and $r(a)$ for (43b) becomes (say) $r_t(a)$, *the number of representations of* $Q^{(t)} = a$ *in terms of the* $4t$*-tuples of rational integers* $(x_1, \ldots, x_{4t})$. It is given by

$$r_t(a) = -\left(\frac{4t}{B_{2t}}\right) \cdot \frac{\sigma_{2t-1}^{(a)} + (-3)^t \sigma_{2t-1}^{(a/3)}}{1+(-3)^t} \tag{47b}$$

for $t = 1$ and 2, according to Lemma 7.

In the case of $\sqrt{2}$ and $\sqrt{5}$ the rational octenary forms corresponding to (47a) are too complicated for the identity of type (40c) or (41c) to be worth explicit formulation. Of course these rational forms (unlike the algebraic forms) have nonunit determinant.

In order to present the simplest type of identities we ignored some very interesting noneven cases such as the "sum of four squares" in $Q(\sqrt{2})$ and $Q(\sqrt{3})$ where the theta-functions $\theta_Q(1, 1; U, -U)$ and $\theta_Q(1, 1; \varepsilon U, \varepsilon' U)$ satisfy the system (36). A partial treatment of these cases appears in [1], [2] but a more thorough treatment of identities, indeed a treatment embracing a larger number of field types, must wait for a later occasion.

References

[1] H. Cohn, *Decomposition into four integral squares in the fields of* $2^{1/2}$ *and* $3^{1/2}$, Amer. J. Math. 82 (1960), pp. 301-322.

[2] — *Cusp forms arising from Hilbert's modular functions for the field of* $3^{1/2}$, Amer. J. Math. 84 (1962), pp. 283-305.

[3] — and G. Pall, *Sum of four squares in a quadratic ring*, Trans. Amer. Math. Soc. 105 (1962), pp. 536-556.

[4] R. Fueter, *Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen*, Leipzig 1924.

[5] F. Götzky, *Über eine zahlentheoretische Anwendung von Modulfunktionen zweier Veränderlichen*, Math. Ann. 100 (1928), pp. 411-437.

[6] E. Hecke, *Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichungen*, Math. Ann. 112 (1936), pp. 664-699.

[7] B. W. Jones, *The arithmetic theory of quadratic forms*, New York 1950.

[8] H. Maass, *Modulformen und quadratische Formen über dem quadratischen Zahlkörper* $R(\sqrt{5})$, Math. Ann. 118 (1941), pp. 65-84.

[9] — *Quadratische Formen über quadratischen Körpern*, Math. Zeit. 51 (1945), pp. 233-254.

[10] L. J. Mordell, *On Mr. Ramanujan's Empirical Expansions of Modular Functions*, Proc. Cambridge Phil. Soc. 19 (1917), pp. 117-124.

[11] — *The definite quadratic forms in eight variables with determinant unity*, Journal de Mathematiques pures et appliquées 17 (1938), pp. 11-46.

[12] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. 36(1935), pp. 527-606; 37(1936), pp. 230-263; 38(1937), pp. 212-291.

UNIVERSITY OF ARIZONA, TUCSON, U. S. A.

Reçu par la Rédaction le 30. 5. 1963

ACTA ARITHMETICA
IX (1964)

Functions and polynomials $(\mathrm{mod}\, p^n)$*

by

L. Carlitz (Durham, North Carolina)

To Professor L. J. Mordell on his seventy-fifth birthday

1. Let p be a fixed prime and n an integer $\geqslant 1$. Let Z_n denote the ring of integers $(\mathrm{mod}\, p^n)$. By a *function* f over Z_n will be meant a mapping of Z_n into itself; that is, $f(a) \in Z_n$ for all $a \in Z_n$. Two functions f, g over Z_n are *equal* provided

$$f(a) \equiv g(a) (\mathrm{mod}\, p^n)$$

for all $a \in Z_n$.

