intersected by every set of parallel planes in an isothermal family, besides the obvious cases of spheres and and planes, are the minimal surfaces.

This paper was presented before the American Mathematical Society, in April, 1944.


---

**NEW TYPES OF RELATIONS IN FINITE FIELD THEORY**

**BY H. S. VANDIVER**

**DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF TEXAS**

Communicated November 27, 1944

In two other recent papers we developed methods which led to several new results in finite field theory, with particular application to ordinary congruences involving rational integers. In the present article we pursue these methods much further, obtaining various new kinds of relations.

The results just referred to gave criteria involving binomial coefficients for the number of roots of an equation in a finite field. To reduce these expressions to simpler forms in order to give more convenient criteria as to the number of roots, it seems necessary to go into considerations involving binomial coefficients which have not been heretofore studied, and so far we can only use these expressions to supply this information in comparatively few cases, some of which will be discussed elsewhere. At present we shall look at the situation from another angle. It is possible to apply the criteria to certain equations where we know in advance the number of roots or some properties of them. When this is done it turns out to be a fruitful method for finding relations of an entirely new type in number theory.

As one example of this, we obtain immediately from the statement of Theorem II of the first paper and the remarks just preceding it, the result that the least residue, positive or zero, of
modulo $p$, is \leq c$ for $p$ any prime of the form $1 + cm$; $m$ odd; $a$ and $b$
being any integers such that $(ab, p) = 1$. In this connection we note the
remarks of H. J. S. Smith$^2$ in connection with a congruence due to Gauss,
which states that if $p = 4n + 1 = h^2 + k^2$ is a prime then
\[ h \equiv \pm \frac{(2n)!}{2(n!)^2} \pmod p. \] (2)

Smith called this a remarkable relation since $h$ may be determined directly
by finding the least residue, in absolute value, of the right-hand member
and this must be also < $\sqrt{p}$. The result concerning $A$ in (1) is some-
what analogous.

1. We now note, as did Cipolla,$^4$ that we may introduce functions in-
volving the roots of a certain congruence aside from merely the number of
them.

For example, consider the expression,
\[ N_r = \sum (x^r - x'^r)^k(x^n - 1), \] (3)
where the summation extends over all distinct elements $x, x' \neq 0$, of a finite
field $F(p^n)$. For the values $x_1$ of $x$ such that $f(x_1) = 0$, this expression re-
duces to $x_1'$, and for an $x$ not an $x_1$, it vanishes in the field.

Hence
\[ N_r = \sum x_1' \]
in $F(p^n)$ where the summation extends over all distinct roots $x$, of $f(x) = 0$.
The relation (3) gives, if $r \not\equiv 0 \pmod {p^n - 1}$ and
\[ (f(x))^k(x^n - 1) = C_0 + C + C_2x^2 + \ldots; \]
\[ N_r = C_1 + C_1 + s + C_1 + 2s + \ldots, \] (4)
where $t = p^n - 1 - r$; $s = p^n - 1$,
and
\[ N_r + 1 = C_2 + C_2s \ldots, \] (5)
for $r \equiv 0 \pmod s$. For the latter case $N_r$ equals, in the field, the number of
roots of $f(x) = 0$. We shall find (4) convenient for further investigations.

From the point of view we are now employing, we shall find use also for
the expression
\[ \sum (x'^r f(x)^d - x'^r f(x)^k(x^n - 1) + d), \] (6)
where the summation extends over all distinct elements \( \not= 0 \) of \( F(p^n) \) which contains (3), and \( d > 0 \). This function obviously reduces to zero in the field.

We now examine the relation
\[
ax^m + 1 = 0; \quad p^n - 1 = mc;
\] (7)
and use the form (3) which gives in this case
\[
N_r = \sum (x^m - x^m (ax^m + 1)^{k(p^n - 1)}),
\] (8)
where the summation extends over all distinct values \( p \) such that \( p^c = 1 \) if we set \( p^{-1} \) in lieu of \( x^m \).

Reducing (8) we obtain for \( x^m = p^{-1} \),
\[
\sum \rho^{-r} - \sum \rho \sum_{t=0}^{k(p^n - 1)} \binom{k(p^n - 1)}{s} a^s \rho^{s-r}
\]
or
\[
- \sum \rho \sum_{t=1}^{k(p^n - 1)} \binom{k(p^n - 1)}{s} a^s \rho^{s-r}.
\]
Summation as to \( \rho \) gives
\[
-c \sum_t \binom{k(p^n - 1)}{t} a^t,
\] (9)
where \( t \) ranges over the integers in the set 1, 2, \ldots \( k(p^n - 1) \) such that \( t \equiv r \) (mod \( c \)). We know from (7) that if \((-a)^c = 1\) then there is just one value \( x^m \) which satisfies the equation, and if \((-a)^c \not= 1\) there is none, that is, \( N_r = (-1)^ca^r \) or 0 in (8), for \( r > 0 \). Assume also \( r < c \). This gives
\[
c \sum_t \binom{k(p^n - 1)}{t} a^t = (-1)^{r+1} a^r \text{ or } 0,
\] (10)
according as \((-a)^c = 1\) or \((-a)^c \not= 1\), and if \( t = 0 \), then we must replace \((-1)^r a^r \) by \(-1\) in this relation.

