$ 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 Erdös 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], Stemmler [18] and Tatuzawa [19] showed that every element in the ring J_d generated by dth powers of integers in $K_{\mathfrak{p}}$ can be represented as a sum of $4nd$ dth powers of integers. As in the rational case, Waring's problem and diagonal equations over $\mathfrak{p}$-adic fields have some similar features but the methods employed by Körner, Stemmler and Tatuzawa 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 $p \leqslant d$, and for each d, there are only a finite number of primes $\mathfrak{p}$ in K under consideration.

By absorbing dth powers of π into the variables and by multiplying by the appropriate power of π 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 π 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 π 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 π, has a non-trivial solution, so that

$$G(d) \leqslant dH(d).$$

As is well known, Hensel's lemma implies that the non-trivial solubility of equation (1) follows from the congruence

$$a_1x_1^d+\ldots+a_sx_s^d \equiv 0 \pmod{\pi^{\gamma e}}, \tag{3}$$

where $p^{\gamma-1}$ exactly divides $2d$ and where $a_1, \ldots, a_s$ are prime to π, having a primitive solution (i.e. a solution with not all the variables $x_1, \ldots, x_s$ divisible by π). Consider the $\binom{s}{r}$ sets $a_{i_1}, \ldots, a_{i_r}$ 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

$$(N^{\gamma e})^{-1}\binom{s}{r} = p^{-ef\gamma}\binom{s}{r}$$

have the same sum (mod $\mathfrak{p}^{\gamma e}$) or equivalently (mod $\pi^{\gamma e}$). Erdös and Rado [12] proved that if

$$(4)\qquad p^{-n\gamma}\binom{s}{r} > (r!)(v-1)^{r+1}\left(1-\frac{1}{2!(v-1)}-\ldots-\frac{r-1}{r!(v-1)^{r-1}}\right)$$

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

$$(s-r+1)^r \geqslant p^{n\gamma}(r!)^2 v^{r+1}$$

and so is satisfied if

$$(s-r+1) \geqslant vr^2 4^{-1+1/r}(p^{n\gamma}v)^{1/r}.$$

Put

$$r = \left[\frac{\log p^{n\gamma}v}{\log 4}\right]+2,$$

where $[x]$ denotes the integer part of the real number x, so that

$$(4p^{n\gamma}v)^{1/r} < 4.$$

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

$$a_{i_1}, \ldots, a_{i_r};\ a_{j_1}, \ldots, a_{j_r};\ \ldots;\ a_{m_1}, \ldots, a_{m_r},$$

of r coefficients (where the distinct sets $\{i_1, \ldots, i_r\}$, $\{j_1, \ldots, j_r\}$, $\ldots$, $\{m_1, \ldots, m_r\}$ of suffices are not necessarily disjoint) such that the sum of each set of coefficients is congruent to a (mod $\pi^{\gamma e}$) 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 $\{i_1, \ldots, i_r\}\cap\{j_1, \ldots, j_r\}\cap\ldots\cap\{m_1, \ldots, m_r\}$ of the sets of the suffices to 0 and so get with suitable elabelling the v disjoint sets

$$a_1, \ldots, a_u;\ a_{u+1}, \ldots, a_{2u};\ \ldots;\ a_{(v-1)u+1}, \ldots, a_{vu}$$

of $u \leqslant r$ coefficients. Now make the following substitution:

$$x_i = \begin{cases} y_1, & 1 \leqslant i \leqslant u, \\ y_2, & u < i \leqslant 2u, \\ \ldots\ldots\ldots\ldots & \\ y_v, & (v-1)u < i \leqslant vu, \\ 0, & \text{otherwise}. \end{cases}$$

Then the congruence (3) becomes

$$a(y_1^d+\ldots+y_v^d) \equiv 0 \pmod{\pi^{\gamma e}}$$

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

$$(5)\qquad y_1^d+\ldots+y_v^d \equiv 0 \pmod{p^\gamma},$$

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

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

$$(6)\qquad H(d) \leqslant \left\{\left[\frac{\log p^{n\gamma}\theta(d)}{\log 4}\right]+2\right\}^2\theta(d)+\theta(d)-1 < 16n^2(\log d)^2\theta(d)$$

for all $d \geqslant 4$. It can be verified readily, by using the addition of residue classes (mod p^γ) for example, that $\theta(d) \leqslant 4d$ for all d, whence since $G(d) \leqslant d\cdot H(d)$, we have