A *polynomial* $F(x)$ is a function of the type

$$F(x) = a_0 + a_1 x + a_2 x^2 + \ldots \qquad (a_j \in Z_n). \tag{1}$$

When $n = 1$ it is well known that every function over Z_n can be represented as a polynomial. When $n > 1$, however, this is no longer true. For example, the function defined by

$$f(a) = \begin{cases} 0 & (a = 0), \\ 1 & (a \neq 0) \end{cases} \tag{2}$$

cannot be represented as a polynomial. This follows from the observation that for any polynomial $F(x)$ we have

$$F(a+p) \equiv F(a) (\mathrm{mod}\, p); \tag{3}$$

clearly (2) and (3) are not compatible.

The representation (1) is, of course, not unique. When $n = 1$ the representation is unique provided $\deg F(x) < p$. When $n \geqslant 1$, let $F(x)$, $G(x)$ be two polynomials such that

$$F(a) \equiv G(a) (\mathrm{mod}\, p^n) \tag{4}$$

* Supported in part by National Science Foundation grant G16485.

for all $a \in Z_n$. Then

$$H(a) \equiv 0 \pmod{p^n} \qquad (a \in Z_n), \tag{5}$$

where $H(x) = F(x) - G(x)$. If $n \leqslant p$ it is known ([1], p. 22, Th. 27) that every polynomial satisfying (5) is of the form

$$\sum_{k=0}^{n} p^{n-k}(x^p - x)^k f_k(x),$$

where the $f_k(x)$ are polynomials with integral coefficients. If $n > p$ the situation is more complicated.

It is of some interest to find conditions that will guarantee that a given function can be represented as a polynomial. For a polynomial $F(x)$ it follows from (1) that

$$\sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} F(c+s) = \sum_j a_j \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} (c+s)^j.$$

Now

$$\sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} (c+s)^j = 0 \qquad (0 \leqslant j < r)$$

and is divisible by $r!$ when $j \geqslant r$. Let $\mu(r)$ denote the highest power of p that divides $r!$. Then we have

$$\sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} F(c+s) \equiv 0 \pmod{p^{\mu(r)}},$$

where c is an arbitrary integer and $r \geqslant 0$. It follows that

$$\sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} F(c+s) \equiv 0 \pmod{p^{\nu(r)}}, \tag{6}$$

where

$$\nu(r) = \min\bigl(n, \mu(r)\bigr). \tag{7}$$

We shall now prove the following criterion.

THEOREM 1. *The function $f(x)$ over Z_n can be represented by a polynomial over Z_n if and only if*

$$\sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} f(c+s) \equiv 0 \pmod{p^{\nu(r)}} \tag{8}$$

for all $c \in Z_n$ and all $r \geqslant 0$.

Proof. We have already proved the necessity of the condition (8). To prove the sufficiency put

$$\Delta^r f(c) = \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} f(c+s), \tag{9}$$

where $f(c)$ is an arbitrary function over Z_n. Now consider the polynomial

$$F(x) = \sum_{j=0}^{N} \frac{1}{j!} \Delta^j f(0) x(x-1)\dots(x-j+1); \tag{10}$$

the integer N will be chosen presently. Since by hypothesis the coefficient $\Delta^j f(0)/j!$ is integral (mod p), it is evident that $F(x)$ is a polynomial over Z_n. Then for $0 \leqslant c < p^n$ we have

$$\begin{aligned} F(c) &= \sum_{j=0}^{N} \frac{1}{j!} \Delta^j f(0) c(c-1)\dots(c-j+1) \\ &= \sum_{j=0}^{N} \Delta^j f(0) \binom{c}{j} = \sum_{j=0}^{N} \binom{c}{j} \sum_{s=0}^{j} (-1)^{j-s} \binom{j}{s} f(s) \\ &= \sum_{s=0}^{N} \binom{s}{s} f(s) \sum_{j=s}^{N} (-1)^{j-s} \binom{c-s}{j-s}. \end{aligned}$$

If $N \geqslant p^n$, the inner sum vanishes unless $s = c$, so that

$$F(c) = f(c). \tag{11}$$

Since (11) holds for $c = 0, 1, \dots, p^n - 1$, it follows from the definition of equality of functions over Z_n that $f(x)$ is *equal* to the polynomial $F(x)$. This completes the proof of the theorem.

