p. 452; the first two lines of Lemma 2.4 should read: "If $a_{m+1}(x), \ldots, a_{m+p}(x)$ are fixed (mod $v$), then one can find for each $i$ $(1 \leqslant i \leqslant k)$ exactly one $j(i) \leqslant k$ such that $x(m+p) \in S_i'$ is equivalent".
p. 452, line 6 from bottom should start with "$\geqslant \varepsilon h P\{\ldots$".
p. 453, line 9 should have at the end "(take $a_1 = 1$ and $r = 1$)".
p. 454, line 4 from bottom should read

$$\Delta_{m,p} \leqslant \lambda_5 \Delta_{m+M+n,p-M-n} + C_5 \lambda_5^n .$$

p. 460, lines 2,3 from bottom should read "($\Sigma''$ is over $k$ from 1 to $a_{m+1}(x)$ but includes only those $k$ with $kq_m \leqslant N$)".
p. 464, formula (3.19) should be: $\frac{q_s(x)}{q_n(x)} \frac{1}{(q_n(x)+q_{n-1}(x))}$.
p. 464, line 2 from bottom $a_1(x), \ldots, a_{m+1}(x)$ should be $a_1(x), \ldots, a_{m+2}(x)$.
p. 466, line 3 $A(\eta)\exp(-(m-p)\eta)$ should be $A(\eta)\exp(-(m-p)B(\eta))$.
p. 469, line 7 $C_8 \frac{t}{\log N}$ should be $-C_8 \frac{|t|}{\log N}$.
p. 469, formula (3.31). The sum over $m$ should run from $m = 2p$ to $m = (\tau-\varepsilon)\log N$. This requires corresponding changes on p. 470.

## References


[1] W. Doeblin, *Remarques sur la theorie métrique des fractions continues*, Comp. Math. 7 (1939-40), pp. 353-371.

[2] J. L. Doob, *Asymptotic properties of Markoff transition probabilities*, Trans. Am. Math. Soc. 63 (1948), pp. 393-421.

[3] G. H. Hardy and E. M. Wright, *An introduction to number theory*, Ch. 10, 3rd edition, Oxford, 1954.

[4] Harry Kesten, *Uniform distribution* mod 1, Ann. of Math. 71 (1960), pp. 445-471.

[5] A. Khintchine, *Kettenbrüche*, Part C, Leipzig, 1956.

[6] B. O. Koopman and J. v. Neumann, *Dynamical systems of continuous spectra*, Proc. Nat. Acad. of Sci. 18 (1932), pp. 255-263.

[7] Paul Lévy, *Théorie de l'addition des variables aléatories*, Ch. 9, 2nd ed., Paris, 1954.

[8] P. Szüsz, *Über einen Kusminschen Satz*, Acta Math. Hung. 12 (1961), pp. 447-453.

[9] H. Weyl, *Über die Gleichverteilung von Zahlen mod Eins*, Math. Ann. 77 (1916), pp. 313-352.


CORNELL UNIVERSITY
ITHACA, NEW YORK

*Reçu par la Rédaction le 6. 2. 1962*

ACTA ARITHMETICA
VII (1962)

# Binomial coefficients in an algebraic number field *

by

L. Carlitz (Durham, N. C.)

**1.** Let $K = R(\Theta)$ denote an algebraic number field of degree $n$ over the rationals. Let $\mathfrak{p}$ be a prime ideal of $K$ and let $p$ be the rational prime divisible by $\mathfrak{p}$. Let $K_{\mathfrak{p}}$ denote the set of numbers of $K$ that are integral (mod $\mathfrak{p}$). Put

$$\binom{a}{m} = \frac{a(a-1)\ldots(a-m+1)}{m!}.$$

We shall prove the following result.

Theorem 1. *The binomial coefficients* $\binom{a}{m}$ *are integral* (mod $\mathfrak{p}$) *for all* $a \in K_{\mathfrak{p}}$ *and all* $m \geqslant 1$ *if and only if* $\mathfrak{p}$ *is a prime ideal of the first degree and moreover* $p$ *does not divide the discriminant of* $K$.

