[5] K. Inkeri and S. Hyyrö, *On the congruence $3^{p-1} \equiv 1 \pmod{p^2}$ and the Diophantine equation $x^2-1=y^p$*, Ann. Univ. Turku A 50 (1961), pp. 1-4.

[6] V. A. Lebesgue, *Sur l'impossibilité, en nombres entiers, de l'équation $x^m=y^2+1$*, Nouv. Ann. de Math. 9 (1850), pp. 178-181.

[7] T. Nagell, *Des équations indéterminées $x^2+x+1=y^n$ et $x^2+x+1=3y^n$*, Norsk Mat. Forenings Skrifter I, 2 (1921), pp. 1-14.

[8] R. Niewiadomski, *Zur Fermatschen Vermutung*, Prace Mat. Fizyczne 42 (1935), pp. 1-10.

[9] R. Obláth, *Über die Zahl x^2-1*, Mathematica B VIII (1939-1940), pp. 161-172.

[10] E. H. Pearson, *On the Congruences $(p-1)! \equiv 1$ and $2^{p-1} \equiv 1 \pmod{p^2}$*, Math. Comp. 17 (1963), pp. 194-195.

[11] C. L. Siegel, *Über die Klassenzahl quadratischer Zahlkörper*, Acta Arithm. 1 (1936), pp. 83-86.

UNIVERSITY OF TURKU, TURKU, FINLAND

Reçu par la Rédaction le 28. 12. 1963

ACTA ARITHMETICA
IX (1964)

Diagonal equations over $\mathfrak{p}$-adic fields

by

B. J. Birch (Manchester)

1. It has been conjectured that every form of degree d in at least d^2+1 variables over a $\mathfrak{p}$-adic field K has a non-trivial zero in K. However, as yet it has not even been proved that there is a constant $\Gamma(d)$ independent of K such that every form of degree d in at least $\Gamma(d)$ variables over a $\mathfrak{p}$-adic field has a non-trivial zero in the field. It is the purpose of this note to fill this gap.

In view of the results of Brauer [3], we can deal with general forms (though with an enormously large number of variables) if we can deal with diagonal forms; so it will be enough to prove

THEOREM. *Given d, there is a constant $G(d)$ such that any form*

$$\sum_{i=1}^{s} a_i x_i^d$$

with coefficients in a $\mathfrak{p}$-adic field K and $s \geqslant G(d)$ will have a non-trivial zero x over K.

Our proof of the theorem is a moderately straightforward, though messy, computation; for some of the variables x_j we substitute expansions $1+\sum_{t=1}^{\infty}\pi^t y_{jt}$, where π generates the prime ideal of K and the y_{jt} are units; and in § 2 we analyse what the powers $(1+\sum_{t=1}^{\infty}\pi^t y_{jt})^d$ look like. This enables us to prove our result fairly easily, and fairly efficiently, in certain favourable cases — this is done in § 3. Introducing devices to avoid various difficulties that arise, we gradually widen the scope of our methods, until in § 4 we can prove our theorem in general.

Unfortunately, the arguments of § 4, though not difficult, are inefficient; so our final result involves an inordinately large number of variables.

Our results may be applied to prove theorems about the solutions of equations over algebraic number fields — see [1]. Results similar to our theorem, but with a far better estimate for $G(d)$, have been proved previously for prime degree d by Lewis [6] and by Gray [5]; for rational p-adic forms Davenport and Lewis [4] have proved the best possible result, that a form $\sum_{i=1}^{s} a_i x_i^d$ over a p-adic field has a non-trivial zero whenever $s \geqslant d^2+1$. Waring's problem is discussed in [2], a companion paper to this.

I would like to thank Prof. D. J. Lewis for going through this note with me; unfortunately we were unable to find any notable simplification.

In what follows, K is a $\mathfrak{p}$-adic field with ring of integers $\mathfrak{o}$, units U, and prime ideal $\mathfrak{p} = (\pi)$. The rational prime above $\mathfrak{p}$ is p, the ramification index is e so that $(\pi^e) = (p)$, and the residue class field $k = \mathfrak{o}/\mathfrak{p}$ has p^f elements so that $N\mathfrak{p} = p^f$. We write $d = p^l m$, with $(m, p) = 1$, and we write $(m, p^f-1) = D$.

