Werk

Titel: On the reduction of Kronecker's modular systems whose elements are functions of t...

Autor: Hancock, Harris

Jahr: 1900

PURL: https://resolver.sub.uni-goettingen.de/purl?243919689_0122|log26

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

On the reduction of *Kronecker*'s modular systems whose elements are functions of two und three variables.

(By Mr. *Harris Hancock* at Cincinnati, Ohio.)

Following the methods given in the lectures at Berlin by Professor *Kronecker*, I have considered in the Quarterly Journal of Mathematics (No. 106, 1894) modular systems of the form

$$[f_1(x),\ f_2(x),\ \ldots,\ f_r(x)],$$

where the functions $f(x)$ are integral in x with integral coefficients. We suppose that there is no divisor common to all these functions, since it could at once be taken out as a factor of the system.

It was shown that such a system was equivalent to a system of the form

$$[m,\ m_1 f_1^{(1)}(x),\ m_2 f_2^{(1)}(x),\ \ldots,\ m_n f_n^{(1)}(x),\ g_1(x),\ g_2(x),\ \ldots],$$

where $m_1, m_2, \ldots, m_n$ are integers and divisors of the integer m, and $f_1^{(1)}(x), f_2^{(1)}(x), \ldots, f_n^{(1)}(x), g_1(x), g_2(x), \ldots$ are integral functions of the variable with integral coefficients.

When the integer m is equal to, say, $p \cdot q^2 \cdot r^3 \cdot \ldots$, where $p, q, r, \ldots$ are prime integers, the modular system was shown to be equivalent to a product of modular systems of the form:

$$[p,\ F],\ [q^2,\ qF_1,\ G],\ [r^3,\ r^2F_2,\ rG_1,\ H],\ \ldots$$

where $F, F_1, F_2, \ldots, G, G_1, \ldots, H, \ldots$ are determinate integral functions of the variable x with integral coefficients.

In *Crelle*'s Journal, Bd. 119, p. 148 canonical forms were derived for such systems. This treatment is (theoretically) sufficient for modular systems whose elements are integral functions of any number of variables:

$$f_1(x, x_1, x_2, \ldots, x_k),\ f_2(x, x_1, x_2, \ldots, x_k),\ \ldots$$

whose coefficients are integers. For make the *Kronecker* substitution

$$x_1 = x^g,\ x_2 = x^{g^2},\ \ldots,\ x_k = x^{g^k},$$

where g is a positive integer and is taken larger than the exponent of the highest power of any variable that appears in the expansion of any of the functions.

The functions $f(x, x_1, \ldots, x_k)$ are thereby transformed into functions $F(x)$ and in such a way that to any term of $f(x, x_1, \ldots, x_k)$ there is a corresponding term in $F(x)$, and to every term in $F(x)$ there corresponds a term in $f(x, x_1, \ldots, x_k)$.

We may in this manner apply the results known for functions of one variable to functions of several variables, and are thus able to derive reduced as well as canonical forms for modular systems in whose elements more than one variable enter.

But for the application of these systems to practical problems, to those arising for example in the Geometry of Two or Three Dimensions, to problems of Mechanics, etc., it seems desirable to have practical methods for their formulation; and consequently I have endeavoured to reduce by direct methods these systems to their simplest forms.

The results of these investigations I present in the following paper.

Modular systems in which the elements are functions involving only two variables.

Consider first modular systems of the form

$$[m_1, m_2, \ldots, g_1(x), g_2(x), \ldots, f_1(x, y), f_2(x, y), \ldots]$$

where $m_1, m_2, \ldots$ are integers, $g_1(x), g_2(x), \ldots$ are integral functions in x with integral coefficients, $f_1(x, y), f_2(x, y)$ are integral functions in x, y with integral coefficients.

For brevity we denote a number of elements $m_1, m_2, \ldots$ by the symbol $N|m|$; and if the number is definite, $\overset{i=n}{\underset{i=1}{N}}|m_i|$ denotes the elements $m_1, m_2, \ldots, m_n$, while $pN|g(x)|$ is the symbol for $pg_1(x), pg_2(x), \ldots$.

We may then denote the above system by

$$[N|m|,\ N|g(x)|,\ N|f(x, y)|].$$

Since we may replace $N|m|$ by m, where m is the greatest common divisor of the integers $m_1, m_2, \ldots$, the system reduces at once to

$$[m, N|g(x)|, N|f(x, y)|].$$

If $m = m_1 \cdot m_2$ where the integers m_1 and m_2 are relatively prime to each other, this system is equal to the product of the two systems

$$[m_1, N|g(x)|, N|f(x,y)|], \quad [m_2, N|g(x)|, N|f(x,y)|].$$

We have therefore to consider (cf. this Journal, Bd. 119, p. 153) modular systems of the form

$$\left[\begin{matrix} p^n, p^{n-1}N|g^{(1)}(x)|, p^{n-2}N|g^{(2)}(x)|, \ldots, pN|g^{(n-1)}(x)|, \\ N|g^n(x)|, p^{n-1}N|f^{(1)}(x,y)|, p^{n-2}N|f^{(2)}(x,y)|, \ldots, N|f^{(n)}(x,y)| \end{matrix}\right],$$

where p is a prime integer and where the indices belonging to the functions are merely used to avoid a great number of different letters and all the functions are integral in their variables with integral coefficients. For brevity we may say that such functions belong to the realm of integrity $[1, x, y]$, where by this realm of integrity we understand that system of integral quantities that is composed of all integral functions of the elements $1, x, y$ including, of course all integers.

When $n = 1$, the above system reduces to a system of the form

$$[p, N|g(x)|, N|f(x,y)|]$$

and by the methods given in this Journal, Bd. 119, p. 153 and p. 154, this system becomes at once

$$[p, g(x), N|f(x,y)|],$$

where $g(x)$ belongs to the realm of integrity $[1, x]$ and is the greatest common divisor (mod. p) of the functions $g_1(x), g_2(x), \ldots$.

If this function $g(x)$ should be an integer, there are two cases that may arise:

1^0. This integer may be $\equiv 0$ (mod. p), and then the system reduces to

$$[p, N|f(x,y)|]$$

and may be treated after methods given later, p. 292; or 2^0, this integer $\not\equiv 0$ (mod. p), when the system reduces to a unit-system and ceases to be of interest.

It may happen that an element $f_1(x,y)$, say, contains a factor $h_1(x)$, so that $f_1(x,y) = h_1(x)f_1'(x,y)$ (mod. p). Then if $h_1(x)$ is not a divisor of $g(x)$, the element $h_1(x)f_1'(x,y)$ may without altering the equivalence of the system be replaced by an element $d_1(x)f_1'(x,y)$ where $d_1(x)$ is a divisor (mod. p) of $g(x)$.

For suppose that $d_1(x)$ is the greatest common divisor (mod. p) of $g(x)$ and $h_1(x)$, then we may always determine two functions $\bar{g}(x)$ and $\bar{h}_1(x)$ belonging to the realm $[1, x]$ such that $g(x)\bar{g}(x)+h_1(x)\bar{h}_1(x)\equiv d_1(x)$ (mod. p), from which it follows that we may add the element

$$d_1(x)f_1'(x, y)\equiv g(x)\bar{g}(x)f_1'(x,y)+h_1(x)\bar{h}_1(x)f_1'(x,y) \text{ (mod. } p)$$

to the system without altering its equivalence.

After this element has been added to the system, the element $h_1(x)f_1'(x,y)$ being a multiple of $d_1(x)f_1'(x,y)$ may be dropped from the system.

We next determine whether the function $g(x)$ is decomposable into factors (mod. p). We say that an integral function in x with integral coefficients is divisible by $g_1(x)$, or is equal to the product of two functions $g_1(x)$ and $g_2(x)$ (mod. p), where $g_1(x)$ and $g_2(x)$ are integral functions in x with integral coefficients, when

$$g(x) = g_1(x)g_2(x)+pk(x),$$

where $k(x)$ is an integral function in x with integral coefficients, or

$$g(x) \equiv g_1(x)g_2(x) \text{ (mod. } p).$$

If then $g(x) \equiv g_1(x)g_2(x)$ (mod. p), and if the functions $g_1(x)$ and $g_2(x)$ have no common divisor (mod. p), then we may always determine two functions belonging to the realm $[1,x]$, $a(x)$ and $b(x)$ such that

$$g_1(x)a(x)+g_2(x)b(x) \equiv 1 \text{ (mod. } p).$$

It follows at once that

$$[p,g(x)] \sim [p,g_1(x)]\,[p,g_2(x)];$$

for this product is equal to $[p^2, pg_1(x), pg_2(x), g_1(x).\,g_2(x)]$. The elements $p^2, pg_1(x), pg_2(x)$ form a modular system $[p^2, pg_1(x), pg_2(x)] \sim p[p, g_1(x), g_2(x)]$

$$\sim p[p, g_1(x), g_2(x), g_1(x)a(x)+g_2(x)b(x)] \sim p[1] \sim p,$$

and

$$[p, g_1(x), g_2(x)] \simeq [p, g(x)].$$

For the sake of greater clearness in that which follows, I shall indicate briefly here what employing methods used by Professor *Kronecker* in his lectures, I have given in the Quarterly Journal of Mathematics (No. 106, p. 106 and arts. 28, 34, 36 and note to art. 42).

