JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

W. L. G. WILLIAMS

On the formal modular Invariants of binary Forms

Journal de mathématiques pures et appliquées 9^e série, tome 4 (1925), p. 169-192.
<http://www.numdam.org/item?id=JMPA_1925_9_4__169_0>

On the formal modular invariants of binary forms

By W. L. G. WILLIAMS.

Introduction.

A. Hurwitz in a paper (1) published over twenty years ago first defined formal modular invariants, but he did not prove that there exists any such invariant not congruent to an algebraic invariant. L. E. Dickson, O. E. Glenn, O. C. Hazlett and others have added to our knowledge of these invariants, but little has been published on the invariants of forms of order greater than two. The problem to which this paper owes its origin is the determination of a fundamental system of invariants of the cubic, mod p, a prime; though no solution of this problem for any prime is to be found in the following pages, results obtained in considering it are now published in the hope not only that some interest may attach to them, but that they may to some slight degree contribute to a solution of this problem.

Article I is devoted to a brief introduction to the subject and to three theorems, two of which are proved by a method different from that employed by Hurwitz in the proof of the first, a method which leads immediately to a proof of the third.

In his discussion of the invariants of the binary cubic Dickson in his Madison Colloquium Lectures (2) has proved the existence for every prime greater than three of a certain invariant; when one examines this invariant, mod 5, one finds, as Dickson points out, that it is the product of two invariants of the same degree neither of which is the product of invariants. An examination of the case when $p = 7$ confronts one with the same circumstance and the question whether

(1) Hurwitz, *Archiv der Math. u. Phys.*, 3$^{\text{te}}$ série, vol. 5, 1903.

(2) *Madison Colloquium Lectures*, p. 48-51.

matters fall out thus for every p greater than 5 is an interesting one. The question is answered in the affirmative in Article II, and other results of kindred nature find their place in the same article.

If q is the order of a binary form and p a prime, it will appear that, unfortunately, our problem resolves itself into $\Phi(q)$ problems, $\Phi(q)$ being the number of numbers less than q and prime to it, one for each prime value of r when p is expressed in the form $qm + r\ (r < q)$. Thus when $q = 2$ there is but one problem (1) since all odd primes are of the form $2m + 1$, and this is one of the circumstances which have made the determination of a fundamental system of invariants less difficult for the quadratic than for forms of higher order.

In Article III various general theorems are proved and the essential differences for the cubic between the case $p = 3m + 1$ and the case $p = 3m + 2$ are made clear. In Article IV and V some of the details of classification according to leading terms of invariants of the cubic, mod 5 and 7, are given; the tediousness of such a classification has made it seem unwise to publish it in more detail, but we illustrate the general theorems already proved, in the cases $p = 5$ and $p = 7$, and prove that there at least twelve independent invariants, mod 5. That it is almost certain that the number of members of a fundamental system varies with the prime, as in the case of seminvariants, will not escape the reader's notice. Article VI contains a generalization of a theorem of Hurwitz and some modular identities involving algebraic invariants of the binary cubic, quartic, and quintic, which are not without interest.

I.

As when a binary q-ic form

$$f = (a_0, a_1, \ldots, a_q)(x, y)^q \qquad \text{is carried over into}$$

$$F = (A_0, A_1, \ldots, A_q)(X, Y)^q \qquad \text{by the linear substitution}$$

$$(A) \qquad \begin{cases} x = l X + m Y \\ y = l' X + m' Y, \end{cases}$$

(1) If we except the very special case which arises from taking $p = 3$ (Dickson, *loc. cit.*, p. 42).

isobaric polynomial, invariant mod p under (1) and (2), is an invariant; and hence a polynomial invariant mod p under (1) and (2) is whose determinant is supposed different from zero, a function

$$I(a_0, \ldots, a_q)$$

is called an (algebraic) invariant of f under all substitutions (A) when

$$I(A_0, \ldots, A_q) = (lm' - l'm)^w I(a_0, \ldots, a_n),$$

so I is called a *formal modular invariant* of f under all substitutions

$$x = lX + mY$$
$$y = l'X + m'Y,$$

l, m, l', m', being integers reduced, mod p, a prime, and $lm' - l'm$ not divisible by p, if

$$I(A_0, \ldots, A_q) \equiv (lm - l'm)^w I(a_0, \ldots, a_q) \qquad (\mathrm{mod}\, p).$$

Every algebraic invariant is thus a formal modular invariant, but the converse is not true. In this paper only invariants which are polynomials in their arguments are considered, and the word invariant is used to denote formal modular invariant.

The transformations

(1) $$\begin{cases} x = X + Y, \\ y = Y; \end{cases}$$

(2) $$\begin{cases} x = Y, \\ y = -X; \end{cases}$$

and

(3) $$\begin{cases} x = X, \\ y = \lambda Y \end{cases}$$

(λ being any integer $\not\equiv 0$, mod p) generate all binary modular substitutions of determinant not divisible by p. A necessary and sufficient condition for the invariance of a polynomial I under (3) is that I be modularly isobaric, mod $(p-1)$, i. e. that the weights $\sigma_1, \sigma_2, \ldots, \sigma_n$ of the terms be congruent, mod $(p-1)$. Consequently a modularly

either an invariant or the sum of invariants, the separate invariants being obtainable by a simple separation according to the weight of the terms. It is thus convenient to speak of a polynomial invariant under (1) and (2) as an invariant, though it may not be an invariant in the strict sense of that term, but the sum of two or more invariants. A polynomial invariant, mod p, under (1) is called a *formal modular seminvariant*. Invariants and seminvariants are homogeneous or the sums of homogeneous seminvariants or invariants.

We employ binomial coefficients

$$\binom{q}{1}, \quad \binom{q}{2}, \quad \cdots, \quad \binom{q}{q-1}$$

and it should be noticed that we confine ourselves rigidly to forms in which all of the binomial coefficients are incongruent to zero, mod p. All theorems are proved under this restriction, even when this fact is not explicitly stated.

As an illustration consider

$$f = ax^3 + 3bx^2y + 3cxy^2 + dy^3,$$

which is carried over into

$$F = AX^3 + 3BX^2Y + 3CXY^2 + DY^3$$

and

$$f' = a'X^3 + 3b'X^2Y + 3c'XY^2 + d'Y^3$$

under (1) and (2) respectively, where

$$(1') \quad \begin{cases} A = a, \\ B = a + b, \\ C = a + 2b + c, \\ D = a + 3b + 3c + d, \\ K = (b^2 - ac)d^2 + (bc^2 - a^2b)d - b^3 - c^3 + a^2c^2 + ab^2c; \end{cases}$$

$$(2') \quad \begin{cases} a' = -d, \\ b' = c, \\ c' = -b, \\ d' = -a. \end{cases}$$

is an invariant of the cubic, mod 5, for it is invariant, mod 5, under (1) and (2). It is homogeneous and modularly isobaric, mod 4.