Proof. To prove the necessity of the stated conditions suppose first that $\mathfrak{p}$ is of degree $f > 1$. Then the residue class ring $K_{\mathfrak{p}}/\mathfrak{p}$ is a finite field of order $p^f$. Since $f > 1$ there exists a number $a \in K_{\mathfrak{p}}$ such that

$$a \not\equiv r \pmod{\mathfrak{p}} \quad (r = 0, 1, \ldots, p-1).$$

Therefore the binomial coefficient $\binom{a}{p}$ is not integral (mod $\mathfrak{p}$).

Next let $\mathfrak{p}$ be of the first degree but let $p$ divide the discriminant of $K$. Then by Dedekind's theorem on discriminantal divisors, $\mathfrak{p}^2 | p$. Also there exists an integer $a$ of $K$ such that ([3], p. 97, Theorem 74]

$$(a, p) = \mathfrak{p}. \tag{1.1}$$

Since $\mathfrak{p}$ is of the first degree, the numbers

$$a, a-1, \ldots, a-p+1$$

constitute a complete residue system (mod $\mathfrak{p}$). Clearly only the first of these numbers is divisible by $\mathfrak{p}$. Therefore by (1.1) the product

$$a(a-1)\ldots(a-p+1)$$

* Supported in part by National Science Foundation grant G 16485.

is divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$. It follows that $\binom{a}{p}$ is not integral $(\mathrm{mod}\,\mathfrak{p})$. This completes the proof of the necessity.

To prove the sufficiency, assume that $\mathfrak{p}$ is of the first degree and that $\mathfrak{p}^2 \nmid p$. Then for $r \geqslant 1$ the numbers

$$0, 1, 2, \ldots, p^r - 1$$

form a complete residue system $(\mathrm{mod}\,\mathfrak{p}^r)$. For if two are congruent $(\mathrm{mod}\,\mathfrak{p}^r)$ we should have $\mathfrak{p}^r | t$, where $1 \leqslant t < p^r$. If $p^s$ is the highest power of $p$ dividing $t$ it follows that $\mathfrak{p}^r | p^s$; since $\mathfrak{p}^2 \nmid p$ we get $r \leqslant s$ which is evidently impossible.

If $a$ is an arbitrary number of $K_\mathfrak{p}$ it follows from the above that the numbers

$$a, a-1, \ldots, a-p^r+1$$

constitute a complete residue system $(\mathrm{mod}\,\mathfrak{p}^r)$. Thus in the sequence

$$a, a-1, \ldots, a-m+1$$

there are $[m/p]$ multiples of $\mathfrak{p}$, $[m/p^2]$ multiples of $\mathfrak{p}^2$, and so on. Therefore the product

$$a(a-1)\ldots(a-m+1)$$

is divisible by $\mathfrak{p}^w$, where

$$w = \left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \ldots$$

Since $m!$ is divisible by exactly $p^w$ and therefore by exactly $\mathfrak{p}^w$, it follows that $\binom{a}{m}$ is integral $(\mathrm{mod}\,\mathfrak{p})$.

As a corollary of Theorem 1 we have

THEOREM 2. *Let $p$ be a rational prime and let $K_p$ denote the set of numbers of $K$ that are integral* $(\mathrm{mod}\,p)$. *Then the binomial coefficients* $\binom{a}{m}$ *are integral* $(\mathrm{mod}\,p)$ *for all $a \in K_p$ and all $m \geqslant 1$ if and only if*

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n \tag{1.2}$$

*where the $\mathfrak{p}_j$ are distinct prime ideals* (*of the first degree*) *of $K$.*

To prove the theorem let

$$(p) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r} \tag{1.3}$$

be the prime ideal decomposition of $(p)$ in $K$, where the $\mathfrak{p}_j$ are distinct prime ideals. Then by Theorem 1, $\binom{a}{m}$ is integral $(\mathrm{mod}\,\mathfrak{p}_j)$ for all $a \in K_{\mathfrak{p}_j}$ and all $m \geqslant 1$ if and only if $\mathfrak{p}_j$ is of the first degree and $e_j = 1$. Since $K_p$ is the intersection of all $K_{\mathfrak{p}_j}$ it follows that $\binom{a}{m}$ is integral for all $a \in K_p$ and all $m \geqslant 1$ if and only if all $\mathfrak{p}_j$ are of the first degree and all $e_j = 1$. Thus (1.3) reduces to (1.2).