Consider the modular system

$$[p, f(x)]$$

where p is a prime integer and $f(x)$ a function of the realm $[1, x]$. For example take the system

$$[5, 2x^2+3x+4].$$

Multiplying the function $2x^2+3x+4$ by the numbers 1, 2, 3, 4, that is, by the complete system of incongruent residues (mod. 5), we have the functions:

$$2x^2+3x+4,\ 4x^2+6x+8,\ 6x^2+9x+12,\ 8x^2+12x+16.$$

These functions when reduced with respect to the modulus 5 are

$$2x^2+3x+4,\ 4x^2+x+3,\ x^2+4x+2,\ 3x^2+2x+1.$$

Hence the modular system $[5, 2x^2+3x+4]$ is equivalent to the system

$$[5, 2x^2+3x+4,\ 4x^2+x+3,\ x^2+4x+2,\ 3x^2+2x+1]$$
$$\sim [5, 4x^2+x+3] \sim [5, x^2+4x+2] \sim [5, 3x^2+2x+1].$$

For the function x^2+4x+2, for example, when multiplied respectively by the numbers 2, 3, 4 becomes (mod. 5)

$$2x^2+3x+4,\ 3x^2+2x+1,\ 4x^2+x+3,$$

which expressions may consequently be added to the system $[5, x^2+4x+2]$ without altering its equivalence.

In general, the system $[p, f(x)]$ is equivalent to the system $[p, rf(x)]$ where the integer r is any one of the complete system of incongruent residues (mod. p).

Hence in the above product, $[p, g_1(x)]\,[p, g_2(x)]$, the coefficients of the highest power of x in both $g_1(x)$ and $g_2(x)$ may be made ***unity,*** while all the other coefficient may be considered reduced, mod. p.

For example the product

$$[7, 2x+3]\,[7, 3x-2] \sim [7, 6x^2+5x-6] \sim [7, x^2+2x+6].$$

On the other hand

$$[7, 2x+3] \sim [7, x+5],$$
$$[7, 3x-2] \sim [7, x+4];$$

and

$$[7, x+5]\,[7, x+4] \sim [7, x^2+9x+20].$$

From this it is seen that in the decomposition of a quadratic function x^2+ax+b into its linear factors (mod. p), where p is a prime integer, if such a decomposition is possible, the integer a cannot be greater than $2p$

and b_1 cannot be greater than p^2. Hence if we have to find the divisors of $1x^2+Ax+B$ (mod. p), where the integers A and B have been reduced, mod. p, we have to investigate whether each of the functions

$$x^2+(A+ip)x+(B+jp) \qquad \left(\begin{smallmatrix} i=0, 1, \\ j=0, 1, 2, \ldots, p-1 \end{smallmatrix}\right)$$

is decomposable into linear factors, giving in all $2p$ different functions to consider.

The same method is at once applicable to the decomposition of a function of any degree into its irreducible factors (mod. p).

We have then to consider modular systems of the form

$$\left[\begin{array}{c} p, g(x)^m, g(x)^{m-1}N\{f^{(1)}(x,y)\}, \; g(x)^{m-2}N\{f^{(2)}(x,y)\}, \ldots \\ g(x)N\{f^{(m-1)}(x,y)\}, \; N\{f^{(m)}(x,y)\} \end{array}\right],$$

where p is a prime integer, $g(x)$ is an irreducible function in x with integral coefficients, and where all other elements are quantities of the realm of integrity $[1, x, y]$.

When $m = 1$, we have a modular system of the form

$$[p, g(x), \; N\{f(x,y)\}].$$

The function $g(x)$ has the form

$$g(x) = 1.x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n,$$

where the integers $a_1, a_2, \ldots, a_n$ have been reduced (mod. p). Hence each of these integers may have the values

$$0, 1, 2, \ldots, p-1.$$

There are consequently p^n such functions of the form $g(x)$ including that function. The p^n-1 functions other than $g(x)$ may be called the complete system of incongruent residues (modd. $p, g(x)$). They have the characteristics: 1^0, the difference of no two of them is $\equiv 0$ (modd. $p, g(x)$) and 2^0, any other function of the realm $[1, x]$ is congruent to one of the representatives of this system (modd. $p, g(x)$).

Suppose that the function $f_1(x,y)$ when expanded in descending powers of y has the form

$$f_1(x, y) = a_0(x)y^m+a_1(x)y^{m-1}+\cdots+a_m(x),$$

where the functions $a_0(x), a_1(x), \ldots, a_m(x)$ are quantities of the realm $[1, x]$.

Further suppose that the expansion of $a_0(x)$ is

$$a_0(x) = a_{00}x^s + a_{01}x^{s-1} + \cdots + a_{0s}$$

where $a_{00}, a_{01}, \ldots, a_{0s}$ are integers.

Since $g(x)$ is an irreducible function (mod. p), and as we may suppose that the coefficients of the powers of y in the above expression have been reduced (modd. $p, g(x)$), it is seen that we may determine two functions belonging to the realm $[1, x]$, $\bar{a}_0(x)$ and $\bar{g}(x)$ such that

$$a_0(x)\bar{a}_0(x) + g(x)\bar{g}(x) = c$$

where c is an integer which is not congruent to zero (mod. p). We may therefore find two integers $\bar{p}$ and $\bar{c}$ satisfying the expression

$$c\bar{c} + p\bar{p} = 1.$$

Hence $\bar{c}a_0(x)\bar{a}_0(x) \equiv 1$ (modd. $p, g(x)$). Further since $\bar{c}\bar{a}_0(x)$ is one of the representatives of the complete system of incongruent residues (modd. $p, g(x)$), it follows that in our given system we may without altering its equivalence replace the element $f_1(x, y)$ by the element $ca_0(x)f_1(x, y) = \varphi_1(x, y)$, say, where $\varphi_1(x, y)$ has the form

$$\varphi_1(x, y) = 1.y^m + c_1(x)y^{m-1} + c_2(x)y^{m-2} + \cdots + c_m(x),$$

where $c_1(x), c_2(x), \ldots, c_m(x)$ are quantities of the realm $[1, x]$. These functions may be considered reduced (modd. $p, g(x)$) and the element $\varphi_1(x, y)$ may be called the ***reduced element*** of $f_1(x, y)$.

We may notice here for the sake of what comes later that the number of different forms that each of the above functions $c_1(x), c_2(x), \ldots, c_m(x)$ can have, is p^n, where n is the degree of the irreducible function $g(x)$.

Hence if $\varphi_1(x, y)$ is an irreducible function in x, y, the number of functions of the form $\varphi_1(x, y)$ is $[p^n]^m = p^{nm}$. We may say here that the $p^{nm} - 1$ functions that are different from $\varphi_1(x, y)$ form a complete system of incongruent residues (modd. $p, g(x), \varphi_1(x, y)$). They have the characteristics 1^0, the difference of no two of them is congruent to zero (modd. $p, g(x), \varphi_1(x, y)$) and 2^0, any function belonging to the realm of integrity $[1, x, y]$ is congruent to one of the representatives of this system (modd. $p, g(x), \varphi_1(x, y)$).

We take instead of the proposed system the system

$$[p, g(x), N\{\varphi(x, y)\}],$$

where the elements $\varphi_1(x, y)$, $\varphi_2(x, y)$, ..., are the reduced elements of $f_1(x, y)$, $f_2(x, y)$, ..., and we suppose that the elements $\varphi_1(x,y)$, $\varphi_2(x,y)$, ... are arranged in the modular system so that those having the highest powers of y come first.

Let

$$\varphi_1(x, y) = 1y^m + c_1(x)y^{m-1} + c_2(x)y^{m-2} + \cdots + c_m(x),$$
$$\varphi_2(x, y) = 1y^k + d_1(x)y^{k-1} + d_2(x)y^{k-2} + \cdots + d_k(x),$$

and suppose that $m \gtreqless k$.

Divide $\varphi_1(x, y)$ by $\varphi_2(x, y)$ and express the result of the division in the form

$$\varphi_1(x, y) = q_1(x, y)\varphi_2(x, y) + r_1(x, y),$$

where $q_1(x,y)$ and $r_1(x,y)$ are quantities of the realm $[1, x, y]$. From this it is seen that $r_1(x,y)$ may be added to our system without altering its equivalence. Its degree in y is less than the degree of $\varphi_2(x,y)$ in y.