For an invariant of degree i and weight $\equiv w$, mod $p-1$, of the binary $q - ic$ form the congruence $iq - 2w \equiv 0$, mod $p-1$, holds (1). It has been pointed out by Dickson that the $(p+1)$ linear polynomials a, $at^3 + 3bt^2 + 3ct + d$ $(t = 0, \ldots, p-1)$ with coefficients reduced, mod p, play a fundamental rôle in the theory of the invariants of the binary cubic. If in

$$\eta^3, \quad (\xi + t\eta)^3 \qquad (t = 0, \ldots, p-1)$$

we set

$$\xi^3 = d, \qquad \xi^2\eta = c, \qquad \xi\eta^2 = b, \qquad \eta^3 = a,$$

we have these $(p+1)$ linear polynomials and a substitution of $\xi + \eta$ for ξ and η for η in these is equivalent to (1'), while

$$(2'') \qquad \xi = -\eta, \qquad \eta = \xi,$$

is equivalent to (2'). Thus the linear polynomials simply change their order under (1'); under the substitution (2'')

$$\eta^3, \quad (\xi + t\eta)^3 \qquad (t = 0, \ldots, p-1),$$

become

$$\xi^3, \quad -\eta^3, \quad -t^3\left(\xi + \frac{p-1}{t}\eta\right)^3 \qquad (t = 1, 2, \ldots, p-1).$$

Since

$$\prod_{t=}^{p-1}(-t^3) \equiv -1 \qquad (\text{mod } p),$$

by Wilson's theorem,

$$a\prod_{t=0}^{p-1}(at^3 + 3bt^2 + 3ct + d)$$

is an invariant of the cubic. Similar reasoning leads us to the general theorem :

---

(1) GLENN, *Amer. Journal of Math.*, vol. 37, 1915, p. 75.

THEOREM I :

$$a_0 \prod_{t=0}^{p-1} \left[a_0 t^q + \binom{q}{1} a_1 t^{q-1} + \ldots + a_q \right]$$

is a formal modular invariant, mod p, of the binary $q - ic$ form

$$a_0 x^q + \binom{q}{1} a_1 x^{q-1} y + \ldots + a_q y^q,$$

where p and q are such that none of

$$\binom{q}{1}, \quad \binom{q}{2}, \quad \ldots, \quad \binom{q}{q-1}$$

is divisible by p (1).

In like manner there follows at once

THEOREM II :

$$K_\lambda = a_0^{\lambda(p-1)} + \sum_{t=0}^{p-1} \left[a_0 t^q + \binom{q}{1} a_1 t^{q-1} + \ldots + a_q \right]^{\lambda(p-1)} \qquad (\lambda = 1, 2, \ldots),$$

are invariants of $(a_0, a_1, \ldots, a_q)(x, y)^q$. Hurwitz proved this theorem by quite a different method for the case $\lambda = 1$, and Dickson (2) independently discovered the invariant K_1. The method due to Hurwitz could easily be applied to the general theorem, but not to the following theorem, whose proof by the present method offers no difficulty.

THEOREM III : *If p is odd and λ is an integer such that $\lambda \frac{p-1}{q}$ is an integer*

$$I = a_0^{\lambda \frac{p-1}{q}} + \sum_{t=0}^{p-1} \left[a_0 t^q + \binom{q}{1} a_1 t^{q-1} + \ldots + a^q \right]^{\lambda \frac{p-1}{q}}$$

is a formal modular invariant of $(a_0, a_1, \ldots, a_q)(x, y)^q$.

Theorem II is of course only a special case of Theorem III.

Dickson has found a fundamental system of invariants of the binary

(1) HURWITZ, *Archiv der Mathematik und Physik*, 3e série, vol. 5, 1903.

(2) DICKSON, *loc. cit.*, p. 44 *et seq.*

quadratic, mod p, but no fundamental system has been given for any form of higher order except the cubic in the special cases when $p = 2$ and $p = 3$ (1).

II.

Other linear polynomials in $a_0, a_1, \ldots, a_q$ than those hitherto considered play their parts in the theory of formal modular invariants. These Dickson has expressed in the forms

$$at + b, \quad a(t^2 - k) + 2bt + c, \quad a(t^3 - 3kt - j) + 3b(t^2 - k) + 3ct + d$$
$$(t, j, k = 0, 1, \ldots, p-1),$$

for the purpose of developing the theory of seminvariants and invariants of linear, quadratic and cubic binary forms. There is another method dealing with these linear polynomials which for certain purposes offers considerable advantages. For not only is there a one-to-one correspondence between the polynomials

$$a_0 t^q + \binom{q}{1} a_1 t^{q-1} + \ldots + a_q \qquad \text{and} \qquad (\xi + t\eta)^q \qquad (t = 0, \ldots, p-1)$$

obtained by an interchange of a_i and $\xi^{q-i}\eta^i$, but there is a like correspondence between the polynomials $a(t^2 - k) + 2bt + c$ and the quadratics $x^2 + 2rxy + sy^2$ obtained by setting $x^2 = c$, $xy = b$, $y^2 = a$, and between

$$a(t^3 - 3kt - j) + 3b(t^2 - k) + 3ct + d$$

and

$$x^3 + 3ux^2y + 3vxy^2 + wy^3$$

obtained by setting $x^3 = d$, $x^2 y = c$, $xy^2 = b$, $y^3 = a$, r, s, u, v, w ranging over the values from 0 to $p - 1$ in such a way as to represent all non-congruent quadratics and cubics of the forms $x^2 + \ldots$ and $x^3 + \ldots$.

As above, a substitution (1) on one of the forms generates a substitution (1′) on the corresponding linear polynomial, and substitution (2), a substitution (2′). (1) and (2) generate all modular binary substitutions of determinant unity; if we call two linear polynomials

(1) GLENN, *Transactions Amer. Math. Soc.*, vol. 19, 1918, p. 117.

equivalent when and only when one of them passes into a multiple of the other by a binary linear modular substitution of determinant congruent to unity, mod p, the questions of equivalence of two linear polynomials and of the equivalence of the forms are identical.