For a special case of Theorem 2 see [1], p. 586, Lemma.



**2.** As in Theorem 1 let $\mathfrak{p}$ be a prime ideal of the first degree such that $\mathfrak{p} \nmid p$. We shall determine the residue $(\mathrm{mod}\,\mathfrak{p})$ of $\binom{a}{m}$. Since, as we have seen above, the numbers

$$0, 1, 2, \ldots, p^N - 1$$

constitute a complete residue system $(\mathrm{mod}\,\mathfrak{p}^N)$ we may put

$$a \equiv c_0 + c_1 p + \ldots + c_{N-1} p^{N-1} \; (\mathrm{mod}\,\mathfrak{p}^N), \tag{2.1}$$

where the $c_j$ are rational integers, $0 \leqslant c_j < p$. Put

$$c = c_0 + c_1 p + \ldots + c_{N-1} p^{N-1}, \tag{2.2}$$

so that by (2.1)

$$a = c + \delta, \qquad \mathfrak{p}^N | \delta. \tag{2.3}$$

It follows from (2.3) that

$$a(a-1)\ldots(a-m+1) \equiv c(c-1)\ldots(c-m+1) \; (\mathrm{mod}\,\mathfrak{p}^N), \tag{2.4}$$

where $m$ is an arbitrary integer $\geqslant 1$. Put

$$m = m_0 + m_1 p + \ldots + m_{r-1} p^{r-1} \qquad (0 \leqslant m_j < p)$$

$$\nu(m) = \left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \ldots + \left[\frac{m}{p^{r-1}}\right].$$

Then (2.4) implies

$$\binom{a}{m} \equiv \binom{c}{m} \; (\mathrm{mod}\,\mathfrak{p}^{N-\nu(m)}). \tag{2.5}$$

We now suppose that $N > \nu(m)$ and recall the theorem due to Lucas ([2], p. 271) that, in the present notation,

$$\binom{c}{m} \equiv \binom{c_0}{m_0}\binom{c_1}{m_1}\ldots\binom{c_{r-1}}{m_{r-1}} \; (\mathrm{mod}\,p). \tag{2.6}$$

It should be observed that if in (2.1) $N$ is replaced by $N+1$, the coefficients $c_0, c_1, \ldots, c_{N-1}$ do not change. We therefore get from (2.5) and (2.6)

$$\binom{a}{m} \equiv \binom{c_0}{m_0}\binom{c_1}{m_1}\ldots\binom{c_{r+1}}{m_{r-1}} \; (\mathrm{mod}\,\mathfrak{p}). \tag{2.7}$$

We may state

THEOREM 3. *Let $\mathfrak{p}$ be a prime ideal of the first degree such that $\mathfrak{p}^2 \nmid p$. If*

$$m = m_0 + m_1 p + \ldots + m_{r-1} p^{r-1} \qquad (0 \leqslant m_j < p) \tag{2.8}$$

*and we put*

$$a \equiv c_0 + c_1 p + \ldots + c_{r-1} p^{r-1} \; (\mathrm{mod}\,\mathfrak{p}^r) \qquad (0 \leqslant c_j < p), \tag{2.9}$$

*where $\alpha$ is an arbitrary number $\epsilon K_{\mathfrak{p}}$, then* (2.7) *holds. In particular* $\binom{\alpha}{m}$ *is prime to* $\mathfrak{p}$ *if and only if*

$$m_j \leqslant c_j \quad (j = 0, 1, \ldots, r-1)\,. \tag{2.10}$$

As a corollary we have the following result supplementary to Theorem 2.