2. If a is an element of K, we write $w(a)$ for the power of π exactly dividing a, so that $\pi^{-w(a)}a$ is a unit. We call $w(a)$ the *weight* of a; it is convenient to take $w(0) = \infty$. For a polynomial g over K, we write $w(g)$ for the weight of the lightest coefficient of g.

If now $f(x, y) = \sum c_j(x) y^j$ is any polynomial in a variable y and other variables x, we define $\lambda(y; f)$, the *level* of y in f, as the least weight of the coefficients of terms of $f(x, y)$ that really involve y; so

$$\lambda(y; f) = \min_{j>0} w(c_j).$$

In this section we compute the level of y in $(1+\pi^t y)^d$ for various values of t. We know

$$(1+\pi^t y)^d = 1+\sum_{j=1}^{d} \binom{d}{j} \pi^{tj} y^j;$$

suppose that $j = p^r k$ with $(k, p) = 1$, $0 \leqslant r \leqslant l$; then we know that

$$p^{l-r} \,\Big\|\, \binom{d}{j} = \binom{p^l m}{p^r k}, \qquad \text{so} \qquad w\left(\binom{d}{j}\right) = (l-r)e.$$

So

$$w\left(\binom{d}{j} \pi^{jt}\right) = (l-r)e + p^r kt,$$

and

$$\lambda\big(y; (1+\pi^t y)^d\big) = \min_{0 \leqslant r \leqslant l} [(l-r)e + p^r t].$$

We deduce

LEMMA 1. *If $e/(p-1)t = p^r$, a power of p, then*

$$\lambda\big(y; (1+\pi^t y)^d\big) = (l-r)e + e/(p-1),$$

and the coefficients of y^{p^r} and $y^{p^{r+1}}$ both have this weight.

Otherwise, there is precisely one term of least weight in $(1+\pi^t y)^d$; it involves y^{p^r}, where r is defined by

$$r = \begin{cases} 0 & \text{for} \quad e < (p-1)t, \\ l & \text{for} \quad e > p^{l-1}(p-1)t \end{cases}$$

and otherwise

$$p^{r-1} < e/(p-1)t < p^r$$

and now

$$\lambda\big(y; (1+\pi^t y)^d\big) = (l-r)e + p^r t.$$

3. In this section, we prove Lemma 3, which is a particular case of our theorem; in order to make the motivation clearer, we first prove Lemma 2, whose statement is similar to that of Lemma 3, but with an extra condition added.

First, we need to define two equivalence relations on the elements of $\mathfrak{o}$.

DEFINITION. If $a, b \in \mathfrak{o}$, we say that a, b are *X-equivalent* if we can write $a/b = \pi^{dt}c$ where t is an integer and c is a unit congruent to a dth power modulo π.

We say a, b are *Y-equivalent* if a/b is a unit times a dth power — that is to say, if $d \mid w(a) - w(b)$.

Note that since the multiplicative group k^* is cyclic of order p^f-1 there are just Dd X-equivalence classes; here $D = (d, p^f-1)$. If a and b have the same weight, then they are X-equivalent if and only if a/b is a dth power modulo π.

LEMMA 2. *Suppose that $(p-1) \nmid e$. Let*

$$f(X, Y) = \sum_{i=0}^{Dd-1} a_i X_i^d + \sum_{j=0}^{d-1} b_j Y_j^d$$

be a form over K, where there is just one coefficient a_i in each X-equivalence class and just one coefficient b_j in each Y-equivalence class. Then we can find X, Y not all zero in K such that $f(X, Y) = 0$.

Proof. (i) By absorbing powers of π into the variables X, Y we may suppose that all the coefficients a, b are in $\mathfrak{o}$, and have weights less than d. Rearranging if necessary, we may suppose that b_j has weight j for $j = 0, \ldots, d-1$ and that a_i has weight w whenever $iD \leqslant w < iD+D$.

(ii) Take $Y_j = 1+\sum_{t=1}^{\infty} \pi^t y_{jt}$ for $j = 0, \ldots, d-1$, and write $X = x$, so that

$$f(X, Y) = F(x, y) = \sum_{i=0}^{Dd-1} a_i x_i^d + \sum_{j=0}^{d-1} b_j \Big(1+\sum_{t=1}^{\infty} \pi^t y_{jt}\Big)^d;$$

we will sometimes call variables x and y *auxiliary* variables.

