angle is described as a something that is attached to the vertex of a triangle, although it is shown how angles may be added, multiplied or divided, this proves nothing as to the actual magnitude of angles. The angles of a spherical triangle are also attached to the vertices and can be added, multiplied or divided in a similar way, but their actual magnitudes are different from the similar angles in a space of two dimensions. Attention ought to be directed to the fact that saying the angle is included between the sides of the triangle which come together and form the vertex adds nothing to the determination of the term "angle."

As a last point in criticism, many authors on geometry introduce misconceptions and misapprehensions into the matter by employing the concepts of the next higher dimension in a discussion which ought to be exclusively in terms belonging to the dimension dealt with. The student should be warned that lines, either straight or curved, have no existence in a space of one dimension, and that planes and curved surfaces do not exist in a space of two dimensions. This would put an end to the talk about a geometry of two dimensions on the surface of a sphere.

ON HIGHER CONGRUENCES AND MODULAR INVARIANTS.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, February 29, 1908.)

1. THE object of this paper is to give a two-fold generalization of Hurwitz's* explicit formula for the number of integral roots of a given congruence modulo p, p being prime. On the one hand, we may derive an equally simple formula which gives, apart from a multiple of p, the number of the roots of a specified order ($\leqq t$) of irrationality; viz., the roots belonging to the Galois field of order p^t. On the other hand, the problem may, without loss of simplicity, be further generalized †

* *Archiv der Math. u. Physik* (3), vol. 5 (1903), p. 17.

† Other generalizations of theoretical importance, but not leading readily to explicit expressions in terms of the coefficients, are given by H. Kühne, *Archiv der Math. u. Physik*, vol. 6 (1904), p. 174.

by replacing the initial field of integers modulo p by an arbitrary Galois field, $GF[p^n]$.

From his formula Hurwitz deduces an (absolute) invariant * of degree $p-1$ of the general binary form under linear transformations taken modulo p. He states that one of the fundamental questions in the theory of modular invariants is "die Frage der Endlichkeit": whether or not all the invariants can be expressed as rational integral functions with integral coefficients of a finite number of the invariants. Emphasizing the difficulty of this question, he answers it only for a special case. As a matter of fact, this question is trivial for modular invariants, since any polynomial in $a_1, \cdots, a_r$ with integral coefficients is congruent modulo p to a polynomial in which the exponent of each a_i is at most $p-1$ (in view of Fermat's theorem $a^p \equiv a$).

2. Consider an equation, with coefficients in any given Galois field $GF[p^n]$ of order p^n,

$$f(x) \equiv a_0 + a_1 x + \cdots + a_r x^r = 0. \tag{1}$$

Let N denote the number of its roots, different from zero, which belong to the $GF[p^{nm}]$. For brevity, set $P = p^{nm}$. Then N is the number of the vanishing expressions $f(\xi)$, where ξ ranges over the $P-1$ marks $\neq 0$ of the $GF[P]$. In that field,

$$1 - k^{P-1} = \begin{cases} 1 \text{ if } k = 0, \\ 0 \text{ if } k \neq 0. \end{cases}$$

Hence $N \equiv N^* \pmod{p}$, where

$$N^* = \sum_{\xi} \{1 - [f(\xi)]^{P-1}\} \equiv -1 - \sum_{\xi} [f(\xi)]^{P-1}.$$

Employing the algebraic expansion

$$[f(\xi)]^{P-1} = \sum_{\mu} C_\mu \xi^\mu, \tag{2}$$

and summing for the marks $\xi \neq 0$ of the $GF[P]$, we get

$$N^* = -1 - \sum_{\mu} C_\mu \left(\sum_{\xi} \xi^\mu\right).$$

* For a cubic form this invariant is exhibited in expanded form for $p \leqq 13$ on p. 221 of my paper on modular invariants, *Trans. Amer. Math. Soc.*, vol. 8 (1907), pp. 205–230. At the time of writing that paper I did not know of Hurwitz's work.