Since $\varphi_1(x,y)$ is a linear function of $\varphi_2(x,y)$ and $r_1(x,y)$, it may be omitted from the system. Let $\Phi_3(x,y)$ be the reduced element of $r_1(x,y)$ (modd. $p, g(x)$). Divide $\varphi_2(x,y)$ by $\Phi_3(x,y)$ and omitting the arguments after the functional signs when no ambiguity can arise, we have

$$\varphi_2 = q_2\Phi_3 + r_2.$$

Let Φ_4 be the reduced element of r_2, which we suppose has been added to the system, drop φ_2 from the system and continuing the process we have

$$\Phi_3 = q_3\Phi_4 + r_3,$$
$$\cdots\cdots\cdots\cdots$$

Since the degrees of the functions $r_3, r_4, \ldots$ in y are continually decreasing without becoming negative, we must finally have

$$\Phi_{\nu-2} = q_{\nu-2}\Phi_{\nu-1} + r_{\nu-2},$$
$$\Phi_{\nu-1} = q_{\nu-1}\Phi_{\nu},$$

where Φ_ν is the reduced element (modd. $p, g(x)$) of $r_{\nu-2}$. From this it is seen that we have been able to replace the two elements $\varphi_1(x,y)$ and $\varphi_2(x,y)$ in the modular system by their greatest common divisor (modd. $p, g(x)$), the element $\Phi_\nu(x,y)$. If this function $\Phi_\nu(x,y)$ should turn out to be congruent to zero (modd. $p, g(x)$), it is seen that the two original elements $\varphi_1(x, y)$ and $\varphi_2(x, y)$ add nothing new to the system; while if

$\Phi_\nu(x,y) \equiv k(x)$ (modd. $p, g(x)$), we are able to determine a function $\bar{k}(x)$ belonging to the realm $[1, x]$ so that

$$k(x)\bar{k}(x) \equiv 1 (\text{modd. } p, g(x)),$$

and the system reduces to a unit-system.

If we continue the above process, it is seen that the original modular system

$$[p, g(x),\ N\{f(x,y)\}]$$

may be replaced by the equivalent modular system

$$[p, g(x),\ f(x,y)]$$

where $f(x,y)$ is the greatest common divisor (modd. $p, g(x)$) of the elements $f_1(x,y)$, $f_2(x,y)$, ...

We may suppose here that the coefficient of the highest power of y of the function $f(x,y)$, when expanded in descending powers of this variable, is unity, while the others have all been reduced (modd. $p, g(x)$).

The form of modular system $[p, g(x), f(x,y)]$ is what I have called a canonical form of the original system (see this Journal, Bd. 118, p. 157), as it may be shown here precisely as it was shown for modular systems involving only one variable, that in whatever manner the reduction of the original modular system may have been performed, the final form which is equivalent to the above form, is identical to it.

Suppose that $f(x,y)$ in the above system is equal to the product of the two functions $F_1(x,y)$ and $F_2(x,y)$ (modd. $p, g(x)$), and further suppose that with respect to these moduli the functions $F_1(x,y)$ and $F_2(x,y)$ have no divisor in common.

We are therefore able to find belonging to the realm $[1, x, y]$ two functions $a(x,y)$ and $b(x,y)$ such that

$$a(x,y)F_1(x,y) + b(x,y)F_2(x,y) = d(x),$$

where $d(x)$ belongs to the realm $[1, x]$..

The function $d(x)$ has no factor in common with $g(x)$, for $g(x)$ being irreducible, it would follow in that case that $d(x)$ was divisible by $g(x)$, and then

$$a(x,y)F_1(x,y) + b(x,y)F_2(x,y) \equiv 0 (\text{modd. } p, g(x)).$$

But in the derivation of $a(x,y)$ and $b(x,y)$ we had

$$F_1 = Q_1 F_2 + F_3,$$
$$F_2 = Q_2 F_3 + F_4,$$
$$\cdots\cdots\cdots\cdots$$
$$F_{\lambda-2} = Q_{\lambda-2} F_{\lambda-1} + F_\lambda,$$
$$F_{\lambda-1} = Q_{\lambda-1} F_\lambda + d(x).$$

If then $d(x) \equiv 0$ (modd. $p, g(x)$), it follows that $F_{\lambda-1}$ is divisible by F_λ with respect to these moduli, and consequently F_1 and F_2; but as we have supposed that these functions did not have a common divisor with respect to these moduli, it follows also that $g(x)$ and $d(x)$ have no divisor in common.

We may therefore determine belonging to the realm $[1,x]$ two functions $\bar{d}(x)$ and $\bar{g}(x)$ so that

$$d(x)\bar{d}(x) + g(x)\bar{g}(x) = c,$$

where c is an integer $\not\equiv 0$ (mod. p); and finally we can find two integers $\bar{c}$ and $\bar{p}$ which satisfy the expression

$$c\bar{c} + p\bar{p} = 1.$$

It follows then at once that the modular system

$$[p, g(x), f(x,y)]$$

is equivalent to the product of the two systems

$$[p, g(x), F_1(x,y)] \quad \text{and} \quad [p, g(x), F_2(x,y)].$$

Hence when we come to the consideration of modular systems which have as elements functions of three variables, a prime integer and an irreducible function of one of the variables, the element involving only two variables may be regarded as an irreducible function or the power of an irreducible function in these two variables.

When the function $g(x)$ irreducible with respect to the modulus p, occurs to the second degree in the modular system, it has the form

(a.) $$[p, g(x)^2, g(x)N\{f(x,y)\}, N\{h(x,y)\}].$$

This system is equivalent to the system

$$[p, pg(x), g(x)^2, g(x)N\{f(x,y)\}, g(x)N\{h(x,y)\}, N\{h(x,y)\}].$$

From the elements $pg(x), g(x)^2, g(x)N\{h(x,y)\}$ we form the system

$$[pg(x), g(x)^2, g(x)N\{h(x,y)\}] \backsim g(x)[p, g(x), N\{h(x,y)\}].$$

We have seen above that

(b.) $$[p, g(x), N\{h(x,y)\}] \sim [p, g(x), \bar{h}(x,y)],$$

where $\bar{h}(x,y)$ is the greatest common divisor (modd. p, $g(x)$) of the elements $h_1(x,y)$, $h_2(x,y)$, ...

From the auxiliary system (b.) it follows on the one hand that

$$\bar{h}(x,y) = pP + g(x)G + \sum_i h_i(x,y)H_i,$$

where P, G, H_i are quantities belonging to the realm $[1, x, y]$; consequently if we write

$$h(x,y) = \bar{h}(x,y) - g(x)G = pP + \sum_i h_i(x,y)H_i,$$

we may add the element $h(x,y)$ to the system (a.) without altering its equivalence.

On the other hand we have from (b.)

$$h_\nu(x,y) = p\pi_\nu + g(x)\gamma'_\nu + \bar{h}(x,y)\alpha_\nu \qquad (\nu=1,2,\ldots).$$

All new quantities introduced belong to the realm $[1,x,y]$, *unless they are otherwise specified.*

But since $\bar{h}(x,y) = h(x,y) + g(x)G$, it follows that

$$h_\nu(x,y) = p\pi_\nu + g(x)\gamma_\nu + h(x,y)\alpha_\nu,$$

where

$$\gamma_\nu = \gamma'_\nu + G\alpha_\nu \qquad (\nu=1,2,\ldots).$$

It is therefore evident that if we add the element $h(x,y)$ to the system (a.) we may instead of the elements $N\{h(x,y)\}$, which appear in this realm, write the elements $g(x)N\{\gamma(x,y)\}$, without altering the equivalence of (a.).

That system becomes then

(a'.) $$[p, g(x)^2, g(x)N\{f(x,y)\}, g(x)N\{\gamma(x,y)\}, h(x,y)\}.$$

Again from the elements $pg(x)$, $g(x)^2$, $g(x)N\{f(x,y)\}$, $g(x)N\{\gamma(x,y)\}$ which are quantities of the system (a'.), we may form the system

$$g(x)[p, g(x), N\{f(x,y)\}, N\{\gamma(x,y)\}] \sim g(x)[p, g(x), f(x,y)],$$

where $f(x,y)$ is the greatest common divisor (modd. p, $g(x)$) of the elements $f_1(x,y)$, $f_2(x,y)$, ..., $\gamma_1(x,y)$, $\gamma_2(x,y)$, ... Hence the system (a'.) becomes

$$[p, g(x)^2, g(x)f(x,y), h(x,y)],$$

which system is equivalent to

$$[p, pg(x), g(x)^2, g(x)f(x,y), g(x)h(x,y), h(x,y)].$$

Further since

(c.) $$g(x)[p, g(x), f(x,y), h(x,y)] \sim g(x)[p, g(x), \theta(x,y)],$$

it follows on the one hand that

$$h(x,y) = pA + g(x)\Phi + \theta(x,y)\Theta$$

and on the other hand that

$$\theta(x,y) = pa+g(x)b+f(x,y)c+h(x,y)d.$$

Consequently

$$g(x)\theta(x,y) = pg(x)a+g(x)^2b+g(x)f(x,y)c+h(x,y)g(x)d,$$

so that the element $g(x)\theta(x,y)$ may be added to the given system, and when this has been done, it follows from (c.) that $g(x)f(x,y)$ may be omitted form this system, which has now the form

$$[p,\ g(x)^2,\ g(x)\theta(x,y),\ g(x)\Phi(x,y)+\theta(x,y)\Theta(x,y)].$$

We note 1^0, that $\theta(x,y)$ being the greatest common divisor (modd. $p, g(x)$) of the functions $f(x,y)$ and $h(x,y)$ its degree in either x or y cannot be greater than the degrees of either of those functions in the respective variables; when expanded in descending powers of y the coefficient of the highest power of $\theta(x,y)$ in y is unity, the others have been reduced (modd. $p, g(x)$); 2^0, owing to the presence of the element $g(x)\theta(x,y)$ in the system we may consider that the coefficients of $\Theta(x,y)$, when expanded in descending powers of y, have been reduced so that the coefficient of its highest power in y is unity, while the others are reduced (modd. $p, g(x)$); 3^0, the function $\Phi(x,y)$ is of less degree in y than the degree in that variable of the function $\theta(x,y)$ and all its coefficients have been reduced (modd. $p, g(x)$). The system in this form is a canonical form of the modular system considered (cf. this Journal, Bd. 119, p. 159).