THEOREM 4. *Let*

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n\,,$$

*where the* $\mathfrak{p}_j$, *are distinct prime ideals of the first degree of* $K$. *Also let*

$$\alpha \equiv c_{k0} + c_{k1}p + \ldots + c_{k,r-1}p^{r-1} \pmod{\mathfrak{p}_k^r} \quad (0 \leqslant c_{kj} < p)\,. \tag{2.11}$$

*Then* $\binom{\alpha}{m}$ *is prime to* $p$ *if and only if*

$$m_j \leqslant \min_{1<k<n} c_{kj} \quad (j = 0, 1, \ldots, r-1)\,,$$

*where*

$$m = m_0 + m_1 p + \ldots + m_{r-1}p^{r-1} \quad (0 \leqslant m_j < p)\,.$$

**3.** It is evident from the proof of Theorem 3 that if $\alpha \equiv \beta \pmod{\mathfrak{p}^r}$ then

$$\binom{\alpha}{m} \equiv \binom{\beta}{m} \pmod{\mathfrak{p}} \tag{3.1}$$

provided $m < p^r$. To get a more general result we require the following

LEMMA. *Let $a, b$ be rational integers such that*

$$a \equiv b \pmod{p^{r+s}} \quad (r \geqslant 1,\ s \geqslant 0)\,.$$

*Then*

$$\binom{a}{m} \equiv \binom{b}{m} \pmod{p^{s+1}} \quad (1 \leqslant m < p^r)\,. \tag{3.2}$$

Proof. Put $a = b + c$ and consider

$$(1+x)^a = (1+x)^b (1+x)^c\,.$$

Clearly (3.2) is an immediate consequence of

$$\binom{c}{m} \equiv 0 \pmod{p^{s+1}} \quad (1 \leqslant m < p^r)\,. \tag{3.3}$$

Since

$$\binom{c}{m} = \frac{c}{m}\binom{c-1}{m-1}$$

and

$$\frac{c}{m} \equiv 0 \pmod{p^{s+1}} \quad (1 \leqslant m < p^r)\,,$$

(3.3) follows at once.

Now let $\alpha, \beta \,\epsilon\, K_{\mathfrak{p}}$, where $\mathfrak{p}$ is of the first degree and $\mathfrak{p}^2 \nmid p$. Then we may put

$$\alpha \equiv a_0 + a_1 p + \ldots + a_{N-1}p^{N-1} \pmod{\mathfrak{p}^N}\,,$$
$$\beta \equiv b_0 + b_1 p + \ldots + b_{N-1}p^{N-1} \pmod{\mathfrak{p}^N}\,,$$



where $0 \leqslant a_j < p$, $0 \leqslant b_j < p$ and $N$ is at our disposal. We assume that

$$\alpha \equiv \beta \pmod{\mathfrak{p}^{r+s}} \tag{3.4}$$

and take $N > r+s$. It follows that

$$a_j = b_j \quad (0 \leqslant j < r+s)\,.$$

Put

$$a = a_0 + a_1 p + \ldots + a_{N-1}p^{N-1}\,,$$
$$b = b_0 + b_1 p + \ldots + b_{N-1}p^{N-1}\,,$$
$$c = a_0 + a_1 p + \ldots + a_{r+s-1}p^{r+s-1}\,,$$

so that

$$\alpha \equiv a\,, \quad \beta \equiv b \pmod{\mathfrak{p}^N}\,, \tag{3.5}$$

$$a \equiv b \equiv c \pmod{p^{r+s}}\,. \tag{3.6}$$

For sufficiently large $N$, it follows from (3.5) that

$$\binom{\alpha}{m} \equiv \binom{a}{m}\,, \quad \binom{\beta}{m} \equiv \binom{b}{m} \pmod{\mathfrak{p}^{s+1}}\,. \tag{3.7}$$

On the other hand, it follows from (3.6) and the Lemma that

$$\binom{a}{m} \equiv \binom{b}{m} \pmod{p^{s+1}}\,. \tag{3.8}$$

Combining (3.7) and (3.8) we get

$$\binom{\alpha}{m} \equiv \binom{\beta}{m} \pmod{\mathfrak{p}^{s+1}}\,.$$

This proves

THEOREM 5. *Let $\mathfrak{p}$ be a prime ideal of the first degree such that $\mathfrak{p}^2 \nmid p$. Let $\alpha, \beta$ be numbers of $K_{\mathfrak{p}}$ such that*

$$\alpha \equiv \beta \pmod{\mathfrak{p}^{r+s}}\,,$$

*where $r \geqslant 1$, $s \geqslant 0$. Then*

$$\binom{\alpha}{m} \equiv \binom{\beta}{m} \pmod{\mathfrak{p}^{s+1}}$$

*for all $m < p^r$.*

THEOREM 6. *Let*

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n$$

*where the $\mathfrak{p}_j$ are distinct prime ideals of the first degree of $K$. Let $\alpha, \beta$ be numbers of $K_p$ such that*