By the writer's Linear Groups, page 54,

$$\sum_{\xi} \xi^{\mu} = \begin{cases} -1 \text{ for } \mu \text{ divisible by } P-1, \\ 0 \text{ for } \mu \text{ not divisible by } P-1. \end{cases}$$

Hence

$$N^* + 1 = \sum C_{\nu(P-1)} \qquad (\nu = 0, 1, \cdots). \tag{3}$$

Inserting the values of P and the C's, we get

$$N^* + 1 = \sum_{\alpha} \frac{(p^{nm}-1)!}{\alpha_0!\ \alpha_1! \cdots \alpha_r!} a_0^{\alpha_0} a_1^{\alpha_1} \cdots a_r^{\alpha_r}, \tag{4}$$

summed for all sets of integers $\alpha_i \geqq 0$ for which

$$\alpha_0 + \alpha_1 + \cdots + \alpha_r = p^{nm} - 1, \tag{5}$$

$$\alpha_1 + 2\alpha_2 + \cdots + r\alpha_r \equiv 0 \pmod{p^{nm}-1}. \tag{6}$$

In (4) the fractional form of the multinomial coefficient is to be replaced by its integral value. In fact, certain of the α's may be multiples of p *.

3. When $nm > 1$, certain of the multinomial coefficients in (4) are multiples of p and the corresponding terms may be dropped from the equation. To this end, set

$$\alpha_i = \sum_{j=0}^{mn-1} c_{ij} p^j \qquad (0 \leqq c_{ij} < p), \tag{7}$$

for $i = 0, 1, \cdots, r$. Further,

$$p^{nm} - 1 = \sum_{j=0}^{mn-1} (p-1)p^j.$$

Then, by well-known theorems, the multinomial coefficient M in (4) is a multiple of p unless

$$\sum_{i=0}^{r} c_{ij} = p - 1 \quad (j = 0, 1, \cdots, mn-1); \tag{5'}$$

while, if these relations hold,

$$M \equiv \prod_{j=0}^{mn-1} \frac{(p-1)!}{c_{0j}!\, c_{1j}! \cdots c_{rj}!} \pmod{p}. \tag{8}$$

In place of (5) we may employ the more exacting relations (5').

* As this is not true in Hurwitz's case $n = m = 1$, we may then place the factor $(p-1)!$ before the summation sign.

Finally, the exponents of each a_i may be made less than p^n by employing

$$a_i^{p^n} = a_i. \tag{9}$$

4. Instead of deleting vanishing terms of (4) by employing relations (5′) in place of (5), we may modify our former method of determining the C_μ. Instead of the algebraic expansion (2) we may employ the modular relation

$$[f(\xi)]^{p^{nm}-1} \equiv \prod_{j=0}^{m-1} [f(\xi)]^{p^{nj}(p^n-1)} = \prod_{j=0}^{m-1} [f(\xi^{p^{nj}})]^{p^n-1}, \tag{10}$$

which follows readily from (9).

The plan of § 3, which employs (9) only at the final stage, has the advantage of furnishing simultaneously the number of roots in the $GF[p^t]$ of equation (1) with coefficients in any $GF[p^n]$, where n is a divisor of t. See the example in § 6.

5. In (1) set $x = x_2/x_1$ and consider the binary form

$$f(x_1, x_2) = a_0x_1^r + a_1x_1^{r-1}x_2 + \cdots + a_rx_2^r \tag{11}$$

in the $GF[p^n]$. Two pairs of marks (x_1, x_2) and (x_1', x_2') of the $GF[p^{nm}]$ will be said to give the same set of solutions of

$$f(x_1, x_2) = 0 \tag{12}$$

if, and only if, there exists a mark ρ of the $GF[p^{nm}]$ for which $x_1' = \rho x_1$, $x_2' = \rho x_2$ in that field. Let A denote the number of distinct sets of solutions, not both zero, of (12) in the $GF[p^{nm}]$. Evidently

$A = N$, when $a_0 \neq 0$ and $a_r \neq 0$ in the $GF[p^n]$;

$A = N + 1$, when just one of the coefficients a_0, a_r is zero;

$A = N + 2$, when $a_0 = a_r = 0$.

Hence in every case $A \equiv A^* \pmod p$, where

$$A^* + a_0^{p^n-1} + a_r^{p^n-1} = N + 2.$$

THEOREM. *The number A of distinct sets of solutions, not both zero, in the $GF[p^{nm}]$ of a homogeneous equation* (12), *with coefficients in the $GF[p^n]$, is congruent to A^* modulo p, where*

$$A^* - 1 = -a_0^{p^n-1} - a_r^{p^n-1} + \sum_\alpha \frac{(p^{nm}-1)!}{\alpha_0!\,\alpha_1!\cdots\alpha_r!} a_0^{\alpha_0}a_1^{\alpha_1}\cdots a_r^{\alpha_r}, \tag{13}$$

subject to (5) *and* (6), *or to* (6), (7) *and* (5′).