When $g(x)$ occurs to the third power, the modular system is of the form

$$(\alpha.)\qquad [p,\ g(x)^3,\ g(x)^2N|f(x,y)|,\ g(x)N|h(x,y)|,\ N|k(x,y)|].$$

We construct the auxiliary modular system

$$(\beta.)\ [p,\ g(x)^2,\ g(x)N|h(x,y)|,\ N|k(x,y)|] \sim [p,\ g(x)^2,\ g(x)\bar{h}(x,y),\ \bar{k}(x,y)];$$

from which it follows at once on the one hand that

$$\bar{k}(x,y) = pM+g(x)^2N+g(x)\sum_i h_i(x,y)Q_i+\sum_j k_j(x,y)R_j.$$

If then we write

$$k(x,y) = \bar{k}(x,y)-g(x)^2N,$$

it is clear that we may add this element to the system $(\alpha.)$ without altering its equivalence.

On the other hand we have from $(\beta.)$

$$k_\nu(x,y) = pa_\nu+g(x)^2b'_\nu+g(x)\bar{h}(x,y)c_\nu+\bar{k}(x,y)d_\nu \qquad (\nu=1,2,\ldots),$$

or

$$k_\nu(x,y) = pa_\nu + g(x)^2 b_\nu + g(x)\bar{h}(x,y)c_\nu + k(x,y)d_\nu,$$

where

$$b_\nu = b'_\nu + Nd_\nu \qquad (\nu=1,2,\ldots).$$

Hence if we add $k(x,y)$ to the system $(\alpha.)$, we may write in that system instead of the elements $N\{k(x,y)\}$ the elements

$$g(x)^2 b_\nu + g(x)\bar{h}(x,y)c_\nu \qquad (\nu=1,2,\ldots).$$

We denote these elements by

$$\underset{\nu}{N}\{g(x)^2 b_\nu(x,y) + g(x)\bar{h}(x,y)c_\nu(x,y)\}.$$

The system $(\alpha.)$ becomes then

$$\begin{bmatrix} p,\ g(x)^3,\ g(x)^2 N\{f(x,y)\},\ g(x)N\{h(x,y)\}, \\ g(x)\underset{\nu}{N}\{g(x)b_\nu(x,y) + \bar{h}(x,y)c_\nu(x,y)\},\ k(x,y) \end{bmatrix},$$

which system, owing to the equivalence

$$\begin{bmatrix} p,\ g(x)^2,\ g(x)N\{f(x,y)\},\ N\{h(x,y)\} \\ \underset{\nu}{N}\{g(x)b_\nu(x,y) + h(x,y)c_\nu(x,y)\} \end{bmatrix} \backsim [p,\ g(x)^2,\ g(x)f(x,y),\ h(x,y)],$$

becomes

$$[p,\ g(x)^3,\ g(x)^2 f(x,y),\ g(x)h(x,y),\ k(x,y)].$$

It is easy to put this system in a canonical form similar to the one given in this Journal, loc. cit. p. 160.

The reduction of modular systems in which the irreducible (mod. p) function $g(x)$ occurs to the fourth or higher powers offers no difficulty.

Modular systems in which the prime integer p occurs to powers higher than the first.

Consider first the modular system

$$[p^2,\ pf(x),\ g(x)],$$

where $f(x)$ and $g(x)$ are quantities of the realm $[1,x]$, and p a prime integer.

Suppose next that $g(x)$ was reducible with respect to the moduli p^2, $pf(x)$, so that

$$g(x) = g_1(x)g_2(x) + pf(x)\psi(x) + p^2\chi(x),$$

the functions $\psi(x)$ and $\chi(x)$ being of the realm $[1,x]$. Further suppose that the functions $g_1(x)$ and $g_2(x)$ have no common factor with respect to the moduli p^2 and $pf(x)$. It follows at once that

$$[p^2, pf(x), g_1(x)]\,[p^2, pf(x), g_2(x)] \backsim [p^2, pf(x)g_1(x), pf(x)g_2(x), g(x) - pf(x)\psi(x)].$$

If it further happened that $g_1(x)$ and $g_2(x)$ have no common factor (mod. p), then

$$[p^2, pf(x)g_1(x), pf(x)g_2(x), g(x)-pf(x)\psi(x)] \sim [p^2, pf(x), g(x)].$$

Returning again to the system $[p^2, pf(x), g(x)]$ suppose first that $g(x)$ is irreducible (mod. p); then

$$[p^2, pf(x), g(x)] \sim [p^2, pf(x), pg(x), g(x)] \sim [p\,|\,p, f(x), g(x)\}, g(x)] \sim [p, g(x)],$$

unless $f(x)$ is a multiple of $g(x)$ and in that case

$$[p^2, pf(x), g(x)] \sim [p^2, g(x)].$$

As we are now considering only modular systems in which the prime integer occurs to a power higher than the first, we need consider only the latter case.

Next let $g(x)$ be an irreducible function (mod. p) in the system $[p^2, pf(x), g(x)^2]$; it follows then that

$$[p\,|\,p, f(x), g(x)^2\}, g(x)^2] \sim [p, g(x)^2]$$

unless $f(x)$ is a multiple of $g(x)$.

If this multiple >1, then

$$[p^2, pf(x), g(x)^2] \sim [p^2, g(x)^2];$$

and if this multiple $= 1$,

$$[p^2, pf(x), g(x)^2] \sim [p^2, pg(x), g(x)^2].$$

Further suppose that $g(x) \equiv g_1(x)g_2(x)$ (mod. p), and make the additional hypothesis that $g_1(x)$ and $g_2(x)$ are irreducible with repect to this modulus. Then as seen above

$$[p^2, pf(x), g(x)] \sim [p, g(x)],$$

if $f(x)$ is not divisible by either $g_1(x)$ or $g_2(x)$ (mod. p); but

$$[p^2, pf(x), g(x)] \sim [p^2, pg_1(x), g(x)],$$

when $f(x)$ is divisible by $g_1(x)$ but not by $g_2(x)$.

After making these preliminary remarks, consider the system

$$[p^2, g(x), pN\{f(x,y)\}, N\{h(x,y)\}],$$

and suppose first that $g(x)$ is irreducible (mod. p).

From the auxiliary system

$$[p, g(x), N\{h(x,y)\}] \sim [p, g(x), \bar{h}(x,y)]$$

we have on the one hand

$$\bar{h}(x,y) = pP + g(x)G + \sum_i h_i(x,y)H_i,$$

so that we may add the $h(x,y) = \bar{h}(x,y) - pP$ to the given modular system without altering its equivalence.

On the other hand we have

$$h_\nu(x,y) = p\pi'_\nu + g(x)\gamma_\nu + \bar{h}(x,y)\delta_\nu \qquad (\nu=1,2,\ldots),$$

or

$$h_\nu(x,y) = p\pi_\nu + g(x)\gamma_\nu + h(x,y)\delta_\nu,$$

where

$$\pi_\nu = \pi'_\nu + P\delta_\nu \qquad (\nu=1,2,\ldots).$$

Hence after we have added $h(x,y)$ to our modular system, we may write instead of the elements $N\{h(x,y)\}$ the elements $pN\{\pi(x,y)\}$, the system thus becoming

$$[p^2,\ g(x),\ pN\{f(x,y)\},\ pN\{\pi(x,y)\},\ h(x,y)].$$

In virtue of the equivalence

$$[p,\ g(x),\ N\{f(x,y)\},\ N\{\pi(x,y)\}] \backsim [p,\ g(x),\ f(x,y)],$$

the above system becomes:

$$[p^2,\ g(x),\ pf(x,y),\ h(x,y)].$$

It follows further from the auxiliary system

$$[p,\ g(x),\ f(x,y),\ h(x,y)] \backsim [p,\ g(x),\ \theta(x,y)],$$

that we may add the element $p\,\theta(x,y)$ to the given system; and, when this has been done, that we may drop from that system the element $p\,f(x,y)$. Owing to the auxiliary system we also have

$$h(x,y) = p\varphi(x,y) + g(x)\,G(x,y) + \theta(x,y)\,\Theta(x,y).$$

The reduced modular system consequently takes the form

$$[p^2, g(x),\ p\theta(x,y),\ p\varphi(x,y) + \theta(x,y)\,\Theta(x,y)].$$

When expanded in descending powers of y, the coefficients of the highest powers of y in both $\theta(x,y)$ and $\Theta(xy)$ are unity, while the other coefficients may be considered reduced (modd. $p, g(x)$). The degree of $\varphi(x,y)$ in y is less than that of $\theta(x,y)$ in y and all the coefficients may be considered reduced (modd. $p, g(x)$). The system is a canonical form of the modular system considered.

Systems in which the element $g(x)$ is reducible (mod. p).

Consider the system

(I.) $$[p^2, g(x),\ pN\{f(x,y)\},\ N\{h(x,y)\}],$$

and suppose that $g(x) \equiv g_1(x)g_2(x)$ (mod. p) but that $g_1(x)$ and $g_2(x)$ are irreducible (mod. p).