It is evident from the proof that we have proved the following slightly stronger result.

THEOREM 2. *The function $f(x)$ over Z_n can be represented by a polynomial over Z_n if and only if*

$$\Delta^r f(0) \equiv 0 \pmod{p^{\nu(r)}} \tag{12}$$

for $0 \leqslant r < p^n$.

2. Returning to (1), it is easily verified that

$$F(x+kp) \equiv F_0(x) + kpF_1(x) + \dots + (kp)^{n-1} F_{n-1}(x) \pmod{p^n}, \tag{13}$$

where k is an arbitrary integer and the $F_j(x)$ are polynomials with integral coefficients. This suggests the condition

$$f(x+kp) \equiv f_0(x)+kpf_1(x)+\ldots+(kp)^{n-1}f_{n-1}(x) \pmod{p^n}, \tag{14}$$

where k is an arbitrary integer and the $f_j(x)$ are functions over Z_n. We shall prove the following result.

THEOREM 3. *The function $f(x)$ over Z_n can be represented by a polynomial over Z_n if and only if* (14) *is satisfied, where k is an arbitrary integer and the $f_j(x)$ are functions over Z_n.*

It will be convenient to state another parallel result. It follows from (1) that

$$\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}F(x+sp) = \sum_j a_j \sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}(x+sp)^j. \tag{15}$$

We have also

$$\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}(x+sp)^j = \sum_{t=0}^{j}\binom{j}{t}x^{j-t}p^t\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}s^t.$$

We have already observed that the inner sum on the right is divisible by $p^{\mu(r)}$ and vanishes for $t<r$. Hence the right member is divisible by $p^{r+\mu(r)}=p^{\mu(rp)}$ and (15) yields

$$\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}F(x+sp) \equiv 0 \pmod{p^{\nu(rp)}}. \tag{16}$$

This suggests

THEOREM 4. *The function $f(x)$ over Z_n can be represented by a polynomial over Z_n if and only if*

$$\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}f(c+sp) \equiv 0 \pmod{p^{\nu(rp)}} \tag{17}$$

for $0 \leqslant r < p^{n-1}$ and all $c \in Z_n$.

3. We shall now prove the equivalence of Theorems 2 and 4. Put

$$\delta^r f(c) = \sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}f(c+sp). \tag{18}$$

It is easily verified that

$$f(c+sp) = \sum_{j=0}^{s}\binom{s}{j}\delta^j f(c). \tag{19}$$

Then, by (9) and (19),

$$\begin{aligned}\Delta^r f(c) &= \sum_{s,t}(-1)^{r-sp-t}\binom{r}{sp+t}f(c+sp+t) \\ &= \sum_{s,t}(-1)^{r-sp-t}\binom{r}{sp+t}\sum_{j=0}^{s}\binom{s}{j}\delta^j f(c+t) \\ &= \sum_{j,t}(-1)^{r-t}\delta^j f(c+t)\sum_s(-1)^{sp}\binom{r}{sp+t}\binom{s}{j}.\end{aligned} \tag{20}$$

Put

$$S(r,t,j) = \sum_s(-1)^{sp}\binom{r}{sp+t}\binom{s}{j}.$$

Then since

$$j!p^j\binom{s}{j} = \sum_{k=0}^{j}b_k\frac{(sp+t)!}{(sp+t-k)!},$$

where the b_k are integers, it follows that

$$j!p^jS(r,t,j) = \sum_k c_k\frac{r!}{(r-k)!}\sum_s(-1)^{sp}\binom{r-k}{sp+t-k}. \tag{21}$$

Now put

$$U(t,r) = \sum_s(-1)^{sp}\binom{r}{sp+t};$$

then we have

$$\sum_\zeta \zeta^{-t}(1-\zeta)^r = p(-1)^tU(t,r), \tag{22}$$

where the summation is over all pth roots of unity.