Following Dickson we call the set of all forms equivalent to a given one a *genus;* we use the same term for the set of all linear polynomials equivalent to a given one. Now Dickson (1) has proved that all quadratics, irreducible, mod p, form a genus; in fact, if $\Phi_1, \Phi_2, \ldots, \Phi_n$ be all the quadratics, irreducible mod p, the product $\Phi_1, \Phi_2, \ldots, \Phi_n$ is carried into itself by any modular binary linear substitution of unit determinant. Let $\Psi_1, \Psi_2, \ldots, \Psi_n$ bet he linear polynomials corresponding to $\Phi_1, \Phi_2, \ldots, \Phi_n$; then $\Psi_1, \Psi_2, \ldots, \Psi_n$ is an invariant as it is invariant under the substitutions induced by (1), (2) and (3). It is in fact exactly the invariant :

$$\Gamma = \Pi \gamma_k$$

(k ranging over the quadratic non-residues of p) forming a member of Dickson's fundamental system of invariants of the quadratic, where

$$\gamma_k = a(t^2 - k) + 2bt + c.$$

The cubic forms, irreducible mod p ($p > 3$), form two genera, each of which includes exactly one half of the irreducible forms; calling the forms of a genus $\Phi_1, \Phi_2, \ldots, \Phi_{\frac{p^3-p}{6}}$, the product $\prod_i \Phi_i$ is carried into itself. We have therefore the

THEOREM : *The product of the* $\frac{p^3-p}{6}$ *linear polynomials corresponding to a genus of irreducible cubic forms* $x^3 + \ldots$ *is an invariant, mod p, of the binary cubic; there are two such invariants, each of the forms* $d^{\frac{p^3-p}{6}} + \ldots$ (2).

---

(1) *Transactions Amer. Math. Soc.*, vol. 12, 1911.

(2) The theorem of p. 49, *Madison Colloquium Lectures* is equivalent to the theorem : *the product of the* $\frac{p^3-p}{3}$ *linear polynomials corresponding to all cubics, irreducible mod p, is an invariant.* Our theorem then states that the invariant is always the product of two invariants, each of degree $\frac{p^3-p}{6}$.

Theorems of a like character for quartics, quintics, sextics and septimics, mod p, follow immediately from the facts regarding genera of irreducible forms of these orders given in Dickson's paper.

Not only is the product of the linear forms of a genus an invariant but the sum of their $\lambda(p-1)$ th powers ($\lambda = 1, 2, \ldots$) are invariants since ψ_k is transformed into $m\psi_l$ (say) and hence $\psi_k^{\lambda(p-1)}$ is transformed into $\psi_l^{\lambda(p-1)}$, mod p, since $m^{\lambda(p-1)} \equiv 1$, mod p, by Fermat's theorem. Also the sum of the products of the $\lambda(p-1)$ th powers of the ψ_s taken two, three, ... at a time are invariants. (Some of them may of course be $\equiv 0$, mod p.)

An example will make clearer the above theorems and the parallelism between irreducible forms and linear polynomials. The single genus of quadratics, irreducible mod 5, consists of the following ten forms:

(a)	x^2+2y^2,	(α)	x^2+3y^2,
(b)	$x^2+2xy+3y^2$,	(β)	$x^2+2xy+4y^2$,
(c)	$x^2+4xy+y^2$,	(γ)	$x^2+4xy+2y^2$,
(d)	$x^2+\ xy+y^2$,	(δ)	$x^2+\ xy+2y^2$,
(e)	$x^2+3xy+3y^2$,	(ε)	$x^2+3xy+4y^2$.

Under substitution (1) these are carried into each other in the order $(a), (b), (c), (d), (e), (a), \ldots$ and $(\alpha), (\beta), (\gamma), (\delta), (\varepsilon), (\alpha), \ldots$; under substitution (2) (a) and (α) are equivalent, ... The corresponding linear polynomials are:

(a)	$2a+c$,	(α)	$3a+c$.
(b)	$3a+2b+c$,	(β)	$4a+2b+c$,
(c)	$\ a+4b+c$,	(γ)	$2a+4b+c$,
(d)	$\ a+\ b+c$,	(δ)	$2a+\ b+c$,
(e)	$3a+3b+c$,	(ε)	$4a+3b+c$

and their product, the sum of their fourth, eighth, ... powers and the sums of the products of these latter taken two, three, ..., nine at a time are invariants.

A remarkable consequence of the present method is the theorem: *Every form* $(a_0, a_1, \ldots, a_{2n})(x, y)^{2n}$ *of even order has an invariant of the form* $a_{2n}^{\frac{p^2-p}{2}} + \ldots$.

Let us first prove this theorem for the quartic

$$ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4 \pmod 5.$$

Squaring the ten irreducible quadratics above we have ten quartics, $\Phi_1, \Phi_2, \ldots, \Phi_{10}$, and the product $\Phi_1\Phi_2\ldots\Phi_{10}$ is invariant under (1) and (2). Forming $\Psi_1, \Psi_2, \ldots, \Psi_{10}$ by making the substitution

$$x^4 = e, \quad x^3y = d, \quad x^2y^2 = c, \quad xy^3 = b, \quad y^4 = a,$$

we see that $\Psi_1\Psi_2\ldots\Psi_{10}$ is an invariant $e^{10} + \ldots$.

Similarly if we raise to the $p-1^{\text{th}}$ power the $\frac{p^2-p}{2}$ quadratics irreducible mod p, and make in each of the $2n - ic$ forms so obtained the substitution

$$x^{2n} = a_{2n}, \quad x^{2n-1}y = a_{2n-1}, \quad \ldots, \quad y^{2n} = a_0,$$

the product of the linear polynomials so obtained an invariant $a_{2n}^{\frac{p^2-p}{2}} + \ldots$.

If we arrange a seminvariant according to the descending powers of the most advanced letter, the first term is called the *leading term* of the seminvariant, and the coefficient of the most advanced letter in the leading term is called its *leader*. Ex. gr. a^2d^2 is the leading term of

$$\mathrm{D} = a^2d^2 - 6abcd + 4b^3d + 4ac^3 - 3b^2c^2$$

and a^2 is the leader of D.

If the leading term of a seminvariant, mod p, is a_{2n}^{λ}, λ must be a multiple of p, μp say (1). If the seminvariant is an invariant, mod p, $iq - 2w \equiv 0$, mod $(p-1)$, viz. $2n\mu p - 4n\mu p \equiv 0$, mod $(p-1)$ whence $\mu \equiv 0$, mod gcd $(p-1, 2n)$ where gcd $(p-1, 2n)$ is the greatest common divisor of $p-1$, $2n$. If $(p-1)$ is prime to n the invariant of the $2n - ic$ whose existence has just been proved has the lowest degree of all invariants whose leaders are constants, and no invariant of such a form with respect to such a modulus differs essentially from a power of this invariant.