Form the auxiliary modular system

$$\text{(II.)}\quad [p, g(x), N|h(x,y)|] \sim [p, g_1(x), N|h(x,y)|]\,[p, g_2(x), N|h(x,y)|]$$
$$\sim [p, g_1(x), H_1(x,y)]\,[p, g_2(x), H_2(x,y)]$$
$$\sim [p, g(x), g_1(x)H_2(x,y), g_2(x)H_1(x,y), H_1(x,y)H_2(x,y)].$$

From this equivalence we have on the one hand, if we use the functional sign for the function itself:

$$h_\nu(x,y) = p\pi_\nu + g\gamma_\nu + g_1H_2\delta_\nu + g_2H_1\beta_\nu + H_1H_2\alpha_\nu \qquad (\nu=1,2,\ldots)$$

and on the other hand:

$$g_1(x)H_2(x,y) = pA_1 + gB_1 + \sum_i h_i(x,y)C_i^{(1)},$$
$$g_2(x)H_1(x,y) = pA_2 + gB_2 + \sum_i h_i(x,y)C_i^{(2)},$$
$$H_1(x,y)H_2(x,y) = pA_3 + gB_3 + \sum_i h_i(x,y)C_i^{(3)}.$$

We note that the product of the first two of these equations is identically equal to the last one multiplied by $g(x)$.

It is seen from this that we may add the elements

$$S_1 = g_1(x)H_2(x,y) - pA_1(x,y),$$
$$S_2 = g_1(x)H_1(x,y) - pA_2(x,y),$$
$$S_3 = H_1(x,y).H_2(x,y) - pA_3(x,y),$$

to the modular system (I.) without altering its equivalence.

We have further

$$h_\nu(x,y) = p[\pi_\nu + A_1\delta_\nu + A_2\beta_\nu + A_3\alpha_\nu] + g\gamma_\nu + S_1\delta_\nu + S_2\beta_\nu + S_3\alpha_\nu \qquad (\nu=1,2,\ldots).$$

Hence after we have added the elements S_1, S_2, S_3 to the system (I.) we may write in that system instead of the elements $h_\nu(x,y)$, the elements $pK_\nu(x,y)$, where we have written $K_\nu(x,y)$ for the expression

$$\pi_\nu + A_1\delta_\nu + A_2\beta_\nu + A_3\alpha_\nu \qquad (\nu=1,2,\ldots).$$

The system becomes then

$$\text{(I'.)}\qquad [p^2, g(x), pN|f(x,y)|, pN|K(x,y)|, S_1, S_2, S_3].$$

From the auxiliary modular system

$$[p, g(x), N|f(x,y)|, N|K(x,y)|]$$
$$\sim [p, g_1(x), N|f(x,y)|, N|K(x,y)|]\,[p, g_2(x), N|f(x,y)|, N|K(x,y)|]$$
$$\sim [p, g_1(x), F_1(x,y)]\,[p, g_2(x), F_2(x,y)]$$
$$\sim [p, g(x), g_1(x)F_2(x,y), g_2(x)F_1(x,y), F_1(x,y)F_2(x,y)],$$

it is seen that the system (I'.) may be written in the form

$$(\text{I}''.)\quad \left[\begin{array}{l|ll} p^2,\ g(x),\ p & g_1(x)\,F_2(x,y), & g_1(x)\,H_2(x,y)-pA_1(x,y), \\ & g_2(x)\,F_1(x,y), & g_2(x)\,H_1(x,y)-pA_2(x,y), \\ & F_1(x,y)\,F_2(x,y), & H_1(x,y)\,H_2(x,y)-pA_3(x,y) \end{array}\right].$$

To this system we may add the element $g_2(x)\{g_1(x)\,H_2(x,y)-pA_1(x,y)\}$, and consequently, owing to the presence of $g(x)$ in the system, the element $pg_2(x)A_1(x,y)$; in the same way we may add

$$pg_2(x)H_1(x,y),\ pg_1(x)A_2(x,y),\ pg_1(x)H_2(x,y),\ pH_1(x,y)H_2(x,y).$$

Form the equivalences:

1) $[p, g, F_1F_2, H_1H_2] \sim [p, g, g_1M_2, g_2M_1, M_1M_2]$,
2) $[p, g_2, F_2, A_2, H_2, M_2] \sim [p, g_2, L_2]$,
3) $[p, g_1, F_1, A_1, H_1, M_1] \sim [p, g_1, L_1]$.

In the formation of the equivalence 2) we observe that we have the elements p^2g_1, since p^2 is an element, pg or $pg_1.g_2$, pg_1F_2, pg_1A_2, pg_1H_2 and pg_1M_2, the last element coming from $p\,[p, g, F_1.F_2, H_1.H_2]$, which is to be added to the system (I''.).

We have from 2)

$$g_1H_2 = g_1\,[p\alpha+g_2\beta+L_2\gamma],$$

and from 3)

$$pA_1 = p\,[p\delta+g_1\zeta+L_1\eta];$$

and consequently

$$g_1H_2-pA_1 \equiv g_1L_2a_1+pg_1a_2+pL_1a_3 \ (\text{modd. } p^2,\ g(x)),$$

where I have written $a_1 = \gamma$, $\alpha-\zeta = a_2$ and $a_3 = -\eta$.

Similarly we have

$$g_2H_1-pA_2 \equiv g_2L_1b_1+pg_2b_2+pL_2b_3 \ (\text{modd. } p^2,\ g(x)),$$

$$H_1H_2-pA_3 \equiv M_1M_2c_1+g_1L_2c_2+g_2L\ c_3+pc_4+pg_1c_5+pg_2c_6 \ (\text{modd. } p^2,\ g(x)).$$

Hence the final form for the system (I.) is

$$\left[\begin{array}{l|ll} p^2,\ g,\ p & g_1\ L_2\ , & g_1L_2a_1+pg_1a_2+pL_1a_3\,, \\ & g_2\ L_1\ , & g_2L_1b_1+pg_2b_2+pL_2b_3\,, \\ & M_1M_2\ , & M_1M_2c_1+g_1L_2c_2+g_2L_1c_3+pc_4+pg_1c_5+pg_2c_6 \end{array}\right].$$

As a corollary consider the system

$$[p^2,\ pg_1(x),\ g(x),\ pN\{f(x,y)\},\ N\{h(x,y)\}]$$

where $g \equiv g_1.g_2 \ (\text{mod. } p)$, and where $g_1(x)$ and $g_2(x)$ are irreducible (mod. p).

This system reduces at once as in the case of the preceding system to the form

$$[p^2, pg_1, g, pN\{f(x,y)\}, pN\{k(x,y)\}, g_1H_2-pA_1, g_2H_1-pA_2, H_1H_2-pA_3],$$

a system which, owing to the equivalence

$$[p^2, pg_1, pN\{f(x,y)\}, pN\{k(x,y)\}] \sim p[p, g_1, F_1],$$

becomes:

$$[p^2, pg_1, g, pF_1, g_1H_2-pA_1, g_2H_1-pA_2, H_1H_2-pA_3].$$

We may add pg_2A_1 to this system, and owing to the presence of pg_1 within this system, also the element pg_1A_1.

Since the system

$$[p^2, pg_2A_1, pg_1A_1] \sim p\,[p, g_2A_1, g_1A_1] \sim p\,[p, A_1],$$

it is seen that we may add pA_1 to the system. We may add pg_2H_1 and consequently pH_1 to the system, which becomes

$$[p^2, pg_1.\ g, pF_1, pA_1, pH_1, g_1H_2, g_2H_1-pA_2, H_1H_2-pA_3];$$

owing to the equivalence

$$[p, g_1, F_1, A_1, H_1] \sim [p, g_1, L_1],$$

we have

$$H_1 = pa_1+g_1a_2+L_1a_3,$$

and consequently the modular system has the form

$$\left[\begin{array}{l} p^2, pg_1(x), g(x), pL_1(x,y), g_1(x)H_2(x,y), \\ \qquad g_2(x)L_1(x,y)a_3(x,y)+pg_2(x)a_1(x,y) \quad -pA_2(x,y) \\ \qquad L_1(x,y)H_2(x,y)a_3(x,y)+pH_2(x,y)a_1(x,y)-pA_3(x,y) \end{array}\right].$$

Suppose next that $g(x) \equiv g_1(x)g_2(x)g_3(x)$ ***(mod. p) and that the functions*** $g_1(x)$, $g_2(x)$ ***and*** $g_3(x)$ ***are irreducible (mod. p).***