We will choose first the x's in order of increasing i and then the y's in order of increasing $j+dt$ as elements of $\mathfrak{o}$ to make $F(x,y)$ vanish. (At the time a given auxiliary variable is chosen we only need its residue class modulo π; more often than not, we will choose an auxiliary variable to be zero.)

(iii) We prove by induction on r that for $0 \leqslant r \leqslant d$ we can choose $x_0, \dots, x_{Dr-1}$ so that

$$\sum_{i=0}^{Dr-1} a_i x_i^d + \sum_{j=0}^{d-1} b_j \equiv 0 \ (\pi^r). \tag{3.1}$$

In fact, this is certainly so for $r=0$; suppose now that we have chosen $x_0, \dots, x_{Dr-1}$ to satisfy (3.1), with $0 \leqslant r \leqslant d-1$. Then $a_{Dr}, \dots, a_{Dr+D-1}$ all have weight r and are in different X-equivalence classes; so either

$$\sum_{i=0}^{Dr-1} a_i x_i^d + \sum_{j=0}^{d-1} b_j \equiv 0 \ (\pi^{r+1})$$

and we have a solution of

$$\sum_{i=0}^{Dr+D-1} a_i x_i^d + \sum_{j=0}^{d-1} b_j \equiv 0 \ (\pi^{r+1}) \tag{3.2}$$

with $x_{Dr} = \dots = x_{Dr+D-1} = 0$, or else the sum on the left of (3.1) is X-equivalent to $-a_I$ for some I between Dr and $Dr+D-1$; we can then choose x_I to satisfy

$$\sum_{i=0}^{Dr-1} a_i x_i^d + a_I x_I^d + \sum_{j=0}^{d-1} b_j \equiv 0 \ (\pi^{r+1}),$$

giving a solution of (3.2) with $x_i = 0$ for $i \neq I$, $Dr \leqslant i < D(r+1)$.

(iv) We assert that for every μ with $\mu \geqslant p^l$ there is at least one variable y_{jt} with level μ in F,

$$\lambda(y_{jt};\ F) = \mu.$$

In fact, write $\lambda\big(y_t;\ (1+\sum_{t=1}^{\infty}\pi^t y_t)^d\big) = \lambda_t$ for short. Then it follows immediately from Lemma 1 that $\lambda_1 \leqslant p^l$ and that $0 \leqslant \lambda_t - \lambda_{t-1} \leqslant p^l$ for all $t \geqslant 2$. Now, $\lambda\big(y_{jt};\ F(x,y)\big) = j+\lambda_t$, where j may take any value from 0 to $d-1$; for any $\mu \geqslant p^l$, we choose λ_t so that $\lambda_t \leqslant \mu < \lambda_t + p^l$, and then $j = \mu - \lambda_t$.

(v) Since $(p-1) \nmid e$, by Lemma 1 there is precisely one term of

$$\Big(1+\sum_{s=1}^{t}\pi^s y_s\Big)^d$$

involving y_t whose coefficient has weight λ_t; in fact,

$$\Big(1+\sum_{s=1}^{t}\pi^s y_s\Big)^d \equiv \Big(1+\sum_{s=1}^{t-1}\pi^s y_s\Big)^d + \binom{d}{p^r}\pi^{p^r t} y_t^{p^r} \ (\pi^{\lambda_t+1})$$

where r is defined as in Lemma 1 and $\lambda_t = (l-r)e+p^r t$. We can write $\binom{d}{p^r}\pi^{p^r t} = \pi^{\lambda_t} u_t$, where u is a unit, and we note that as y runs through all the residue classes modulo π so does y^{p^r}.

(vi) For each $\mu \geqslant d$, fix a pair of suffices $j(\mu), t(\mu)$ so that the auxiliary variable $y_{j(\mu),t(\mu)}$, which we denote by $y_{(\mu)}$ for short, has level μ in F, $\lambda(y_{(\mu)};F) = \mu$.