---

(1) Williams, *Transactions Amer. Math. Soc.*, vol. 22, 1921, p. 61.

III.

If I is an invariant, mod p, of a form $f = (a_0, a_1, \ldots, a_q)(x, y)^q$ and A^m is the m^{th} iteration of the Aronhold operator

$$A = a_0^p \frac{\partial}{\partial a_0} + a_1^p \frac{\partial}{\partial a_1} + \ldots + a_q^p \frac{\partial}{\partial a_q},$$

A^m I is also an invariant of f (which may be $\equiv 0$, mod p) ([1]). Applying this theorem to the discriminant

$$D = a^2 d^2 - 6abcd + 4b^3 d + 4ac^3 - 3b^2 c^2$$

of the binary cubic form we see that this form has invariants whose leading terms are $a^2 d^{p+1}$ and $a^2 d^{2p}$. None of these three invariants is a polynomial with integral coefficients in the other two. If $a^2 d^r$ is the leading term of an invariant of the cubic, using the notation of Article I, $q = 3$, $i = r + 2$, $w \equiv 3r$, mod $(p-1)$, whence $3r + 6 \equiv 6r$, mod $(p-1)$. If $p-1$ is not divisible by 3, $r \equiv 2$, mod $(p-1)$; if p is of the form $3m+1$, $r \equiv 2$, mod $\frac{p-1}{3}$. We shall show later how actually to construct an invariant of the cubic, mod 5, for every value of $r \equiv 2$, mod 4, and an invariant of the cubic, mod 7, for every value of $r \equiv 2$, mod $2\left(= \frac{7-1}{3}\right)$, for which seminvariants exist.

Suppose that d^λ is the leading term of an invariant, mod p; then $3\lambda \equiv 6\lambda$, mod $(p-1)$. If p is of the form $3m+2$, λ must be a multiple of $p-1$; if p is of the form $3m+1$, λ must be a multiple of $\frac{p-1}{3}$. But λ must also be a multiple of p, for is $d^s + \ldots$ is a seminvariant, mod p, of the binary cubic, s must be divisible by p ([2]). λ must then be a multiple of $p(p-1)$ when p is of the form $3m+2$, and a multiple $\frac{p(p-1)}{3}$ when p is of the form $3m+1$. If for $p = 3m+2$ there exists an invariant, mod p, led by $d^{p(p-1)}$, then no invariant led by any power of d is essentially different from a power of this invariant, and if for $p = 3m+1$ an invariant, mod p, led by $d^{\frac{p(p-1)}{3}}$ exists, no

([1]) GLENN, *Bulletin Amer Math. Soc.*, vol. 21, 1915, p. 170.

([2]) WILLIAMS, *loc. cit.*, p. 69.

invariant, mod p, led by a power of d is essentially different from a power of this invariant (1). We proceed to show that these invariants exist for values of $p > 3$. There is no loss in generality by making the proofs for the simple cases $p = 5$, and $p = 7$.

1. If $p = 5$, consider the polynomials

$$a, \quad at^3 + 3bt^2 + 3ct + d \qquad (t = 0, \ldots, p-1 = 4),$$

viz.

$$\begin{aligned} a, \quad d, \quad P_1 &= a + 3b + 3c + d, \\ P_2 &= 3a + 2b + c + d, \\ P_3 &= 2a + 2b + 4c + d, \\ P_4 &= a + 3b + 2c + d. \end{aligned}$$

Under transformation (1) we have the substitution

$$\begin{bmatrix} a & d & P_1 & P_2 & P_3 & P_4 \\ a & P_1 & P_2 & P_3 & P_4 & d \end{bmatrix}$$

and under (2)

$$\begin{bmatrix} a & d & P_1 & P_2 & P_3 & P_4 \\ -d & a & (-1)^3 P_4 & (-2)^3 P_2 & (-3)^3 P_3 & (-4)^3 P_1 \end{bmatrix} (2).$$

Consider the sum

$$\begin{aligned} &(dP_1P_2P_3P_4)^4 + (aP_1P_2P_3P_4)^4 + (aP_2P_3P_4d)^4 + (aP_2P_4dP_1)^4 \\ &\quad + (aP_4dP_1P_2)^4 + (adP_1P_2P_3)^4, \end{aligned}$$

each term containing all of a, d, P_1, P_2, P_3, P_4 except a, d, P_1, P_2, P_3, P_4, respectively. Since under (1) and (2)

$$a^4 + d^4 + P_1^4 + P_2^4 + P_3^4 + P_4^4 \quad \text{and} \quad adP_1P_2P_3P_4$$

are invariant, then the sum under consideration is also invariant and we have the

---

(1) Two invariants I_1 and I_2 whose leading terms are $S_1 d^{\lambda_1}$ and $S_2 d^{\lambda_2}$ respectively, are *not essentially different* if $\lambda_1 = \lambda_2$ and there exists a constant $k \not\equiv 0$, mod p, such that $kS_1 \equiv S_2$, mod p; $kI_1 - I_2 \equiv$ an invariant $I_3 = S_3 d^{\lambda_3} + \ldots$, λ_3 being $< \lambda_1$.

(2) $\begin{pmatrix} P_t \\ P_c \end{pmatrix}$ where c is the integer between 0 and p, which is $\equiv \frac{p-1}{t}$, mod p, by Article I.

THEOREM :

$$[dP_1 \dots P_{p-1}]^{p-1} + \sum_{t=0}^{p-1} a^{p-1}[at^3 + 3bt^2 + 3ct + d]^{p-1}$$
$$\times [a(t+1)^3 + 3b(t+1)^2 + 3c(t+1) + d]^{p-1}$$
$$\times \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\times [a(t+p-1)^3 + 3b(t+p-1) + 3c(t+p-1) + d]^{p-1},$$

is an invariant of the binary cubic form

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3;$$

ist leading term is $d^{p(p-1)}$ *and, if* p *is of the form* $3m+2$, *no invariant, mod* p, *whose leading term is a power of* d *is essentially different from a power of this invariant.*

2. If $p-1$ is divisible by 3, since $(-t^3)^{\frac{p-1}{3}} \equiv 1, \bmod p$, for $t = 1, \dots, p-1$, we have the

THEOREM :

$$[dP_1 \dots P_{p-1}]^{\frac{p-1}{3}} + \sum_{t=0}^{p-1} [at^3 + 3bt^2 + 3ct + d]^{\frac{p-1}{3}} \dots$$
$$\times [a(t+p-1)^3 + 3b(t+p-1)^2 + 3c(t+p-1) + d]^{\frac{p-1}{3}}$$

is an invariant of

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3 \qquad (\bmod p),$$

when p *is of the form* $3m+1$; *its leading term is* $d^{\frac{p(p-1)}{3}}$, *and no invariant, mod* p, *whose leading term is a power of* d *is essentially different from a power of this invariant.*