Next we recall that in the cyclotomic field $R(e^{2\pi i/p})$, where R is the rational field, we have

$$(p) = (1-\beta)^{p-1} \qquad (\beta = e^{2\pi i/p}).$$

We infer from (22) that $U(t,r)$ is divisible by at least p^E, where

$$E = \begin{cases}\dfrac{r}{p-1}-1 & (p-1 \mid r),\\[2ex] \left[\dfrac{r}{p-1}\right] & (p-1 \nmid r).\end{cases} \tag{23}$$

On the other hand, since

$$\mu(r) = \left[\frac{r}{p}\right] + \left[\frac{r}{p^2}\right] + \ldots < \frac{r}{p-1},$$

it follows that

$$\mu(r) \leqslant \begin{cases} \dfrac{r}{p-1} - 1 & (p-1 \mid r), \\ \left[\dfrac{r}{p-1}\right] & (p-1 \nmid r). \end{cases}$$

Therefore $E \geqslant \mu(r)$.

Returning to (2.1), we see that

$$j!\,p^j S(r,t,j) \equiv 0 \pmod{p^{\mu(r)}}. \tag{24}$$

Now assume that (17) is satisfied, that is

$$\delta^r f(c) \equiv 0 \pmod{p^{\nu(rn)}} \quad (0 \leqslant r < p^{n-1}). \tag{25}$$

Then it follows from (20), (24), (25) that

$$\Delta^r f(c) \equiv 0 \pmod{p^{E'}},$$

where

$$E' = \min_j \{n,\ \mu(jp) - j - \mu(j) + \mu(r)\}.$$

Since $\mu(jp) = j + \mu(p)$, this reduces to $E' = \nu(n)$. Hence (17) implies (12).

To prove the converse we take

$$f(c+sp) = \sum_{j=0}^{sp} \binom{sp}{j} \Delta^j f(c)$$

from which it follows that

$$\begin{aligned} \delta^r f(c) &= \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} \sum_{j=0}^{sp} \binom{sp}{j} \Delta^j f(c) \\ &= \sum_{j=0}^{rp} \Delta^j f(c) \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} \binom{sp}{j}. \end{aligned} \tag{26}$$

Since the inner sum on the extreme right is an rth difference of the polynomial

$$px(px-1)\ldots(px-j+1)/j!,$$

it follows that

$$j! \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} \binom{sp}{j} \equiv 0 \pmod{p^{r+\mu(r)}}.$$

Then assuming that

$$\Delta^j f(c) \equiv 0 \pmod{p^{\nu(j)}}, \tag{27}$$

it is evident, that each term in the extreme right member of (26) is divisible by $p^{\nu(rn)}$. Since (12) implies (27), it follows that (12) implies (17).

We have therefore proved the equivalence of (12) and (17) and so the equivalence of Theorems 2 and 4.

4. We now prove Theorem 3. If we assume that (14) holds we get

$$\delta^r f(c) \equiv \sum_{j=r}^{n-1} p^j f_j(c) \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} s^j \pmod{p^n}.$$

Since the inner sum is divisible by $p^{\mu(r)}$, it is evident that we get

$$\delta^r f(c) \equiv 0 \pmod{p^{\nu(rn)}}.$$

Hence (14) implies (17).

As for the converse, we have already seen that (17) implies (12), which in turn implies that $f(x)$ can be represented by a polynomial. Moreover, it has already been observed that every polynomial satisfies (14). This completes the proof of the equivalence of (14) and (17). Hence we proved Theorem 3.