Write $F^*(y)$ for the form in the variables of the sequence $\{y_{(\lambda)}\}$ obtained from F by choosing the x's as in (iii) to satisfy (3.1) with $r=d$, and setting all the auxiliary variables y not in the sequence $\{y_{(\lambda)}\}$ equal to zero. Write $F^*_\lambda(y)$ for F^* with $y_{(\mu)}$ set equal to zero for $\mu \geqslant \lambda$. We assert that for each $\lambda \geqslant d$ we can choose $y_{(d)}, \dots, y_{(\lambda-1)}$ so that

$$F^*_\lambda(y) \equiv 0 \ (\pi^\lambda). \tag{3.3}$$

We prove this by induction on λ; the induction starts, since (3.3) with $\lambda = d$ is just (3.1) with $r=d$. So suppose $y_{(d)}, \dots, y_{(\lambda-1)}$ have been chosen to satisfy (3.3), we have to show we can choose $y_{(\lambda)}$ to satisfy (3.3) with $\lambda+1$ for λ. As in (v), we have

$$F^*_{\lambda+1}(y) \equiv F^*_\lambda(y) + \pi^\lambda u_\lambda y_{(\lambda)}^{p^r} \ (\pi^{\lambda+1}),$$

where u is a unit. As y^{p^r} runs through all the residue classes modulo π, we can certainly find $y_{(\lambda)}$ to make $F^*_{\lambda+1} \equiv 0 \ (\pi^{\lambda+1})$.

(vii) We have thus shown that for each $\lambda > 0$ we can find $X^{(\lambda)}, Y^{(\lambda)}$ with the variables $Y^{(\lambda)}$ units and $f(X^{(\lambda)}, Y^{(\lambda)}) \equiv 0 \ (\pi^\lambda)$.

Take a limit point (X, Y) of the sequence $\{X^{(\lambda)}, Y^{(\lambda)}\}$; then $f(X,Y) = 0$ as required.

Lemma 3. *Let*

$$f(X, Y) = \sum a_i X_i^d + \sum b_j Y_j^d$$

where there are just $l+1$ coefficients a_i in each X-equivalence class, and just $l+1$ coefficients b_j in each Y-equivalence class. Then we can find X, Y not all zero in K such that $f(X,Y) = 0$.

Remark. We have omitted the condition $e \nmid (p-1)$ from Lemma 2. Accordingly, stage (v) of the proof of Lemma 2 breaks down for certain values of t; in fact when $e/(p-1)t$ is a power of p less than p^l, there may be more than one term of

$$\Big(1+\sum_{s=1}^{t}\pi^s y_s\Big)^d$$

of level λ_t involving y_t; and (3.3) is no longer necessarily soluble.

For the moment, call y_t exceptional when $e/(p-1)t$ is a power of p. The choice of an exceptional y_t is liable to be useless, so one must find a dodge by which one may avoid needing to use exceptional y's. There are various ways of doing this; the method we use is not the most efficient, we use it because it leads fairly easily to a proof of Lemma 4 in the final section.

Proof of Lemma 3. Dividing through by b_0, we may suppose that $b_0 = 1$. As in Lemma 2, we may suppose that all the coefficients a, b are in $\mathfrak{o}$, and have weights less than d. We can thus write

$$f(X, Y) = \sum_{k=0}^{l}\Big[\sum_{i=0}^{Dd-1} a_{ik}X_{ik}^d + \sum_{j=0}^{d-1} b_{jk}Y_{jk}^d\Big]$$

where b_{jk} has weight j and a_{ik} has weight w whenever $iD \leqslant w < iD+D$; for each k there is just one a_{ik} in each X-equivalence class.

Write $[e/d]+1 = E$, $[e/d] = E^*$; possibly $E = 1$. Substituting $\pi^{Ek}x_{jk}$ for X_{jk} and $\pi^{Ek}Y'_{jk}$ for Y_{jk}, we get

$$f = \sum_{k=0}^{l}\pi^{dEk}\Big[\sum_{i=0}^{Dd-1} a_{ik}x_{ik}^d + \sum_{j=0}^{d-1} b_{jk}Y'^{d}_{jk}\Big].$$

Substitute

$$Y'_{00} = 1+\sum_{t=1}^{E^*}\pi^{tm}y_{00t}+\sum_{t=e}^{\infty}\pi^t z_t,$$

$$Y'_{jk} = 1+\sum_{t=1}^{E^*}\pi^{tm}y_{jkt} \quad \text{for} \quad (j, k) \neq (0, 0);$$

then by Lemma 1,

$$Y'^{d}_{ik} \equiv \Big(1+\sum_{s=1}^{t-1}\pi^{sm}y_{iks}\Big)^d + \binom{d}{p^l}\pi^{td}y_{ikt}^{p^l} \ (\pi^{tp^l+1}) \quad \text{for} \quad 1 \leqslant t \leqslant E^*,$$

$$Y'^{d}_{00} \equiv \Big(1+\sum_{s=1}^{E^*}\pi^{sm}y_{00s}+\sum_{s=e}^{t-1}\pi^s z_s\Big)^d + d\pi^t z_t \ (\pi^{le+t+1}) \quad \text{for all } t \geqslant e.$$