The invariants of the last two theorems are sums of $(p-1)$ terms and it is very easy to see what the leading terms are. Invariants more complicated in type are made up by forming the sum of all the products $q\,(2 \leq q \leq p-2)$ at a time of $a^\lambda d^\lambda$,

$$P_1^\lambda = (a + 3b + 3c + d)^\lambda,$$
$$P_2^\lambda = (2^3 a + 3 \cdot 2^2 b + 3 \cdot 2c + d)^\lambda,$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots,$$
$$P_{p-1}^\lambda = \left(\overline{p-1}^3 + 3\overline{p-1}^2 b + 3\overline{p-1}c + d\right)^\lambda.$$

where $P_t = at^3 + 3bt^2 + 3ct + d$ and λ is a multiple of $p-1$ if p is of the form $3m+2$ and a multiple of $\frac{p-1}{3}$ if p is of the form $3m+1$.

Each term of the sum is of the form

$$a^\lambda d^\lambda P_{i_1}^\lambda \dots P_{i_{q-2}}^\lambda \quad \text{or} \quad a^\lambda P_{i_1}^\lambda \dots P_{i_{q-1}}^\lambda \quad \text{or} \quad d^\lambda P_{i_1}^\lambda \dots P_{i_{q-1}}^\lambda \quad \text{or} \quad P_{i_1}^\lambda \dots P_{i_q}^\lambda.$$

Under transformation (1) each term has a unique first, second, ... successor and its p th successor is itself, whence it is evident that the sum is formed by adding C_q^{p+1} [the number of combinations of $(p+1)$ things taken q at a time] seminvariants and is itself a seminvariant. Under transformation (2) each term is carried into a term of the sum and if A is carried into B, B is carried into A. [In fact if $A = P_{i_1}^\lambda, \dots, P_{i_q}^\lambda$, $B = P_{r_1}^\lambda, \dots, P_{r_q}^\lambda$, where $i_j r_j \equiv p-1$, mod p $(i = 1, 2, \dots, q)$]. Hence the sum is an invariant since it is invariant under (1) and (2) and we have the

THEOREM: *The sums of the products taken q at a time $(2 \leqq q \leqq p-2)$ of a^λ, d^λ, P^λ $(at^3 + 3bt^2 + 3ct + d)^\lambda$ $(t = 1, \dots, p-1)$ are invariants, mod p, of the binary cubic form, λ being a multiple of $p-1$ if p is of the form $3m+2$, and a multiple of $\frac{p-1}{3}$ if p is of the form $3m+1$.*

In like manner may be proved the

THEOREM: *The sum of all the terms of the type $a^{l\lambda} d^{m\lambda}$, $a^{m\lambda} d^{l\lambda}$, $a^{l\lambda} P^{m\lambda}$, $\dots$ $(l = 1, 2, \dots; m = 1, 2, \dots)$ is an invariant; likewise the sum of all the terms of the type $a^{l\lambda} d^{m\lambda} P_1^{n\lambda}$ is an invariant.*

The sum of the following is an invariant, mod 5, of the last type:

(1) $a^4 P_1^8$	(1) $d^4 P_4^8$	(2) $d^4 P_2^8$	(3) $d^4 P_3^8$	(4) $d^4 P_1^8$	(5) $d^4 a^8$
(2) $a^4 P_2^8$	(6) $P_1^4 d^8$	(12) $P_1^4 P_3^8$	(1) $P_1^4 P_4^8$	(5) $P_1^4 P_2^8$	(9) $P_1^4 a^8$
(3) $a^4 P_3^8$	(10) $P_2^4 P_1^8$	(10) $P_2^4 P_4^8$	(8) $P_2^4 d^8$	(16) $P_2^4 P_3^8$	(8) $P_2^4 a^8$
(4) $a^4 P_4^8$	(11) $P_3^4 P_2^8$	(7) $P_3^4 d^8$	(14) $P_3^4 P_1^8$	(14) $P_3^4 P_4^8$	(7) $P_3^4 a^8$
(5) $a^4 d^8$	(12) $P_4^4 P_3^8$	(13) $P_4^4 P_1^8$	(15) $P_4^4 P_2^8$	(9) $P_4^4 d^8$	(6) $P_4^4 a^8$

The sum of each group of five is a seminvariant, and the terms marked (1) are carried into each other by substitution (2), those

marked (2) carried into each other by the same substitution, etc., (11) and (16) being carried into themselves.

It is easy to prove that every formal modular seminvariant (invariant) of the covariants

$$(b^2-ac)x^2+(bc-ad)xy+(c^2-bd)y^2,$$
$$(a^2d-3abc+2b^3)x^3+(abd-2ac^2+b^2c)x^2y$$
$$+(-acd+2b^2d-bc^2)xy^2+(-ad^2+3bcd-2c^3)y^3$$

is a formal modular seminvariant (invariant) of the cubic.

IV.

In this article the preceding general theorems are applied to the case of the binary cubic, mod 5, and an attempt to classify its invariants is made, though a fundamental system is not determined.

Since $p-1$ is not divisible by 3 for $p=5$, the exponent q of any invariant $d^q+\ldots$ is divisible by 20; there exist invariants with the leader d^{20} e. g.

$$\begin{aligned} M = d^4 P_1^1 P_2^1 P_3^1 P_4^1 &+ a^1 P_1^1 P_2^1 P_3^1 P_1^1 \\ &+ a^1 P_2^1 P_3^1 P_4^1 d^4 \\ &+ a^1 P_3^1 P_4^1 d^4 P_1^1 \\ &+ a^1 P_4^1 d^4 P_1^1 P_2^1 \\ &+ a^1 d^4 P_1^1 P_2^1 P_3^1 (1). \end{aligned}$$

There then exists an invariant $d^{20\lambda}+\ldots$ for $\lambda=1, 2, \ldots$ and any invariant whose leading term is a power of d^{20} does not differ essentially from a power of M.