Let the modular system under consideration be

(a.) $$[p^2, g(x), pN\{f(x,y)\}, N\{h(x,y)\}].$$

Form the modular system

$$\begin{aligned}[p, g(x), N\{h(x,y)\}] &\sim [p, g_1, N\{h(x,y)\}]\,[p, g_2, N\{h(x,y)\}]\,[p, g_3, N\{h(x,y)\}] \\ &\sim [p, g_1, H_1(x,y)]\,[p, g_2, H_2(x,y)]\,[p, g_3, H_3(x,y)] \\ &\sim [p, g, g_1g_2H_3, g_1g_3H_2, g_2g_3H_1, g_1H_2H_3, g_2H_1H_3, g_3H_1H_2, H_1H_2H_3],\end{aligned}$$

from which we have on the one hand

$$\begin{aligned}
g_1\, g_2 H_3 &= pA_1 + gB_1 + \Sigma h_i C_i^{(1)},\\
g_1\, g_3 H_2 &= pA_2 + gB_2 + \Sigma h_i C_i^{(2)},\\
g_2\, g_3 H_1 &= pA_3 + gB_3 + \Sigma h_i C_i^{(3)},\\
g_1 H_2 H_3 &= pA_4 + gB_4 + \Sigma h_i C_i^{(4)},\\
g_2 H_1 H_3 &= pA_5 + gB_5 + \Sigma h_i C_i^{(5)},\\
g_3 H_1 H_2 &= pA_6 + gB_6 + \Sigma h_i C_i^{(6)},\\
H_1 H_2 H_3 &= pA_7 + gB_7 + \Sigma h_i C_i^{(7)}.
\end{aligned}$$

We may therefore add the quantities

$$\begin{aligned}
g_1\, g_2 H_3 - pA_1 &= R_1,\\
g_1\, g_3 H_2 - pA_2 &= R_2,\\
g_2\, g_3 H_1 - pA_3 &= R_3,\\
g_1 H_2 H_3 - pA_4 &= R_4,\\
g_2 H_1 H_3 - pA_5 &= R_5,\\
g_3 H_1 H_2 - pA_6 &= R_6,\\
H_1 H_2 H_3 - pA_7 &= R_7,
\end{aligned}$$

to the given system without altering its equivalence.

It also follows on the other hand that

$$\begin{aligned}
h_\nu(x,y) = {} & pa'_\nu + gb_\nu + g_1 g_2 H_3 c_\nu^{(1)} + g_1 g_3 H_2 c_\nu^{(2)} + g_2 g_3 H_1 c_\nu^{(3)}\\
& + g_1 H_2 H_3 c_\nu^{(4)} + g_2 H_1 H_3 c_\nu^{(5)} + g_3 H_1 H_2 c_\nu^{(6)} + H_1 H_2 H_3 c_\nu^{(7)} \qquad (\nu = 1,2,\ldots)
\end{aligned}$$

or

$$h_\nu(x,y) = pa_\nu + gb_\nu + \sum_{i=1}^{i=7} R_i c_\nu^{(i)},$$

where

$$a_\nu = a'_\nu + \sum_{i=1}^{i=7} A_i c_\nu^{(i)} \qquad (\nu = 1,2,\ldots).$$

Hence after we have added the seven elements $\overset{i=7}{N}\{R_i\}$ to the modulas system we may add instead of the elements $N\{h(x,y)\}$ the elementr $pN\{a(x,y)\}$, the system thus becoming

$$\left[p^2,\ g(x),\ pN\{f(x,y)\},\ pN\{a(x,y)\},\ \overset{i=7}{N}\{R_i\}\right].$$

Owing to the equivalence

$$[p,\ g,\ N\{f(x,y),\ N\{a(x,y)\}] \sim$$

$$[p,\ g_1,\ N\{f(x,y)\},\ N\{a(x,y)\}]\ [p,\ g_2,\ N\{f(x,y)\},\ N\{a(x,y)\}]$$

$$[p,\ g_3,\ N\{f(x,y)\},\ N\{a(x,y)\}] \sim [p,\ g_1,\ K_1(x,y)]\ [p,\ g_2,\ K_2(x,y)]\ [p,\ g_3 K_3(x,y)]$$

$$\sim [p,\ g,\ g_1 g_2 K_3,\ g_1 g_3 K_2,\ g_2 g_3 K_1,\ g_1 K_2 K_3,\ g_2 K_1 K_3,\ g_3 K_1 K_2,\ K_1 K_2 K_3],$$

the system may be written

$$\left[\begin{array}{l|ll} p^2,\ g(x),\ p & g_1\,g_2K_3\,, & g_1\,g_2H_3-pA_1\,, \\ & g_1\,g_3K_2\,, & g_1\,g_3H_2-pA_2\,, \\ & g_2\,g_3K_1\,, & g_2\,g_3H_1-pA_3\,, \\ & g_1K_2K_3\,, & g_1H_2H_3-pA_4\,, \\ & g_2K_1K_3\,, & g_2H_1H_3-pA_5\,, \\ & g_3K_1K_2\,, & g_3H_1H_2-pA_6\,, \\ & K_1K_2K_3\,, & H_1H_2H_3-pA_7 \end{array}\right].$$

Since we may add $p(g_1g_2H_3-pA_1)$, it is seen that we may add to the system:

$$\begin{array}{l} pg_1g_2H_3,\ pg_1g_3H_2,\ pg_2g_3H_1, \\ pg_1g_2A_6,\ pg_1g_3A_5,\ pg_2g_3A_4, \\ pg_1H_2H_3,\ pg_2H_1H_3,\ pg_3H_1H_2, \\ pg_1Ag_3,\ p_2A_2,\ pg_3A_1,\ pH_1H_2H_3. \end{array}$$

We have therefore to form the systems

$$\begin{array}{l} [p^2,\ pg,\ pK_1K_2K_3,\ pH_1H_2H_3] \backsim p\,[p,\ g,\ K_1K_2K_3,\ H_1H_2H_3] \\ \quad \backsim p\,[p,\ g_1,\ S_1]\,[p,\ g_2,\ S_2]\,[p,\ g_3,\ S_3], \end{array}$$

or

1) $[p,\ g,\ K_1K_2K_3,\ H_1H_2H_3]$
$\quad \backsim [p,\ g,\ g_1g_2S_3,\ g_1g_3S_2,\ g_2g_3S_1,\ g_1S_2S_3,\ g_2S_1S_3,\ g_3S_1S_2,\ S_1S_2S_3]$,
2) $[p,\ g_2g_3,\ K_2K_3,\ H_2H_3,\ S_2S_3,\ A_3] \backsim [p,\ g_2g_3,\ g_2M_3,\ g_3M_2,\ M_2M_3]$,
3) $[p,\ g_1g_2,\ K_1K_2,\ H_1H_2,\ S_1S_2,\ A_1] \backsim [p,\ g_1g_2,\ g_1Q_2,\ g_2Q_1,\ Q_1Q_2]$,
4) $[p,\ g_1g_3,\ K_1K_3,\ H_1H_3,\ S_1S_3,\ A_2] \backsim [p,\ g_1g_3,\ g_1N_3,\ g_3N_1,\ N_1N_3]$,
5) $[p,\ g_3,\ K_3,\ H_3,\ S_3,\ M_3,\ N_3,\ A_6] \backsim [p,\ g_3,\ L_3]$,
6) $[p,\ g_2,\ K_2,\ H_2,\ S_2,\ M_2,\ Q_2,\ A_5] \backsim [p,\ g_2,\ L_2]$,
7) $[p,\ g_1,\ K_1,\ H_1,\ S_1,\ N_1,\ Q_1,\ A_4] \backsim [p,\ g_1,\ L_1]$.

We may therefore write our system in the form

$$\left[\begin{array}{l|ll} p^2,\ g(x),\ p & g_1\,g_2\,L_3\,, & g_1\,g_2H_3-p\,A_1\,, \\ & g_1\,g_3\,L_2\,, & g_1\,g_3H_2-p\,A_2\,, \\ & g_2\,g_3\,L_1\,, & g_2\,g_3H_1-p\,A_3\,, \\ & g_1M_2M_3\,, & g_1H_2H_3-p\,A_4\,, \\ & g_2N_1N_3\,, & g_2H_1H_3-p\,A_5\,, \\ & g_3Q_1Q_2\,, & g_3H_1H_2-p\,A_6\,, \\ & S_1\,S_2\,S_3\,, & H_1H_2H_3-p\,A_7\,. \end{array}\right]$$

where, if we make use of the formulae 4), 5), 6) and 7), $g_1g_2H_3-pA_1$ has the form:

$$g_1g_2H_3-pA_1 \equiv g_1g_2L_3a_1+pg_1L_2a_2+pg_2L_1a_3+pg_1g_2a_4+pQ_1Q_2a_5 \text{ (modd. } p^2,\ g(x)),$$

and similarly:

$$g_1g_3H_2-pA_2 \equiv g_1g_3L_2b_1+pg_1L_3b_2+pg_3L_1b_3+pg_1g_3b_4+pN_1N_3b_5 \text{ (modd. } p^2,\ g(x)),$$
$$g_2g_3H_1-pA_3 \equiv g_2g_3L_1c_1+pg_2L_3c_2+pg_3L_2c_3+pg_2g_3c_4+pM_2M_3c_5 \text{ (modd. } p^2,\ g(x)),$$
$$g_1H_2H_3-pA_4 \equiv g_1g_2L_3d_1+g_1g_3L_2d_2+g_1M_2M_3d_3+pg_1g_2d_4 + pg_1g_3d_5+pg_1d_6+pL_1d_7 \text{ (modd. } p^2,\ g(x)),$$
$$g_2H_1H_3-pA_5 \equiv g_1g_2L_3e_1+g_2g_3L_1e_2+g_2N_1N_3e_3+pg_1g_2e_4 + pg_2g_3e_5+pg_2e_6+pL_2e_7 \text{ (modd. } p^2,\ g(x)),$$
$$g_3H_1H_2-pA_6 \equiv g_1g_3L_2m_1+g_2g_3L_1m_2+g_3Q_1Q_2m_3+pg_1g_3L_2m_4 + pg_2g_3m_5+pg_3m_6+pL_3m_7 \text{ (modd. } p^2,\ g(x)),$$
$$H_1H_2H_3-pA_7 \equiv S_1S_2S_3n_1+g_1g_2L_3n_2+g_1g_3L_2n_3+g_2g_3L_1n_4+g_1M_2M_3n_5 + g_2N_1N_3n_6+g_3Q_1Q_2n_7+pg_1g_2n_8+pg_1g_3n_9+pg_2g_3n_{10}+pg_1n_{11} + pg_2n_{12}+pg_3n_{13}+pn_{14} \text{ (modd. } p^2,\ g(x)).$$

Reduction of the modular system

$$[p^2,\ g(x)^2,\ pN\{f(x,y)\},\ g(x)N\{h(x,y)\},\ pg(x)N\{k(x,y)\},\ N\{m(x,y)\}],$$

where $g(x)$ *is an irreducible function* (mod. p).