We have thus

$$f = F(x, y, z) = \sum_{k=0}^{l}\pi^{dEk}\Big[\sum_{i=0}^{Dd-1} a_{ik}x_{ik}^d + \sum_{j=0}^{d-1} b_{jk}\Big(1+\sum_{t=1}^{E^*}\pi^{tm}y_{jkt}+\varepsilon_{jk}\sum_{t=e}^{\infty}\pi^t z_t\Big)^d\Big]$$

with $\varepsilon_{jk} = 0$ unless $j = k = 0$, $\varepsilon_{00} = 1$, and the levels of the various auxiliary variables are given by

$$\lambda(x_{ik}; F) = dEk+[i/D],$$

$$\lambda(y_{jkt}; F) = dEk+j+td,$$

$$\lambda(z_t; F) = el+t.$$

We deduce that for every $\mu \geqslant 0$ there is a variable of F with level μ. In fact, if $\mu \geqslant e(l+1)$, $\lambda(z_t; F) = \mu$ for $t = \mu-el$. If $\mu < e(l+1)$, take $k = \min(l, [\mu/dE])$, and write $\tau = [(\mu-kdE)d^{-1}]$. If now $\min(\tau, E^*) \geqslant 1$, take $t = \min(\tau, E^*)$ and $j = \mu-kdE-td$; we certainly have $j < d$ since $\mu-ldE-E^*d < (l+1)e-ld[e/d]-ld-d[e/d] < d$; and so $\lambda(y_{jkt}; F) = \mu$. Finally, if $\mu < e(l+1)$ and either $\mu-kdE < d$ or $e < d$ we have $\mu-kdE < d$; for in fact if $e < d$ then $E = 1$ and $\mu-kd < \max\big(d, e(l+1)-ld\big) \leqslant d$. Take $w = \mu-kdE$; then $\lambda(x_{ik}; F) = \mu$ for $wD \leqslant i < (w+1)D$.

Now we can prove the lemma. For each level λ, choose a set of auxiliary variables with level λ in F — this set of variables is to consist of either a single variable y or a single variable z or a set of D variables x, one in each possible X-congruence class. Set all other variables in F equal to zero. When this has been done, write $F_\lambda(x, y, z)$ for F with all remaining variables of level λ and above set equal to zero. Then

$$F(x, y, z) \equiv F_\lambda(x, y, z) \ (\pi^\lambda).$$

We prove by induction on λ that we can solve

$$F_\lambda(x, y, z) \equiv 0 \ (\pi^\lambda);$$

this is trivial when $\lambda = 0$. But now, for $\lambda > 0$, we have

$$F_{\lambda+1}(x, y, z) - F_\lambda(x, y, z)$$
$$\equiv \begin{cases} \displaystyle\sum_{i=0}^{D-1} a_{i+Dw,k}\pi^{dEk}x_{i+Dw,k}^d \ (\pi^{\lambda+1}) & \text{with } w+dEk = \lambda, \\ b_{jk}\binom{d}{p^l}\pi^{dEk+td}y_{jkt}^{p^l} \quad (\pi^{\lambda+1}) & \text{with } dEk+j+td = \lambda, \\ d\pi^t z_t \ (\pi^{\lambda+1}) & \text{with } t+el = \lambda \end{cases}$$

according as our set of variables of level λ in F is a set of x's or a y or a z. In any case, we can certainly choose this set from $\mathfrak{o}$ so that

$$F_{\lambda+1} \equiv 0 \ (\pi^{\lambda+1}).$$

Hence, for every $\lambda > 0$, we can find X, Y with the Y's units so that $f(X, Y) \equiv 0$ (π^λ). Hence we can solve $f(X, Y) = 0$ $\mathfrak{p}$-adically, as required.

4. In this section, we prove our main theorem in general. We deduce it quite easily from Lemma 4, which will be proved on the lines of Lemma 3.