Every invariant led by a is of the form $ad^{20\mu+5}+\ldots$ ($\mu=0, 1, 2, \ldots$) for seminvariants whose leader is a have as leading terms a, ad^5, ad^{10}, ad^{15}, ... and the only ones of these which satisfy the condition $iq-2w\equiv 0$, mod 4, are of the form $d^{20\mu+5}$. There exists such an

---

(1) Since $\frac{p^3-p}{6}=p(p-1)$ when $p=5$, M and the products of the members of the two genera of linear polynomials corresponding to the two genera of irreducible cubics have the same leading term when $p=5$. For another form of expressing these invariants c. Dickson: *loc. cit.*, page 50.

invariant for every value of μ, viz $(a\delta_{00})M^{\mu}$, where as above

$$\delta_{00}=\prod_{t=0}^{4}(at^3+3bt^2+3ct+d).$$

It is easy to derive from the relation $iq-2w\equiv 0$, mod 4, that if the leading term of an invariant is of the form $a^i d^q$, $q\equiv 2$, mod 4.

An invariant exists for every value of q satisfying this condition. When $q=2$ it is the algebraic invariant :

$$D=a^2d^2+(4b^3-6abc)d+2b^2c^2-ac^3;$$

for $q=6$, it is

$$D_1=a^2d^6+(2b^3+2abc)d^5+a^6d^2+(2a^3bc+b^3+2abc^3+2ab^3c)d^4+2a^3c^3+ac^5+2b^6c^2+2b^2c^6,$$

obtained by operating on D with the Aronhold operator

$$a^3\frac{\partial}{\partial a}+b^3\frac{\partial}{\partial b}+c^3\frac{\partial}{\partial c}+d^3\frac{\partial}{\partial d};$$

when $q\equiv 10$ it is $(a\delta_{00})^2$.

Those whose leaders are a^2d^{14} and a^2d^{18} arise in a more complicated way. Consider the linear factors of

$$\gamma_1=\prod_{t=0}^{4}[a(t^2-1)+2bt+c]$$

and of

$$\delta_{02}=\prod_{t=0}^{4}[a(t^3-3.2t)+3b(t^2-2)+3ct+d]\ (^1),$$

viz.

$$\begin{aligned}
A&=4a\quad+c, & \alpha&=\quad 4b\quad+d,\\
B&=\quad 2b+c, & \delta&=\quad 2b+3c+d,\\
C&=3a+4b+c, & E&=\ a+\ b+\ c+d,\\
D&=3a+\ b+c, & \varepsilon&=4a+\ b+4c+d,\\
\beta&=\quad 3b+c, & \gamma&=\quad 2b+2c+d.
\end{aligned}$$

(1) $\gamma_1\delta_{02}$ is an invariant as will be noticed later; there is a misprint in (51), p. 50 of *Madison Colloquium Lectures* where it is referred to as $\gamma_1\partial_{03}$.

Transformation (1) induces a circular substitution on the constituents of each set. If A $\leftrightarrow$ B means A is carried into B and B is carried into A under substitution (2), we have

$$\begin{aligned} A^2 &\leftrightarrow \alpha^2, \\ B^2 &\leftrightarrow -B^2, \\ C^2 &\leftrightarrow -\gamma^2, \\ D^2 &\leftrightarrow -\delta^2, \\ E^2 &\leftrightarrow \varepsilon^2. \end{aligned}$$

Then the sum of

$A^2\alpha^q$	B^2D^q	$-\delta^2E^q$	α^2A^q	$-\gamma^2\varepsilon^q$	β^2C^q
$B^2\delta^q$	$C^2\beta^q$	$-E^2\varepsilon^q$	δ^2B^q	$-\alpha^2\gamma^q$	A^2D^q
C^2E^q	D^2A^q	$-\varepsilon^2\gamma^q$	E^2C^q	$-\delta^2\alpha^q$	$B^2\beta^q$
$D^2\varepsilon^q$	β^2B^q	$-\gamma^2\alpha^q$	ε^2D^q	$-E^2\delta^q$	C^2A^q
$\beta^2\gamma^q$	A^2C^q	$-\alpha^2\delta^q$	$\gamma^2\beta^q$	$-\varepsilon^2E^q$	D^2B^q

is an invariant when $q = 2, 6, 10, \ldots$. When $q = 2$, the sum of the first three groups is an invariant which is congruent, mod 5, to a multiple of D. The leading terms for $q = 6, 10, \ldots$ are

$$a^2d^6, \quad a^2d^{10}, \quad a^2d^{14}, \quad a^2d^{18}, \quad \ldots.$$

Of these

$$D_2 = a^2d^{14} + \ldots$$

and

$$D_3 = a^2d^{18} + \ldots,$$

are not polynomials with integral coefficients in the invariants previously mentioned in this section. But any invariant whose leader is a^2 is not essentially different from one of D, D_1, $(a\delta_{00})^2$, D_2, D_3, or one of these multiplied by a power of M.

Invariants led by a^3 must have as leading terms a^3d^3, a^3d^7, a^3d^{11}, ... in order that the relation $3q \equiv 2w$, mod 4, shall be satisfied. But no invariant with the leading term a^3d^3 can exist, as under substitution (2) a^3d^3 is carried into $-a^3d^3$. Since

$$\begin{aligned} a\delta_{00}D &= a^3d^7 + \ldots, \\ a\delta_{00}D_1 &= a^3d^{11} + \ldots, \\ (a\delta_{00})^3 &= a^3d^{15} + \ldots, \\ a\delta_{00}D_2 &= a^3d^{19} + \ldots, \\ a\delta_{00}D_3 &= a^3d^{23} + \ldots \end{aligned}$$

and multiplication of these by the proper power of M gives any other possible leading term $a^3 d^{4q+3}$, we see that any invariants led by a^3 are essentially equal to a polynomial in $a\delta_{00}$, D, D_1, D_2, D_3 and M. Consideration of invariants led by higher powers of a leads us to the

THEOREM: *Any invariant led by a power of a has the same leading term as a product of powers of some or all of* D, D_1, D_2, D_3, $a\delta_{00}$ *and* M.

$$K = K_1 = a^4 + \sum_{t=0}^{4} (at^3 + 3bt^2 + 3ct + d)^4$$
$$\equiv (b^2 - ac)d^2 + (bc^2 - a^2b)d - b^4 - c^4 + a^2c^2 + ab^2c \pmod 5,$$

$$K_2 = a^8 + \sum_{t=0}^{4} (at^3 + 3bt^2 + 3ct + d)^8$$
$$\equiv (b^2 - ac)d^6 + (3bc^2 + 2a^2b)d^5 + (2a^3c + 3ac^3 + b^4)d^4$$
$$+ (2a^2b^3 - a^4b + 3b^3c^2 + bc^4)d$$
$$+ a^4c^2 + a^2c^4 + 3b^4 + 3c^4 + 3a^3b^2c + 3ab^2c^3 + ab^4c,$$

$$K_3 = a^{12} + \sum_{t=0}^{4} (at^3 + 3bt^2 + 3ct + d)^{12}$$
$$\equiv (b^2 - ac)d^{10} + (3a^3c + 4b^4 + 3ac^3)d^9$$
$$+ (3a^4b + b^3c^2 + 2bc^4 + 4a^2b^3)d^8 + (b^{10} + 4a^3c^3)d^7$$
$$+ (3a^4b^3 + 2b^3c^4 + bc^{10} - a^{10}b)d + 4c^{12} + a^2c^{10} + a^{10}c^2$$
$$+ 2ab^4c^3 + 2a^3b^4c + 4a^4c^4 + a^3b^2c^3 + ab^{10}c,$$

are invariants led by $\Delta = b^2 - ac$, and it is apparent that every invariant led by Δ has the same leader as one of these or its product by a power of M, for from the relation $3q \equiv 2\alpha$, mod 4, the possible leading terms are Δd^2, Δd^6, Δd^{10}, Δd^{14}, Δd^{18}, Δd^{22}, ...