Now take the expression (6), and set \( ax^m + 1 \) for \( f(x) \) and \((-r)\) for \( r \) Expansion gives, if \( p^n - 1 > d > 0 \),
\[
c \sum \binom{d}{t} a^t - \sum \left( d + (p^n - 1)k \right) a^t = 0,
\]
or
\[
\sum t \left( d + (p^n - 1)k \right) a^t = \sum \binom{d}{t} a^t,
\] (11)
t_1 ranging over all the values in the set 0, 1, 2, \ldots, \( d \), such that \( t_1 \equiv r \) (mod \( c \)), and \( t \) ranges over all the values in the set 0, 1, 2, \ldots, \( k(p^n - 1) \) such
that \( t \equiv r \pmod{c} \). For \( n = 1, a = 1, c = p^n - 1 \) and \( d \not\equiv 0 \pmod{p^n - 1} \) the relation (11) gives

\[
\sum_{i} \left( \frac{d + (p^n - 1)k}{t} \right) \equiv \left( \frac{d}{t} \right) \pmod{p},
\]

if \( d < p^n - 1 \), which is due to the writer, \(^4\) and for \( n = 1, t \equiv 0 \pmod{(p - 1)} \) to Bachmann. \(^5\)

Now set

\[
\left( \frac{v}{w} \right) = 0,
\]

for \( w > v \), then relations (10) and (11) give the

**Theorem I.** If \( p^n - 1 = mc, p \) prime, \( k > 0, a \) is any element, \( \not\equiv 0 \), of a finite field \( F(p^n) \) then for \( 0 < r < c \),

\[
\sum_{s=0}^{\infty} c \left( \frac{k(p^n - 1)}{r + cs} \right) a^{cs} = (-1)^{r+1} a^r \text{ or } 0,
\]

according as \( (-a)^e = 1 \), or \( (-a)^e \not\equiv 1 \), also

\[
\sum_{k=1}^{\infty} c \left( \frac{k(p^n - 1)}{ch} \right) a^{ch} = -1 \text{ or } 0,
\]

with the same conditions on \( a \).

For \( d > 0, 0 \leq r < c \), then

\[
\sum_{s=0}^{\infty} \left( \frac{d + (p^n - 1)k}{r + cs} \right) a^{cs} \equiv \sum_{s=0}^{\infty} \left( \frac{d}{r + cs} \right) a^{cs}.
\]

2. To obtain certain other results we shall find it convenient here to introduce in the finite field of residue classes of a prime ideal \( (p) \) where \( p \) a primitive root of a prime \( l \) and use the algebraic field defined by a primitive \( l \)th root of unity designated by \( \zeta \). The ideal \( (p) \) is a prime ideal in said field. Set \( p^{l-1} - 1 = lc \). Then if \( a \) is prime to \( p \) and also \( a + 1 \not\equiv 0 \pmod{p} \), then \( 1 + a\zeta \) is also prime to \( p \) and

\[
(1 + a\zeta)^r \equiv \zeta^k \pmod{p},
\]

for some \( k, 0 \leq k < l \).

Expand the left hand member and collect powers of \( \zeta \), then the result may be written

\[
A_0 + A_1\zeta + \ldots + A_{l-1}\zeta^{l-1} \equiv 0 \pmod{p}.
\]

We note that this congruence also holds if we set \( \zeta^2, \zeta^3 \ldots, \zeta^{l-1} \) in lieu of \( \zeta \). Then we also note that

\[
A_0 + A_1 + \ldots + A_{l-1} \equiv 0,
\]
since \( c \) is divisible by \( (p - 1) \) and \( a + 1 \not\equiv 0 \pmod{p} \). The relations (15) and (16) after making the substitutions of the various powers of \( \zeta \) already indicated give \( l \) congruences from which we may eliminate the \( A \)'s since the determinant formed by the \( \zeta \)'s is an alternant which is prime to \( p \). Hence

\[
A_i \equiv 0; \quad i = 0, 1, \ldots, l - 1.
\]

Using the actual values of the \( A \)'s we have

\[
\left( \binom{cr}{k} \right) a^k + \left( \binom{cr}{k+l} \right) a^{k+l} + \ldots \equiv 1 \pmod{p},
\]

and since \( a \not\equiv 0 \pmod{p} \),

\[
\left( \binom{cr}{m} \right) + \left( \binom{cr}{km+l} \right) a^l + \ldots \equiv 0 \pmod{p},
\]

for \( m \not\equiv k \).

These give the

**Theorem II.** If \( p \) is a prime, and also a primitive root of a prime \( l \), with \( p^{l-1} - 1 = lc \), and \( r \) is any integer \( > 0 \), \( a \) is an integer with \( (a(a + 1), p) = 1 \), then for some \( k \) in the set \( 0, 1, \ldots, l - 1 \), we have

\[
\sum_{s=0}^{\infty} \left( \binom{cr}{k+sl} \right) a^{k+sl} \equiv 1 \pmod{p},
\]

and for any \( m \) in the set \( 0, 1, \ldots, l - 1 \) with \( m \not\equiv k \), we have

\[
\sum_{s=0}^{\infty} \left( \binom{cr}{m+sl} \right) a^{sl} \equiv 0 \pmod{p}.
\]

---

1 These Proceedings, 30, 362-367, 368-370 (1944).
3 Cipolla, Periodico. di Mat., 22, 36-41 (1907).
5 Bachmann, Niedere Zahlentheorie, II, 46 (1910).