$$\alpha \equiv \beta \pmod{p^{r+s}}\,,$$

*where $r \geqslant 1$, $s \geqslant 0$. Then*

$$\binom{\alpha}{m} \equiv \binom{\beta}{m} \pmod{p^{s+1}}$$

*for all $m < p^r$.*

**4.** If again $\mathfrak{p}$ is of the first degree and $\mathfrak{p}^2 \nmid p$ we can determine the highest power of $\mathfrak{p}$ dividing $\binom{\alpha}{m}$ in the following way. Put

$$m = m_0 + m_1 p + \ldots + m_{r-1} p^{r-1} \qquad (0 \leqslant m_j < p)$$

and let $\alpha \equiv a \pmod{\mathfrak{p}^N}$, where

$$a = a_0 + a_1 p + \ldots + a_{N-1} p^{N-1} \qquad (0 \leqslant a_j < p) .$$

For $N$ sufficiently large it is clear that $\binom{\alpha}{m}$ and $\binom{a}{m}$ are divisible by the same powers of $\mathfrak{p}$; moreover for $\binom{\alpha}{m}$ this is the same as the highest power of $p$ dividing $\binom{a}{m}$.

Now by Kummer's rule ([2], p. 270) the highest power of $p$ dividing

$$\binom{b+c}{c} \qquad (b \geqslant 0, c \geqslant 0) ,$$

where

$$b = b_0 + b_1 p + \ldots + b_s p^s \qquad (0 \leqslant b_j < p) ,$$
$$c = c_0 + c_1 p + \ldots + c_s p^s \qquad (0 \leqslant c_j < p) ,$$

is determined as follows. Let

$$(4.1) \qquad \begin{aligned} b_0 + c_0 &= a_0 + e_0 p , \\ b_1 + c_1 + e_0 &= a_1 + e_1 p , \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{s-1} + c_{s-1} + e_{s-2} &= a_{s-1} + e_{s-1} p , \\ b_s + c_s + e_{s-1} &= a_s + e_s p , \end{aligned}$$

where each $e = 0$ or $1$. Then $\binom{b+c}{b}$ is divisible by exactly $p^e$, where

$$e = e_0 + e_1 + \ldots + e_s .$$

We now put

$$(4.2) \qquad a^{(k)} = a_0 + a_1 p + \ldots + a_k p^k \qquad (k = 0, 1, 2, \ldots) ,$$

so that

$$\alpha \equiv a^{(k)} \pmod{\mathfrak{p}^{k+1}} ,$$

and apply Kummer's rule to

$$(4.3) \qquad \binom{a^{(k)}}{m} \qquad (k = r, r+1, \ldots) .$$

We assume that $m \leqslant a^{(r)}$. It follows that all the binomial coefficients (4.3) are divisible by exactly the same power of $p$, for clearly there is no additional "carrying" when $k > r$.

This proves

THEOREM 7. *Let $\mathfrak{p}$ be a prime ideal of the first degree such that $\mathfrak{p}^2 \nmid p$ and let*

$$m = m_0 + m_1 p + \ldots + m_{r-1} p^{r-1} \qquad (0 \leqslant m_j < p) ,$$
$$\alpha \equiv a_0 + a_1 p + \ldots + a_r p^r \pmod{\mathfrak{p}^{r-1}} \qquad (0 \leqslant a_j < p) .$$



*Moreover assume that*

$$m \leqslant a = a_0 + a_1 p + \ldots + a_r p^r .$$

*Then the highest power of $\mathfrak{p}$ dividing $\binom{\alpha}{m}$ is the same as the highest power of $p$ dividing $\binom{a}{m}$. The latter power can be found by means of Kummer's rule* (4.1).