Now from K, K_2, K_3, and M we can make up invariants having the same leaders as Δd^q when $q \equiv 2, 6, 10$, mod 20; no invariant Δa^q with the leading term Δd^q for $q \equiv 14, 18$, mod 20, can exist, for not even such seminvariants exist, as may be seen from the fact that such seminvariants cannot be made up from the members of a fundamental system of seminvariants, mod 5, given on page 52 of *Madison Collo-*

quium Lectures (1), or from the theorem of Article VII of the present writer's dissertation (2). In fact, any invariant led by any power of Δ does not differ essentially from a product of powers of some or all of these four invariants, so long as the degree of the leader does not exceed the degree of d in the leading term.

When the leading term is $a\Delta$ the relation $3q \equiv 2w$, mod 4, gives as leading terms of possible invariants $a\Delta d^3$, $a\Delta d^7$,.... If an invariant with $a\Delta d^3$ as its leading term exists, it will be easy to form from it and the invariants already mentioned an invariant with the same leading term as any invariant in this list. Such an invariant G_1 does in fact exist and is $3(a\delta_{00} - G)$ where $G = ad^5 - a^5d - 3(bc^5 - b^5c)$ (3); it may be obtained independently by operating on 3K with the operator :

$$B = (a^3d - 3abc + 2b^3)\frac{\partial}{\partial a} + (abd - 2ac^2 + b^2c)\frac{\partial}{\partial b}$$
$$+ (acd + 2b^2d - bc^2)\frac{\partial}{\partial c} + (-ad^2 + 3bcd - 2c^3)\frac{\partial}{\partial d}.$$

A detailed discussion of the invariants of the binary cubic, mod 5, from the present point of view would be too tedious for publication, especially as these methods have not led to a determination of a fundamental system, mod 5. The only other independent invariants known to me are

$$\gamma_1\delta_{02} = \prod_{t=0}^{4}[a(t^3-1) + 2bt + c][a(t^3-t) + 3b(t^2-2) + 3ct + d]$$

mentioned in Article IV, and the invariant

$$Q = \prod_{k}\Gamma_k$$

---

(1) *Loc. cit.*

(2) *Loc. cit.*

(3) *Madison Coll. Lect.*, page 50 : That this is an invariant is easily verified; it may be obtained by writing $a' = a^p$, $b' = b^p$, $c' = c^p$, $d' = d^p$ in the joint invariant

$$ad' - a'd - 3(bc' - b'c)$$

of the two cubics $(a, b, c, d)(x, y)^3$ and $(a', b', c', d')(x, y)^3$, where $p = 5$.

(k ranging over the quadratic non-residues of 5) where

$$\Gamma_k = (b^2 - ac)(t^2 - k) + (bc - ad)t + c^2 - bd.$$

This is an invariant of the cubic, for it is an invariant of the covariant

$$(b^2 - ac)x^2 + (bc - ad)xy + (c^2 - bd)y^2.$$

The leading term of this last invariant is

$$(b^5 - a^4b)^2 d^{10}.$$

We have seen that even in the very simple case $p = 5$ the cubic has at least twelve independent invariants, $a\delta_{00}$, G_1, K, K_2, K_3, D, D_1, D_2, D_3, γ, δ_{02}, M and Q. A brief treatment of the invariants of the same form when $p = 7$ will bring out some striking differences between the cases when p is of the form $3m + 1$ and of the form $3m + 2$.

V.

From the point of view of classification by leaders there are marked contrasts between the invariants of the cubic for $p = 5$ and $p = 7$. Just as when $p = 5$, the invariant of lowest degree whose leader is a is $a\delta_{00}$, which is now

$$a\prod_{t=0}^{6}(at^3 + 3bt^2 + 3ct + d) \equiv ad^7 + \ldots,$$

but the condition $iq - 2w = 0$, mod $(p - 1)$, imposes no more stringent conditions on an invariant $a^2d^4 + \ldots$ than that $\lambda \equiv 0$, mod 2. We have in fact the algebraic invariant D, and the formal modular invariant

$$K \equiv a^6 + \sum_{t=0}^{6}(at^3 + 3bt^2 + 3ct + d)^6,$$

which has as its leader a numerical multiple of a^2. Indeed

$$-K \equiv -K_1 = a^2d^4 + (b^3 + 2abc)d^3 + 3(b^2c^2 + ac^3)d^2 + a^4d^2 + (3bc^4 - 2a^3bc + 3a^2b^3)d + b^6 + c^6 + 3ab^4c + 3a^2b^2c^2 + a^3c^3.$$

There is no invariant with leading term a^2d^6 nor indeed with leading term a^2d^{2r+5}, a^2d^{2r+6}, for no such seminvariants exist (1). By operating with the Aronhold operator on D and K we obtain:

$$\begin{aligned}
D_1 = {} & a^2d^8 + (2b^3 + 4abc)d^7 + a^8d^2 + (4a^7bc + 4ab^7c + 4abc^7 + 6b^9)d \\
& + 2b^8c^2 + 2b^2c^8 + 3a^7c^3 + 2ac^9,
\end{aligned}$$

$$\begin{aligned}
K_2 = {} & a^2d^{10} + (6b^3 + 5abc)d^9 + (5b^6c^2 + 5ac^3 + 4a^5)d^8 \\
& + (6bc^5 + 4a^3bc + 6a^2b^3)d^7 + 4a^8d^5 \\
& + (4a^7bc + 6b^9 + 4ab^7c + 4abc^7)d^3 \\
& + (6a^7c^3 + a^{10} + 5b^8c^2 + 5b^2c^8 + 4ac^9)d^2 \\
& + (5a^9bc + 5a^8b^3 + 6b^7c^4 + 4a^3b^7c + 4a^2b^9 + 4a^3bc^7 + 3bc^{10})d \\
& + 6a^7b^4c + 5a^8b^2c^2 + 6a^9c^3 + 5b^{12} + 5c^{12} + 3ab^{10}c \\
& + 5a^2b^8c^2 + 6ab^4c^7 + 5a^2b^2c^8 + 6a^3c^9.
\end{aligned}$$

An invariant whose leading term is a^2d^{14} is $(a\delta_{00})^2$.