LEMMA 4. *Let $\mathscr{S}$ be any set of X-equivalence classes. Let $f(X) = \sum a_i X_i^d$ be any form over K with at least $2l+2$ coefficients a_i in each X-equivalence class in $\mathscr{S}$. Then either f represents zero non-trivially over K or else $-f$ takes a value not in any of the equivalence classes in $\mathscr{S}$.*

Proof. Let representatives of the equivalence classes in $\mathscr{S}$ be $\gamma_1, \ldots, \gamma_\sigma$; we may suppose that all of $\gamma_1, \ldots, \gamma_\sigma$ are integers with weight less than d. Thus, we may suppose

$$f = \sum_{k=0}^{l}\Big(\sum_{i=1}^{\sigma} a_{ik}X_{ik}^d + \sum_{j=1}^{\sigma} b_{jk}Y_{jk}^d\Big)$$

where a_{ik}/γ_i and b_{jk}/γ_j are always units congruent mod π to dth powers (here we have renamed some of the variables of f as X's, some as Y's, and we have set any left over equal to zero).

As in Lemma 3, we suppose that $b_{00} = 1$, and substitute

$$X_{ik} = \pi^{Ek} x_{ik},$$

$$Y_{00} = 1 + \sum_{t=1}^{E^*} \pi^{tm} y_{00t} + \sum_{t=e}^{\infty} \pi^t z_t,$$

$$Y_{jk} = \pi^{Ek}\Big[1 + \sum_{t=1}^{E^*} \pi^{tm} y_{jkt}\Big] \quad \text{for} \quad (j, k) \neq (0, 0);$$

so that $f(X, Y) = F(x, y, z)$. Each variable of F will have a level in F; as before, F_λ denotes F with all auxiliary variables of level λ and above set equal to zero. If φ is an integer in one of the equivalence classes in $\mathscr{S}$, then as in the proof of Lemma 3 there is a variable of F with level equal to the weight of φ; and if this variable is an x, there is a variable x of F whose coefficient is in the same class as φ. Consequently, if the variables with levels less than λ have already been chosen so that $F_\lambda \equiv 0$ (π^λ), then, taking $\varphi = -F_\lambda$, we see that we can choose the variables with level λ so that $F_{\lambda+1} \equiv 0$ $(\pi^{\lambda+1})$.

Suppose then that we try to solve the congruence

$$F_\lambda(x, y, z) \equiv 0 \ (\pi^\lambda) \tag{4.1}$$

for $\lambda = 1, 2, 3, \ldots$ If (4.1) is soluble for every λ, then we can solve $F(x, y, z) = 0$ and so obtain a non-trivial $\mathfrak{p}$-adic solution of $f(X, Y) = 0$. Otherwise, there is a λ such that we have a solution x, y, z of (4.1), but

$$F_{\lambda+1}(x, y, z) \equiv 0 \ (\pi^{\lambda+1})$$

is insoluble. Then by the previous paragraph, $-F_\lambda$ is in none of the equivalence classes in $\mathscr{S}$; so $-f$ takes a value not in any of the equivalence classes in $\mathscr{S}$.

Proof of our theorem. Define $H(\sigma) = (2l+3)^{d-\sigma+1}(D^2d)^{d-\sigma}$ for $1 \leqslant \sigma \leqslant d$. We will prove by induction on $d-\sigma$ that if $\mathscr{S}$ is a set of σ X-equivalence classes, and $f = \sum a_i X_i^d$ is any form with at least $H(\sigma)$ coefficients in each class in $\mathscr{S}$, then f represents zero properly.

This is certainly true when $\sigma = d$, by Lemma 3; so the induction starts. Suppose then that f is as described. Since $H(\sigma) > [(2l+2)D^2d + 1]H(\sigma+1)$ we may write

$$f = \sum_{k=1}^{DdH(\sigma+1)} f_k(X^{(k)}) + f_0(X^{(0)})$$

where each f_k has at least $(2l+2)$ coefficients in each X-equivalence class in $\mathscr{S}$ and f_0 has at least $H(\sigma+1)$ coefficients in each class.