THEOREM 8. *Let*

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n ,$$

*where the $\mathfrak{p}_j$ are distinct prime ideals of the first degree. Let*

$$m = m_0 + m_1 p + \ldots + m_{r-1} p^{r-1} \qquad (0 \leqslant m_j < p) ,$$
$$\alpha \equiv c_k \equiv c_{k0} + c_{k1} p + \ldots + c_{k,r} p^r \pmod{\mathfrak{p}_k^{r+1}} \qquad (0 \leqslant c_{kj} < p;\ k = 1, \ldots, n) .$$

*Let $p^{e_k}$ denote the highest power of $p$ dividing $\binom{c_k}{m}$ and assume that*

$$m \leqslant \min(c_1, \ldots, c_k) .$$

*Then the binomial coefficient $\binom{\alpha}{m}$ is divisible by exactly $p^e$, where*

$$e = \min(e_1, \ldots, e_k) .$$

Remark. The hypothesis $m \leqslant a$ occurring in Theorem 7 is necessary for the application of Kummer's rule. A like remark applies to the hypothesis

$$m \leqslant \min(c_1, \ldots, c_n)$$

in Theorem 8.

As a corollary of the last two theorems we have

THEOREM 9. *Let $\mathfrak{p}$ be a prime ideal of the first degree such that $\mathfrak{p}^2 \nmid p$ and let $m < p^r$. Then if*

$$\alpha \equiv \beta \equiv a \pmod{\mathfrak{p}^{r+1}} ,$$

*where*

$$a = a_0 + a_1 p + \ldots + a_r p^r \qquad (0 \leqslant a_j < p)$$

*and in addition $m \leqslant a$ it follows that $\binom{\alpha}{m}$ and $\binom{\beta}{m}$ are divisible by exactly the same power of $\mathfrak{p}$.*

*If moreover*

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n ,$$

*where the $\mathfrak{p}_j$ are distinct prime ideals of the first degree, then $\binom{\alpha}{m}$ and $\binom{\beta}{m}$ are divisible by exactly the same power of $p$.*

Remark. As in Theorems 7 and 8 the condition $m \leqslant a$ is necessary for Kummer's rule.

### References


[1] L. Carlitz, *Some arithmetic properties of a special sequence of polynomials*, Duke Math. Journ. 26 (1959), pp. 583-590.

[2] L. E. Dickson, *History of the theory of numbers*, vol. 1, Washington 1919.

[3] E. Hecke, *Theorie der algebraischen Zahlen*, Leipzig 1923.


*Reçu par la Rédaction le 12. 2. 1962*

ACTA ARITHMETICA
VII (1962)

# Solvability of certain equations in a finite field *

by

L. CARLITZ (Durham, N. C.)

**1.** Let $q = p^n$, where $p$ is a prime, and let $GF(q)$ denote the finite field of order $q$. Schwarz [4] has given an elegant proof of the following theorem. *If $k \mid p-1$, if $a_1, \ldots, a_k$ are non-zero numbers of $GF(q)$ and $a$ is an arbitrary number of the field, then the equation*

$$a_1x_1^k + \ldots + a_kx_k^k = a$$

*has at least one solution in the field.*

Using the same method, the writer [2] has proved the following theorems.

THEOREM 1. *Let $k \mid p-1$ and let $a_1, \ldots, a_k$ be non-zero numbers of $GF(q)$. Let $g(x_1, \ldots, x_k)$ be an arbitrary polynomial with coefficients in $GF(q)$ of degree less than $k$. Then the equation*

$$a_1x_1^k + \ldots + a_kx_k^k = g(x_1, \ldots, x_k)$$

*has at least one solution in the field.*

THEOREM 2. *If $f(x_1, \ldots, x_k)$ is homogeneous of degree $k$ while $g(x_1, \ldots, x_k)$ is arbitrary of degree less than $k$, and*

$$\sum_{x_1, \ldots, x_k \in GF(q)} \{f(x_1, \ldots, x_k)\}^{q-1} \neq 0\,, \tag{1.1}$$

*then the equation*

$$f(x_1, \ldots, x_k) = g(x_1, \ldots, x_k) \tag{1.2}$$

*has at least one solution in the field. Alternatively the condition* (1.1) *may be replaced by the equivalent statement that the number of solutions of the equation*

$$f(x_1, \ldots, x_k) = 0 \tag{1.3}$$

*is not divisible by $p$.*

By the degree of $g(x_1, \ldots, x_k)$ is understood the total degree.

* Supported in part by National Science Foundation grant G 16485.