All invariants led by a constant are essentially the same as powers of

$$\begin{aligned}
M = {} & (dP_1P_2P_3P_4P_5P_6)^2 + (adP_1P_2P_3P_4P_5)^2 \\
& + (aP_1P_2P_3P_4P_5P_6)^2 + (adP_2P_3P_4P_5P_6)^2 \\
& + (adP_1P_3P_4P_5P_6)^2 + (adP_1P_2P_4P_5P_6)^2 \\
& + (adP_1P_2P_3P_5P_6)^2 + (adP_1P_2P_3P_4P_6)^2 \\
= {} & d^{12} + \dots.
\end{aligned}$$

Now multiplying D, D_1, K, K_2 and $(a\delta_{00})^2$ by the proper powers of M we obtain invariants with the same leading term as those of all invariants led by a^2, as can be easily verified.

These invariants do not, however, complete the fundamental system so far as invariants led by a power of a are concerned, for by operating with B we obtain

$$L = a^3d^5 + \dots$$

an invariant obviously independent of them.

VI.

A. Hurwitz in his original paper on the so-called formal modular invariants cited above discussed the invariant, mod p $(p > 2)$ of the

(1) Williams, *loc. cit.*, p. 74.

binary quadratic $ax^2 + 2bxy + cy^2$,

$$K = K_1 = -a^{p-1} - \sum_{t=0}^{p-1} (at^2 + 2bt + c)^{p-1}$$

and proved it congruent, mod p, to $(b^2 - ac)^{\frac{p-1}{2}}$. Assuming the theorem (1) that every absolutely isobaric formal modular invariant is congruent, mod p, to a rational integral algebraic invariant, the truth of Hurwitz's identity is obvious, for this invariant is absolutely isobaric, and as $\Delta = b^2 - ac$ is the only algebraic invariant of the binary quadratic, K must be a constant multiple of a power of Δ. The power must be the $\frac{p-1}{2}$ th and the constant multiplier is 1, since

$$\sum_{t=0}^{p-1} (2bt)^{p-1} \equiv b^{p-1} \pmod{p}.$$

One generalization is that

$$-a_0^{p-1} - \sum_{t=0}^{p-1} \left[a_0 t^q + \binom{q}{1} a_1 t^{q-1} + \ldots + a_q \right]^{p-1}$$

is an invariant of the binary $q - ic$ form

$$a_0 x^q + \binom{q}{1} a_1 x^{q-1} y + \ldots + a_q y^q;$$

to this we have called attention in Article I.

We call attention to an interesting generalisation of another kind, viz, if p is a prime such that $\frac{2(p-1)}{q}$ is an integer, the invariant

$$-a_0^{\frac{2(p-1)}{q}} - \sum_{t=0}^{p-1} (a_0 t^q + \ldots + a_q)^{\frac{2(p-1)}{q}}$$

(1) Miss Olive C. Hazlett writes that she announced the proof of this important and difficult theorem at the December, 1924, meeting of the American Math. Soc. The theorem is true, if and only if $p > 2$.

is algebraic. The proof that this is an invariant is given in Article II *supra*. It is of weight $p-1$, for if we ascribe to t the weight 1 every term in the expansion of $(a_0 t^q + \ldots + a_q)^{\frac{2(p-1)}{q}}$ is of weight $2p-2$. Now the invariant is simply the coefficient of t^{p-1} in this expansion and is therefore of weight $p-1$ throughout. The theorem of Hurwitz is the special case of the theorem when $q=2$.

The special case $q=3$ gives as simple a result as $q=2$, provided p is of the form $3m+1$. For the only algebraic invariant of the binary cubic

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

is

$$D = a^2d^2 - 6abcd + 4b^3d + 4ac^3 - 3b^2c^2$$

and hence when p is of the form $3m+1$

$$-a^{\frac{2p-2}{3}} - \sum_{t=0}^{p-1} (at^3 + 3bt^2 + 3ct + d)^{\frac{2(p-1)}{3}} \equiv \binom{\frac{2}{3}(p-1)}{\frac{1}{3}(p-1)} D^{\frac{p-1}{6}} \pmod{p} \quad (1);$$

in particular, when $p=7$,

$$-a^3 - \sum_{t=0}^{6} (at^3 + 3bt^2 + 3ct + d)^3 \equiv D \qquad (\mathrm{mod}\ 7),$$

which may easily be verified directly.

When $q>3$ the results are less simple, for there are always two or more algebraic invariants. The quartic has two algebraic invariants

$$I = ae - 4bd + 3c^2,$$
$$J = (ac - b^2)e + 2bcd - ad^2 - c^3.$$

Putting $p=5$, 7, and 11 we have

$$-a^2 - \sum_{t=0}^{4} (at^4 + 4bt^3 + 6ct^2 + 4dt + e)^2 \equiv 2I \qquad (\mathrm{mod}\ 5),$$

$$-a^3 - \sum_{t=0}^{6} (at^4 + 4bt^3 + 6ct^2 + 4dt + e)^3 \equiv J \qquad (\mathrm{mod}\ 7)$$

(1) For direct verification of this result, see my paper, *Fundamental Systems of Formal Modular Protomorphs of Binary Forms*, soon to appear in the *Transactions of the Amer. Math. Soc.*

and

$$-a^5-\sum_{t=0}^{10}(at^5+4bt^3+6ct^2+4dt+e)^5\equiv 4\mathrm{IJ}\qquad(\mathrm{mod}\ 11).$$

These results are evident without any calculation since no other combinations of I and J of the proper degree are possible, and the constant multiplier is obtained by a comparison of the terms containing e alone.

For the quintic

$$-a^5-\sum_{t=0}^{10}(at^5+5bt^4+10ct^3+10dt^2+5et+f)^5\equiv 6\mathrm{I}_5\qquad(\mathrm{mod}\ 11),$$

where

$$\begin{aligned}\mathrm{I}_5=a^2f^2-10abef+4acdf+16ace^2-12ad^2e+16b^2df+9b^2e^2\\-12bc^2f-7bcde+8bd^3+8c^3e-3c^2d^2.\end{aligned}$$