5. We now give a few simple applications. However we remark first that in applying Theorem 4 it suffices to take $c = 0, 1, \ldots, p-1$. This can be proved as follows. Making use of (18) and (19) we get, for $k \geqslant 0$,

$$\begin{aligned} \delta^r f(c+kp) &= \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} f(c+kp+sp) \\ &= \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} \sum_{j=0}^{k+s} \binom{k+s}{j} \delta^j f(c) \\ &= \sum_{j=0}^{k+r} \delta^j f(c) \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} \binom{k+s}{j} \\ &= \sum_{j=r}^{k+r} \delta^j f(c) \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} \binom{k+s}{j}, \end{aligned}$$

since $\binom{k+s}{j}$ is a polynomial in k of degree r. If we now assume that

$$\delta^j f(c) \equiv 0 \pmod{p^{\nu(jn)}}$$

for some fixed c, it follows at once that

$$\delta^j f(c+kp) \equiv 0 \pmod{p^{\nu(jn)}}$$

for all $k \geqslant 0$. This evidently proves the truth of the assertion made above.

As a first example we take the function $f_1(x)$ defined as follows:

$$f_1(c) = \begin{cases} 1 & (p\nmid c), \\ 0 & (p\mid c). \end{cases} \tag{28}$$

Since

$$\delta^r f_1(c) = 0 \qquad (r \geqslant 1)$$

for all c it is evident that Theorem 4 applies. Indeed, it is easily verified that

$$f_1(x) = x^{p^{n-1}(p-1)}. \tag{29}$$

Next, for p odd, we take

$$f_2(c) = \left(\frac{c}{p}\right), \tag{30}$$

where (c/p) is the Legendre symbol. Again Theorem 4 applies. Indeed we have

$$f_2(x) = x^{p^{n-1}(p-1)/2}. \tag{31}$$

The function $f_3(x)$ defined by

$$f_3(c) = \begin{cases} c & (p\nmid c), \\ 0 & (p\mid c) \end{cases} \tag{32}$$

is closely related to (28). Clearly

$$f_3(x) = x^{p^{n-1}(p-1)+1}. \tag{33}$$

We may also mention the function

$$f_4(c) = \begin{cases} c^{-1} & (p\nmid c), \\ 0 & (p\mid c). \end{cases} \tag{34}$$

Since

$$\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}\frac{1}{c+sp} = \frac{r!\,p^r}{c(c+p)\dots(c+rp)},$$

it is evident that Theorem 4 applies. We find that

$$f_4(x) = x^{p^{n-1}(p-1)-1}, \tag{35}$$

provided $p^n > 4$. The case $p^n = 4$ is evidently covered by (32) and (33).

Incidentally we may apply Theorem 2 or 4 to a polynomial to obtain a congruence. For example, we may mention

$$F(x) = x^{kp^{n-1}(p-1)-k} \tag{36}$$

where $k \geqslant 1$; this may be replaced by the function defined by

$$f(c) = \begin{cases} c^{-k} & (p\nmid c), \\ 0 & (p\mid c). \end{cases} \tag{37}$$

In the above examples we have $f(c) = 0$ whenever $p\mid c$. This is of course not necessary. As an instance we cite the following function:

$$f_5(c) = \begin{cases} 0 & (p\nmid c), \\ 1 & (p\mid c). \end{cases} \tag{38}$$

This evidently satisfies

$$f_5(x) = (1-x^{p-1})^n. \tag{39}$$

Moreover, by comparison with (34), it is clear that

$$f_5(x) = 1-f_1(x), \tag{40}$$

although the polynomial representations are not the same.

The function defined by

$$f_6(c+kp) = c^{p^{n-1}} \qquad (0 \leqslant c < p) \tag{41}$$

satisfies Theorem 4; indeed, we have

$$f_6(x) = x^{p^{n-1}}. \tag{42}$$

A slightly more interesting example is given by

$$f_7(c+kp) = c \qquad (0 \leqslant c < p). \tag{43}$$

More generally we may consider the class of functions over Z_n that satisfy

$$f(c+p) = f(c). \tag{44}$$

Clearly these functions satisfy (17) and therefore admit of polynomial representations. We shall prove the following result.