We form the auxiliary modular system

$$p[p,\ g(x)^2,\ g(x)N\{h(x,y)\},\ N\{m(x,y)\}] \sim p[p,\ g(x)^2,\ g(x)H(x,y),\ M(x,y)];$$

from which we have on the one hand:

$$m_\nu(x,y) = pa'_\nu+g^2b_\nu+gHc_\nu+Md_\nu \qquad (\nu=1,2,\ldots),$$
$$g(x)h_\mu(x,y) = pe'_\mu+g^2r_\mu+gHs_\mu+Mt_\mu \qquad (\mu=1,2,\ldots),$$

and on the other hand:

$$M(x,y) = pA+g^2B+g\sum_i h_ib_i+\sum_i m_iE_i,$$
$$g(x)H(x,y) = pA_1+g^2N+g\sum_i h_iP_i+\sum_i m_iR_i.$$

We may therefore add

$$M(x,y)-pA = S,$$
$$g(x)H(x,y)-pA_1 = S_1,$$

to the given modular system.

Further since

$$m_\nu(x,y) = pa_\nu+g^2b_\nu+S_1c_\nu+Sd_\nu,$$

where

$$a_\nu = a'_\nu + A_1 c_\nu + A d_\nu \qquad (\nu=1,2,\ldots)$$

and

$$g(x)h_\mu(x,y) = pe_\mu + g^2 r_\mu + S_1 s_\mu + S t_\mu,$$

where

$$e_\mu = e'_\mu + A_1 s_\mu + A t_\mu \qquad (\mu=1,2,\ldots),$$

we may instead of the elements $N\{m(x,y)\}$ and $g(x)N\{h(x,y)\}$ write the elements $pN\{a(x,y)\}$ and $pN\{e(x,y)\}$ in our modular system, which becomes

$$[p^2, g^2, pN\{f(x,y)\}, pgN\{k(x,y)\}, pN\{a(x,y)\}, pN\{e(x,y)\}, S_1, S].$$

Further since

$$[p, g^2, N\{(f(x,y)\}, gN\{k(x,y)\}, N\{a(x,y)\}, N\{e(x,y)\}] \sim [p, g^2, gL, V],$$

the system may be written

$$[p^2, g^2, pgL, pV, S_1, S].$$

Since $S = M - pA$, $S_1 = gH - pA_1$, we may add the elements pM, pgA_1, pgH to the system.

Write

$$1) \qquad [p, g^2, V, M] \sim [p, g^2, gW, Z],$$

and

$$2) \qquad [p, g, L, W, A_1, H] \sim [p, g, Y].$$

The system is then

$$[p^2, g^2, pgY, pZ, gH - pA_1, M - pA]$$

where from 1) and 2) $gH - pA_1$ and $M - pA$ have the form

$$gH - pA_1 \equiv gYa_1 + pgb_1 + pYc_1 \text{ (modd. } p^2, g(x)^2),$$
$$M - pA \equiv Za + gb + pc \text{ (mod. } g(x)^2).$$

Reduction of modular systems in which the prime integer p occurs to the third power.

Consider first the system

$$[p^3, p^2 h(x), pk(x), g(x)],$$

and suppose that $g(x)$ is irreducible (mod. p).

The system

$$[p^3, p^2 k(x), p^2 g(x)] \sim p^2[p, k(x), g(x)] \sim p^2[1],$$

unless $k(x) = g(x)\bar{g}(x) + p\varphi(x)$, and consequently unless $pk(x) \equiv p^2\varphi(x)$ (mod. $g(x)$).

We have in this case

$$[p^3, p^2h(x), p^2\varphi(x), g(x)].$$

But the system

$$[p^3, p^2h(x), p^2\varphi(x), p^2g(x)]$$

is equivalent to

$$p^2[p, h(x), \varphi(x), g(x)] \sim p^2[1],$$

unless

$$h(x) = g(x)\gamma(x)+p\chi(x),$$

and

$$\varphi(x) = g(x)k(x)+p\psi(x).$$

Hence $p^2h(x)$ and $p^2\varphi(x)$ may be omitted from the system, which becomes then

$$[p^3, g(x)].$$

The system $[p^3, g(x), p^2N\{f(x,y)\}, pN\{h(x,y)\}, N\{k(x,y)\}]$ *reduces without any trouble to the form*

$$[p^3, g(x), p^2F(x,y), pH(x,y), K(x,y)].$$

The reduction of the system

$$[p^3, g(x), p^2N\{f(x,y)\}, pN\{h(x,y), N\{k(x,y)\}]$$

where $g(x) \equiv g_1(x).g_2(x)$ (mod.p) *and where* $g_1(x)$ *and* $g_2(x)$ *are irreducible* (mod. p).

From the auxiliary system

$$[p^2, g(x), pN\{h(x,y)\}, N\{k(x,y)]$$

$$\sim \left[\begin{array}{l|ll} p^2, g(x), p & g_1 L_2, & S_1 \\ & g_2 L_1, & S_2 \\ & M_1 M_2, & S_3 \end{array}\right],$$

we have on the one hand

$$k_\nu(x,y) = p^2a'_\nu+gb_\nu+pg_1L_2c_\nu+pg_2L_1d_\nu+pM_1M_2e_\nu+S_1\alpha_\nu+S_2\beta_\nu+S_3\gamma_\nu \quad (\nu=1,2,\ldots),$$

and on the other hand

$$S_1 = p^2A_1+gB_1+p\sum_i h_i(x,y)C_i^{(1)}+\sum_i k_i(x,y)D_i^{(1)},$$
$$S_2 = p^2A_2+gB_2+p\sum_i h_i(x,y)C_i^{(2)}+\sum_i k_i(x,y)D_i^{(2)},$$
$$S_3 = p^2A_3+gB_3+p\sum_i h_i(x,y)C_i^{(3)}+\sum_i k_i(x,y)D_i^{(3)}.$$

From this it is seen that the quantities

$$T_1 = S_1 - p^2 A_1 ,$$
$$T_2 = S_2 - p^2 A_2 ,$$
$$T_3 = S_3 - p^2 A_3$$

may be added to the given system.

It follows also that

$$k_\nu(x,y) = p^2 a_\nu + g b_\nu + p g_1 L_2 c_\nu + p g_2 L_1 d_\nu + p M_1 M_2 e_\nu + T_1 \alpha_\nu + T_2 \beta_\nu + T_3 \gamma_\nu ,$$

where

$$a_\nu = a'_\nu + A_1 \alpha_\nu + A_2 \beta_\nu + A_3 \gamma_\nu \qquad (\nu = 1, 2, \ldots).$$

Hence instead of the elements $N\{k(x,y)\}$ we may add to the given modular system the elements

$$N_\nu \{p^2 a_\nu + p g_1 L_2 c_\nu + p g_2 L_1 d_\nu + p M_1 M_2 e_\nu\},$$

which becomes then

$$\left[p^3,\ g,\ p^2 N\{f(x,y)\},\ pN\{h(x,y)\},\ pN_\nu\{pa_\nu + g_1 L_2 c_\nu + g_2 L_1 d_\nu + M_1 M_2 e_\nu\}, T_1,\ T_2,\ T_3 \right],$$

a system, which owing to the equivalence

$$p[p^2,\ g,\ pN\{f(x,y)\},\ N\{h(x,y)\},\ N_\nu\{pa_\nu + g_1 L_2 c_\nu + g_2 L_1 d_\nu + M_1 M_2 e_\nu\}]$$
$$\backsim p \left[\begin{array}{c|ll} p^2,\ g,\ p & g_1 N_2 , & R_1 \\ & g_2 N_1 , & R_2 \\ & Q_1 Q_2 , & R_3 \end{array} \right],$$

way be written in the form

$$\left[\begin{array}{c|ll|ll} p^3,\ g,\ p^2 & g_1 N_2 , & p & R_1 , & T_1 \\ & g_2 N_1 , & & R_2 , & T_2 \\ & Q_1 Q_2 , & & R_3 , & T_3 \end{array} \right].$$

In this system the functions $R_1, R_2, \ldots$ have the form

$$R_1 = g_1 M_2 - pC_1 , \qquad T_1 = g_1 P_2 - pB_1 - p^2 A_1 ,$$
$$R_2 = g_2 M_1 - pC_2 , \qquad T_2 = g_2 P_1 - pB_2 - p^2 A_2 ,$$
$$R_3 = M_1 M_2 - pC_3 , \qquad T_3 = P_1 P_2 - pB_3 - p^2 A_3 .$$

We may therefore add $p^2 R_1$ to the system, or the element $p^2 g_1 M_2$ and in the same way the elements $p^2 g_2 M_1$, $p^2 g_2 C_1$, $p^2 g_1 P_2$, $p^2 g_2 B_1$, etc. and continue the reduction as on p. 281.