We may suppose that no f_k represents zero properly, since otherwise so would f. Hence by Lemma 4 each $-f_k$ represents a value in an equivalence class not in $\mathscr{S}$. So $-\sum_{k=1}^{D^2dH(\sigma+1)} f_k(X^{(k)})$ represents a form $\sum_{k=1}^{D^2dH} b_k Y_k^d$ with none of the coefficients b_k in any of the classes in $\mathscr{S}$. By the pigeonhole principle, there is an equivalence class containing at least $DH(\sigma+1)$ of the coefficients b_k. Let a representative of this class be γ, so that $-\sum f_k$ represents a form $\gamma \sum_{i=1}^{DH} u_k Y_k^d$ with each $u_k \equiv 1$ (π). Now, we can solve $\sum_{i=1}^{D} y_i^d \equiv -1$ (π); so $\sum f_k$ represents $\gamma \sum_{k=1}^{H(\sigma+1)} u_k' Y_k^d$ with each $u_k' \equiv 1$ (π). Adjoin the class of γ to $\mathscr{S}$, giving a set $\mathscr{S}'$ consisting of $\sigma+1$ X-equivalence classes; then f represents a form f' which has at least $H(\sigma+1, d)$ coefficients in each of the $\sigma+1$ classes in $\mathscr{S}'$.

By the induction hypothesis, f' represents zero properly. So f represents zero properly, as required.

Hence $f = \sum_{i=1}^{s} a_i x_i^d$ represents zero properly whenever $s > (2l+3)^d \times (D^2d)^{d-1}$. This proves our theorem.

This estimate for G may be improved fairly easily, but at present I do not see how to get an estimate which is a power of d, rather than a dth power.

References

[1] B. J. Birch, *Waring's problem in algebraic number fields*, Proc. Cambridge Phil. Soc. 57 (1961), pp. 449-459.

[2] — *Waring's problem for $\mathfrak{p}$-adic number fields*, Acta Arithm. 9 (1964), pp. 169-176.

[3] R. Brauer, *Homogeneous algebraic equations*, Bull. Amer. Math. Soc. (2) 51 (1945), pp. 749-755.

[4] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc., Ser. A, 274 (1963), pp. 443-460.

[5] J. Gray, S.M. *Diagonal forms of prime degree* (University of Notre Dame, thesis, 1958).

[6] D. J. Lewis, *Cubic congruences*, Michigan Math. Journ. 4 (1957), pp. 85-95.

UNIVERSITY OF MANCHESTER

Reçu par la Rédaction le 4. 1. 1964

ACTA ARITHMETICA
IX (1964)

Some remarks on a method of Mordell in the Geometry of Numbers

by

P. MULLENDER (Amsterdam)

1. Some years ago Lekkerkerker [1] gave a short analysis of a method of Mordell in the Geometry of Numbers, by which sometimes an estimate can be obtained for the critical determinant of an n-dimensional star body by reducing the problem to an $(n-1)$-dimensional one. In this note we add a few remarks that may lead to further elucidation of the method.

2. We consider two distance functions F and G, defining two star bodies K_F and K_G, both of the finite type, in an n-dimensional (Euclidean) space X. We suppose there is a group Ω of automorphs of K_F, all having the property that the contragredient transformation is an automorph of K_G, i.e. we suppose there is a group of non-singular $n\times n$-matrices A, such that $F(A.x) = F(x)$ and $G(\tilde{A}.x) = G(x)$ for all $x \epsilon X$, $\tilde{A}$ denoting the transposed inverse of A.

It is not difficult to prove that, if R is the k-dimensional linear subspace of X generated by $k+1$ linearly independent points, including the origin o, of the lattice

$$\Lambda = \{x \mid x = L.u,\ u \epsilon U\},$$

where L denotes a non-singular $n\times n$-matrix and U the set of all points of X with integral coordinates, then the $(n-k)$-dimensional subspace S of X through o and perpendicular to R is generated by $n-k+1$ linearly independent points of the contragredient lattice

$$\tilde{\Lambda} = \{x \mid x = \tilde{L}.u,\ u \epsilon U\},$$

where $\tilde{L}$ is the transposed inverse of L. Further, denoting the k- and $(n-k)$-dimensional lattices $R \cap \Lambda$ and $S \cap \tilde{\Lambda}$ by λ and $\tilde{\lambda}$, respectively, we have for the determinants

$$(1) \qquad d(\Lambda) = \frac{d(\lambda)}{d(\tilde{\lambda})} = \frac{1}{d(\tilde{\Lambda})}.$$