THEOREM 5. *A function satisfying* (44) *can be represented in the form*

$$f(x) = \sum_{c=0}^{p-1} f(c)\{1-(x-c)^{p-1}\}^n. \tag{45}$$

The proof is simple. The polynomial

$$L_c(x) = \{1-(x-c)^{p-1}\}^{p^{n-1}} \tag{46}$$

satisfies

$$L_c(a) = \begin{cases} 1 & (c \equiv a \pmod p), \\ 0 & (c \not\equiv a \pmod p). \end{cases}$$

Consequently, if we put $F(x) = \sum_{c=0}^{p-1} f(c) L_c(x)$, it is evident that

$$F(a) = f(c) \qquad (a \equiv c \pmod p)$$

and therefore $F(x) = f(x)$.

The polynomial (46) is suggested by the Lagrange interpolation formula. In general, this interpolation formula cannot be employed for functions over Z_n; however in the special case covered by Theorem 5 there is no difficulty.

For the function defined by (43), we evidently have

$$f_7(x) = \sum_{c=0}^{p-1} c L_c(x). \tag{47}$$

We remark that

$$L_a(x) L_b(x) = 0 \quad (a \not\equiv b), \qquad (L_a(x))^2 = L_a(x) \tag{48}$$

exactly as in the case $n = 1$.

It is of some interest to mention the function defined by

$$f(c+kp) = k^2 p \qquad (0 \leqslant c < p). \tag{49}$$

In the first place it is evidently a function over Z_n. Secondly, we have

$$\delta f(c) = p, \qquad \delta^2 f(c) = 2p, \qquad \delta^r f(c) = 0 \quad (r > 2).$$

Thus for $n \geqslant 2$, $p > 2$, $r = 2$, (17) is not satisfied, so that $f(x)$ is not a polynomial. Also for $n > 2$, $p = 2$, $r = 2$, (17) is not satisfied. However, for $n = 2$, $p = 2$, (17) is satisfied and we have $f(x) = x(x-1)$.

6. A few words may be added about functions and polynomials over Z_n in two variables. Functions $f(x, y)$ are defined in the obvious way. A polynomial is a function of the type

$$\sum_{i,j} a_{ij} x^i y^j \qquad (a_{ij} \in Z_n).$$

Corresponding to Theorems 2, 3 and 4 we have the following results.

THEOREM 6. *The function $f(x, y)$ over Z_n can be represented by a polynomial over Z_n if and only if*

$$\Delta_x^r \Delta_y^s f(0, 0) \equiv 0 \pmod{p^E},$$

for $0 \leqslant r < p^n$, $0 \leqslant s < p^n$, where

$$E = \min\big(n, \mu(r) + \mu(s)\big)$$

and

$$\Delta_x^r \Delta_y^s f(0, 0) = \sum_{j=0}^{r} \sum_{k=0}^{s} (-1)^{r+s-j-k} \binom{r}{j} \binom{s}{k} f(j, k).$$

THEOREM 7. *The function $f(x, y)$ over Z_n can be represented by a polynomial over Z_n if and only if*

$$f(x+rp, y+sp) \equiv \sum_{j+k<n} (rp)^j (sp)^k f_{j,k}(x, y) \pmod{p^n},$$

where r, s are arbitrary integers and the $f_{j,k}(x, y)$ are functions over Z_n.

THEOREM 8. *The function $f(x, y)$ over Z_n can be represented by a polynomial over Z_n if and only if*

$$\delta_x^r \delta_y^s f(a, b) \equiv 0 \pmod{p^E} \tag{50}$$

for $0 \leqslant r < p^{n-1}$, $0 \leqslant s < p^{n-1}$ and all $a, b \in Z_n$, where

$$E = \min\big(n, \mu(rp) + \mu(sp)\big)$$

and

$$\delta_x^r \delta_y^s f(a, b) = \sum_{j=0}^{r} \sum_{k=0}^{s} (-1)^{r+s-j-k} \binom{r}{j} \binom{s}{k} f(a+jp, b+kp).$$

It suffices to assume that (50) holds when $0 \leqslant a < p$, $0 \leqslant b < p$.