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

$$G(d) < 16n^2(\log d)^2 d^2.$$

This estimate evidently has a factor n^2 and so of e^2f^2 where e is the ramification index and p^f 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. Weil ([24], p. 502) has proved that if $d^4 \leqslant p^f$, then the congruence

$$ax^d+by^d+cz^d \equiv 0 \pmod{\pi},$$

where a, b and c are prime to π, has a primitive solution. It follows by a straightforward inductive argument and Hensel's lemma that if $d^4 \leqslant p^f$ then

$$H(d) \leqslant 3^{\gamma e}.$$

Plainly if $\mathfrak{p}$ is unramified, so that $e = 1$, then $H(d) \leqslant 3^\gamma$ and combining this result with (6) gives a uniform estimate

$$G(d) < 36(\log d)^2 d^2$$

when $\mathfrak{p}$ 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 $\mathfrak{p}$, 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 $\mathfrak{p}$ be unramified and suppose $p-1$ does not divide the exponent d, where $p > 7$ is the rational prime above. Then*

$$G(d) < C(\log d)^5 d^{3/2}$$

where C is an absolute constant, or if d is sufficiently large

$$G(d) < d^{3/2+\varepsilon}$$

for any positive ε.

Proof. If $p-1$ does not divide d then

$$\theta(d) < 18(\log d)d^{1/2}$$

([10] and [23]). Suppose first that $p^f \leqslant d^4$. Then since $n = f$, (6) implies that

$$H(d) < \left\{\left[\frac{\log d^{4\gamma}\theta(d)}{\log 4}\right]+2\right\}^2\theta(d)+\theta(d)-1 < C(\log d)^5 d^{1/2},$$

where C is an absolute constant.

When $d^4 \leqslant p^f$ we have that

$$H(d) \leqslant 3^\gamma < 3p^{\tau/2} \leqslant 3d^{1/2}$$

since $p > 7$. As $G(d) \leqslant dH(d)$, the theorem follows.

If $\mathfrak{p}$ is unramified and d is odd or, more generally if $(d, p-1)$ divides $\frac{1}{2}(p-1)$, so that -1 is a dth power residue $(\bmod\, \mathfrak{p}^\gamma)$, then $\theta(d) = 2$. It can be verified readily that given any positive ε,

$$G(d) < d^{1+\varepsilon}$$

providing d is sufficiently large when $\tau = 0$ and p is sufficiently large $(p > 3^{1/\varepsilon})$ when $\tau > 0$. Of course if (d, p^f-1) divides $\frac{1}{2}(p^f-1)$, so that -1 is a dth power residue $(\bmod\, \pi^\gamma)$, a simple box argument can be used. For if $2^s > N(\pi^\gamma) = p^{\gamma f}$, the congruence (3) with $e = 1$, must have a primitive solution, whence

$$H(d) < \frac{\log p^{\gamma f}}{\log 2}.$$

As before it follows that if $\mathfrak{p}$ is unramified and (d, p^f-1) divides $\frac{1}{2}(p^f-1)$ then given any positive ε

$$G(d) < d^{1+\varepsilon}$$

for d or p sufficiently large.

Dr Peter Pleasants has pointed out that it is not possible to improve the Erdös–Rado result sufficiently to give a uniform estimate. For let $a_1, \ldots, a_f$ be $\mathfrak{p}$-adic units whose images in the residue class field k $(= \mathrm{GF}(p^f))$ form a basis over $\mathrm{GF}(p)$. Then no two distinct subsets of the $\frac{\gamma ef}{d}\left[\frac{\log p}{\log 2}\right]$ numbers of the form

$$2^{i-1}a_j\pi^{r-1}, \quad 1 \leqslant i \leqslant \frac{\log p}{\log 2}, 1 \leqslant j \leqslant f,\ 1 \leqslant r \leqslant \gamma e/d,$$

have the same sum $(\bmod\, \pi^{\gamma e})$. 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 dth 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 Pleasants 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