The function defined by the second member of (13) *is an absolute modular invariant of the binary form* (11).

6. Examples. Let $r = 3$, so that (11) is a binary cubic. First, let $p = 3$, $m = n = 1$; the invariant* is seen to be

$$K = a_1^2 + a_2^2 - a_0a_2 - a_1a_3. \tag{14}$$

Next, let $p = 3$, $nm = 2$. As in (7), set

$$\alpha_i = c_{i0} + 3c_{i1} \qquad (c_{ij} = 0, 1, 2).$$

Then, by (5′) and (6),

$$\sum_{i=0}^{3} c_{i0} = 2, \ \sum_{i=0}^{3} c_{i1} = 2, \ c_{10} + 2c_{20} + 3c_{30} + 3c_{11} + 6c_{21} + 9c_{31} \equiv 0 \pmod 8.$$

The sets of values of the c_{ij} are as follows:

c_{01}	c_{11}	c_{21}	c_{31}	c_{00}	c_{10}	c_{20}	c_{30}
2	0	0	0	2	0	0	0
1	0	1	0	1	0	1	0
1	1	0	0	0	0	1	1
1	0	1	0	0	2	0	0
0	0	1	1	1	1	0	0
0	2	0	0	1	0	1	0
0	0	2	0	0	0	2	0
0	1	0	1	0	0	2	0
0	0	2	0	0	1	0	1
0	0	0	2	0	0	0	2
0	1	0	1	0	1	0	1
0	2	0	0	0	2	0	0

In view of (8), the resulting function (13) is

$$\begin{aligned} &a_0^4a_2^4 + a_0^3a_1^3a_2a_3 - a_0^3a_1^2a_2^3 + a_0a_1a_2^3a_3^3 - a_0a_1^6a_2 \\ &\qquad + a_2^8 - a_1^3a_2^2a_3^3 - a_1a_2^6a_3 + a_1^4a_3^4 + a_1^8. \end{aligned} \tag{15}$$

Taking $n = 2$, $m = 1$, we have in (15) an absolute invariant† of the binary cubic in the $GF[3^2]$.

Taking $n = 1$, $m = 2$, and reducing by $a^3 \equiv a$, we get

$$\begin{aligned} J = {} &a_0^2a_2^2 - a_0a_1a_2a_3 + a_0a_1^2a_2 + a_2^2 \\ &+ a_1a_2^2a_3 + a_1^2a_3^2 + a_1^2 \pmod 3, \end{aligned} \tag{15′}$$

an absolute invariant of the binary cubic in the $GF[3]$.

* See (14), *Transactions*, l. c., p. 211.

† See (78), *Transactions*, l. c., p. 227; direct by (58), p. 222.

Now K and J, increased by unity, give (apart from a multiple of 3) the number of sets of values for which a cubic form (with the coefficients not all zero) vanishes in the $GF[3]$ and the $GF[3^2]$, respectively. We find that *

$$J = K + \Delta^2 - \Delta \quad (\Delta = \text{discriminant}),$$
$$K^2 + K = J^2 + J.$$

But K is not a rational function of J (in view of the first and second forms below), nor J a rational function of K (in view of the second and third forms):

Form.	K	J	Δ
$x^3 - xy^2 + y^3$	-1	-1	1
$x^3 + xy^2$	0	-1	-1
x^3	0	0	0
$x^2y + xy^2$	-1	-1	1
x^2y	1	1	0
Vanishing	0	0	0

Every cubic can be transformed modulo 3 into one of those given in the table (*Transactions*, l. c., page 232).

THE UNIVERSITY OF CHICAGO,
January, 1908.

NOTE ON JACOBI'S EQUATION IN THE CALCULUS OF VARIATIONS.

BY PROFESSOR MAX MASON.

(Read before the American Mathematical Society, February 29, 1908.)

IN Weierstrass's theory of the calculus of variations † it is shown that the determinant

$$\omega = \frac{\partial y}{\partial t}\frac{\partial x}{\partial a} - \frac{\partial x}{\partial t}\frac{\partial y}{\partial a}$$

formed from the equations $x = x(t, a)$, $y = y(t, a)$ of a family of extremals of the integral

* If we employ the invariant $P = \Delta + 1 - K$ (l. c., p. 211), we have
$$J = K^2 + K + P - 1.$$

† See for example Bolza, Lectures on the calculus of variations, Chicago, 1904.