The proofs of these theorems are exactly like the proofs in the case of a single variable and will be omitted.

Consider a function $f(x, y)$ such that, for every $a \in Z_n$, $f(a, y)$ is a polynomial in y and, for every $b \in Z_n$, $f(x, b)$ is a polynomial in x. It might be supposed that such a function is necessarily a polynomial in x, y. That this is not the case can be seen from the example (compare (49))

$$f(a+jp, b+kp) = jkp, \tag{51}$$

where $0 \leqslant a < p$, $0 \leqslant b < p$ and j, k are arbitrary integers. Then

$$\delta_x \delta_y f(a, b) = f(a+p, b+p) - f(a, b+p) - f(a+p, b) + f(a, b) = p.$$

Thus, for $n \geqslant 2$, $r = 1$, $s = 1$, (50) is not satisfied and therefore $f(x, y)$ is not a polynomial in x, y. However

$$f(a+jp, y) = j\Big\{y - \sum_{b=0}^{p-1} bL_b(y)\Big\},$$

where $L_b(y)$ is defined by (46).

Remark. We note that Rédei and Szele [2] have made a detailed study of the polynomial representation of functions over rings and in particular over Z_n; the polynomials considered are in an enlarged ring.

References

[1] L. E. Dickson, *Introduction to the theory of numbers*, Chicago 1929.

[2] L. Rédei und T. Szele, *Algebraisch-zahlentheoretische Betrachtungen über Ringe. I*, Acta Mathematica 79 (1947), pp. 291-320.

Reçu par la Rédaction 19. 6. 1963

ACTA ARITHMETICA
IX (1964)

On the representation of rational functions as sums of squares

by

J. W. S. Cassels (Cambridge)

To my teacher and friend Professor L. J. Mordell for his 75th birthday in gratitude

Theorem 1. *Let k be any field and denote by $k(x)$ and $k[x]$, respectively, the field of rational functions and the ring of polynomials in a single variable x having coefficients in k. Then any $f \in k[x]$ which is the sum of squares of elements of $k(x)$ is the sum of the same number of squares of elements of $k[x]$.*

What is essentially new in this enunciation is that the same number of squares suffices. Without this condition the result stated has been proved by Artin [1], who adapted a proof by Landau [5] of the fact that every positive define function in $\boldsymbol{Q}[x]$ (where $\boldsymbol{Q}$ is the field of rationals) is the sum of eight squares of elements of $\boldsymbol{Q}[x]$ (cf. also Witt [6] for some related results).

As almost immediate consequences of Theorem 1 we have:

Theorem 2. *Let $d \in k$ and suppose that the characteristic of k is not 2. A necessary and sufficient condition that $x^2 + d$ be the sum of $n > 1$ squares in $k(x)$ is that*

either -1 *is the sum of* $n-1$ *squares of* k
or d *is the sum of* $n-1$ *squares of* k.

Theorem 3. *Let $\boldsymbol{R}$ denote the field of real numbers and let $x_1, \ldots, x_n$ be independent variables over $\boldsymbol{R}$. Then $x_1^2 + \ldots + x_n^2$ is not the sum of $n-1$ squares of elements of $\boldsymbol{R}(x_1, \ldots, x_n)$.*

Theorem 3 answers a problem of Professor N. J. Fine which reached me *via* Professor Mordell and Professor Davenport. The case $n \leqslant 4$ has already been proved by Davenport [4] in another way. I am grateful to him for showing me his manuscript before publication.

Proof of Theorem 1. The proof is essentially an adaption to the "power series case" of Davenport's proof [3] of my theorem [2] that if