[1] J. Ax and S. Kochen, *Diophantine problems over local fields I*, Amer. J. Math. 87 (1965), pp. 605–630.
[2] B. J. Birch, *Diagonal equations over* $\mathfrak{p}$*-adic fields*, Acta Arith. 9 (1964), pp. 291–300.
[3] J. Bovey, $\Gamma^*(8) = 39$, ibid. 25 (1974), pp. 145–150.
[4] R. Brauer, *A note on systems of homogeneous algebraic equations*, Bull. Amer. Math. Soc. (2) 51 (1945), pp. 749–755.
[5] J. Browkin, *On forms over p-adic fields*, Bull. Acad. Polon. Sci. 14(1966), pp. 489–492.
[6] C. Chevalley, *Demonstration d'une hypothese de M. Artin*, Abh. Math. Sem. Univ. Hamburg 11 (1936), pp. 73–75.
[7] P. Cohen, *Decision procedures for real and p-adic fields*, Comm. Pure Appl. Math. 22 (1969), pp. 131–151.
[8] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc. A 274 (1963), pp. 443–460.
[9] M. M. Dodson, *Homogeneous additive congruences*, Philos. Trans. Roy. Soc. London, Ser. A, 261 (1967), pp. 163–210.
[10] — *On a function due to S. Chowla*, J. Number Theory 5 (1973), pp. 287–292.
[11] — *A note on homogenous additive equations over p-adic fields*, Ann. Univ. Turku, Ser. A I, 164 (1974), pp. 3–7.
[12] P. Erdös and R. Rado, *Intersection theorems for systems of sets*, J. London Math. Soc. 35 (1960), pp. 85–90.
[13] J. S. M. Gray, *Diagonal forms of prime degree*, University of Notre Dame thesis, 1958.
[14] O. Körner, *Über das Waringsche Problem in algebraischen Zahlkörpern*, Math. Ann. 144 (1961), pp. 224–238.
[15] D. J. Lewis, *Cubic congruences*, Michigan Math. J.4 (1957), pp. 85–95.
[16] L. G. Peck, *Diophantine equations in algebraic number fields*, Amer. J. Math. 66 (1944), pp. 122–136.

[17] C. L. Siegel, *Additive Theorie der Zahlenkörper II*, Math. Ann. 88 (1923), pp. 184–210.
[18] R. M. Stemmler, *The easier Waring problem in algebraic number fields*, Acta Arith. 6 (1961), pp. 447–468.
[19] T. Tatuzawa, *On Waring's problem in algebraic number fields*, ibid. 24 (1973), pp. 37–60.
[20] G. Terjanian, *Une contre-exemple à une conjecture d'Artin*, C. R. Acad. Sci. Paris, Ser. A, 262 (1966), p. 612.
[21] — *Sur la dimension diophantienne des corps p-adiques*, Acta Arith. 34 (1978), pp. 127–130.
[22] A. Tietäväinen, *On a problem of Chowla and Shimura*, J. Number Theory 3 (1971), pp. 247–252.
[23] — *Proof of a conjecture of S. Chowla*, ibid. 7 (1975), pp. 353–356.
[24] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (1949), pp. 497–508.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF YORK
Heslington, York, England

Received on 23.4.1976
and in revised form on 12.7.1979 (843)

ACTA ARITHMETICA
XL (1982)

К одной формуле Зигеля

Т. В. Вепхвадзе (Тбилиси)

§1. Пусть $f = \sum_{1\leqslant k\leqslant j\leqslant m} a_{kj}x_kx_j$ — целочисленная квадратичная форма с индексом инерции n, $S(f, q)$ — соответствующая сумма Гаусса, $d = (-1)^{[m/2]}\det(2f)$ — дискриминант формы f; далее пусть z и τ — комплексные переменные, причем $\operatorname{Im}\tau > 0$.

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

$$\Psi_m(\tau, z; f) = 1 + e^{\frac{\pi i(2n-m)}{4}}|d|^{-1/2}\times \tag{1}$$
$$\times \sum_{q=1}^{\infty} \sum_{\substack{H=-\infty\\(q,H)=1}}^{\infty} \frac{S(fH, q)}{q^{m/2}(q\tau-H)^{n/2}(q\bar{\tau}-H)^{(m-n)/2}|q\tau-H|^{z}},$$

регулярную при фиксированном τ и $\operatorname{Re} z > 2 - m/2$, можно аналитически продолжить в полную окрестность точки $z = 0$. Далее, положив

$$\theta_m(\tau; f) = \Psi_m(\tau, z; f)|_{z=0}, \tag{2}$$

доказал, что при $m \geqslant 3$ имеет место равенство

$$F_m(\tau; f) = \theta_m(\tau; f), \tag{3}$$

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

В случае $m > 4$ функция (2) совпадает с рядом Эйзенштейна–Зигеля, а формула (3) — с известной формулой Зигеля ([13], теорема 3).

В упомянутой выше работе Раманатхан утверждает, что в случае положительных и ненулевых неопределенных бинарных квадратичных форм функцию (1) невозможно аналитически продолжить в полную окрестность точки $z = 0$.

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