As a corollary to the reduction of the above system consider the system

$$[p^3,\ p^2g_2,\ pg_1,\ g,\ p^2N\{f(x,y)\},\ pN\{h(x,y)\},\ N\{k(x,y)\}],$$

where $g \equiv g_1 \cdot g_2 \pmod{p}$ and g_1 is irreducible (mod. p).

Since

$$[p^3,\ p^2g_1,\ p^2g_2] \backsim p^2[p,\ g_1,\ g_2] \backsim p^2[1],$$

unless

$$g_2 = g_1 \cdot \bar{g}_1 + p\chi,$$

so that

$$p^2g_2 = p^2g_1 \cdot \bar{g}_1 + p^3\chi,$$

it follows that p^2g_2 must be omitted from the system; otherwise it is not of the form considered.

The system may therefore, as above, be written in the form

$$[p^3,\ pg_1,\ g,\ p^2N\{f(x,y)\},\ pN\{h(x),y\}$$
$$pN\{pa_\nu + g_1L_2c_\nu + g_2L_1d_\nu + M_1M_2e_\nu\},\ T_1,\ T_2,\ T_3]$$
$$\backsim [p^3,\ pg_1,\ g,\ p^2F,\ pH,\ T_1,\ T_2,\ T_3].$$

Here, as above, the elements T_1, T_2, T_3 have the form

$$T_1 = g_1P_2 - pB_1 - p^2A_1,$$
$$T_2 = g_2P_1 - pB_2 - p^2A_2,$$
$$T_3 = P_1P_2 - pB_3 - p^2A_3.$$

We may therefore add to the system the element p^2B_1. Hence if the system does not reduce to one in which the prime integer occurs only to the second power, B_1 must have the form $B_1 = g_1B_1' + p\varphi$, and hence in the modular system T_1 has the form $g_1P_2 - p^2A_1'$. It follows then that we may also add $p^2g_2A_1'$ to the system. If we suppose that g_2 is irreducible (mod. p), then A_1' must be divisible by $g_1(x)$ mod. p, and consequently the element T_1 takes the form g_1P_2 and the system reduces to

$$[p^3,\ pg_1,\ g,\ p^2F,\ pH,\ g_1P_2,\ g_2P_1 - pB_2 - p^2A_2,\ P_1P_2 - pB_3 - p^2A_3].$$

To this system we may also add p^2T_2 or $p^2g_2P_1$, and owing to the presence of pg_1 in the system also $p^2g_1P_1$. Owing to the equivalence $[p^3,\ p^2g_1P_1,\ p^2g_2P_1] \backsim p^2[p,\ g_1P_1,\ g_2P_1] \backsim p^2[p,\ P_1]$, it follows that we may add p^2P_1 to the system and finally combine p^2F with p^2P_1 as we have repeatedly done.

The reduction of the modular system

$$[p^3,\ g,\ p^2N\{f(x,y)\},\ pN\{h(x,y)\},\ N\{k(x,y)\}],$$

where $g \equiv g_1g_2g_3 \pmod{p}$ *and* g_1, g_2, g_3 *are irreducible* (mod. p).

Applying the same principles as on p. 282 this system is seen to be equivalent to

$$\left[\begin{array}{l|l|ll|ll} p^3,\ g,\ p^2 & g_1\,g_2W_3\,, & p & V_1\,, & U_1 \\ & g_1\,g_3W_2\,, & & V_2\,, & U_2 \\ & g_2\,g_3W_1\,, & & V_3\,, & U_3 \\ & g_1T_2\ T_3\,, & & V_4\,, & U_4 \\ & g_2X_1\ X_3\,, & & V_5\,, & U_5 \\ & g_3\,Y_1\ Y_2\,, & & V_6\,, & U_6 \\ & Z_1\,Z_2\,Z_3\,, & & V_7\,, & U_7 \end{array}\right],$$

Where the elements $V_1, V_2, \ldots, U_1, U_2, \ldots$ have the form

$$\begin{aligned} V_1 &= g_1\,g_2M_3 - pC_1\,, & U_1 &= g_1\,g_2H_3 - pB_1 - p^2A_1\,, \\ V_2 &= g_1\,g_3M_2 - pC_2\,, & U_2 &= g_1\,g_3H_2 - pB_2 - p^2A_2\,, \\ V_3 &= g_2\,g_3M_1 - pC_3\,, & U_3 &= g_2\,g_3H_1 - pB_3 - p^2A_3\,, \\ V_4 &= g_1M_2M_3 - pC_4\,, & U_4 &= g_1H_2H_3 - pB_4 - p^2A_4\,, \\ V_5 &= g_2M_1M_3 - pC_5\,, & U_5 &= g_2H_1H_3 - pB_5 - p^2A_5\,, \\ V_6 &= g_3M_1M_2 - pC_6\,, & U_6 &= g_3H_1H_2 - pB_6 - p^2A_6\,, \\ V_7 &= M_1M_2M_3 - pC_7\,, & U_7 &= H_1H_2H_3 - pB_7 - p^2A_7. \end{aligned}$$

We may add to this system p^2V_1 or $p^2g_1g_2M_3$, pg_3U_1 or $p^2g_3B_1$, etc. We may then continue the reduction as on p. 284.

The preceding reductions have all been made for systems having the form

$$[N\{m\},\ N\{g(x)\},\ N\{f(x,y)\}].$$

We have therefore assumed the presence of an integer and an integral function of one variable with integral coefficients within these systems.

If the system is given to us in the form

$$[N\{f(x,y)\}],$$

then, since the functions $f_1(x,y), f_2(x,y), \ldots$ have not all a common divisor (as such a divisor may be always taken out as a divisor of the system), it is in general possible to find functions $\bar{f}_1(x,y), \bar{f}_2(x,y), \ldots$ such that

$$f_1(x,y)\,\bar{f}_1(x,y) + f_2(x,y)\,\bar{f}_2(x,y) + \cdots = g(x),$$

where $g(x)$ belongs to the realm $[1, x]$.

When there is no solution common to any two of the equations $f_1(x,y) = 0$, $f_2(x,y) = 0, \ldots$, we may by the algorithm of the greatest common divisor determine functions $\bar{f}_1(x,y)$, $\bar{f}_2(x,y)$ which produce the identical relation

$$f_1(x,y)\,\bar{f}_1(x,y) + f_2(x,y)\,\bar{f}_2(x,y) + \cdots = m$$

where m is an integer.

Geometrically interpreted the curves $f_1(x,y) = 0$, $f_2(x,y) = 0, \ldots$ have in this case no point of intersection or contact. They are, so to speak, isolated curves.

Neglecting for the time being this very special case, our hypotheses amount only to the supposition of the existence of an integer within the given system. In other words we suppose that we may produce integers by linear combinations of the elements of the system, the coefficients being quantities of the realm of integrity $[1, x, y]$. For example grant that we may effect the presence of two functions $g_1(x)$ and $g_2(x)$, such as $g(x)$ above, and that there is no value of x which causes both of these functions to vanish simultaneously; we may then by the algorithm of the greatest common divisor derive two functions $\bar{g}_1(x)$ and $\bar{g}_2(x)$ belonging to the realm $[1, x]$ such that

$$g_1(x)\,\bar{g}_1(x) + g_2(x)\,\bar{g}_2(x) = m,$$

where m is an integer.

Suppose, however, that we *have modular systems in which it is not possible to introduce integers as elements.*

As the simplest case consider a system of the form

$$[g(x), f_1(x,y), f_2(x,y)]$$

where $g(x)$ is a linear function of the elements $f_1(x,y)$ and $f_2(x,y)$ whose coefficients belong to the realm $[1, x, y]$.

As no integers appear as elements in the system, we shall do away with the restriction that only integers may enter the realm of rationality, and shall also allow rational numbers to enter this realm, although the functions that enter must be integral in x and y.

Suppose then that $f_1(x,y) = h_1(x) f_1^{(1)}(x,y)$, then if $h_1(x)$ is not a divisor of $g(x)$, the element $h_1(x) f_1^{(1)}(x,y)$ may be replaced by an element

$d_1(x)f_1^{(1)}(x,y)$, where $d_1(x)$ is a divisor of $g(x)$ and this may be done without altering the equivalence of the system.

For if we denote the greatest common divisor of $g(x)$ and $h_1(x)$ by $d_1(x)$ we may always determine belonging to our fixed realm of rationality two functions $\bar{g}(x)$ and $\bar{h}_1(x)$ so that

$$g(x)\bar{g}(x)+h_1(x)\bar{h}_1(x) = d_1(x),$$

where $d_1(x)$ likewise belongs to this realm.

From this it follows that we may add $d_1(x)f_1(x,y)$ to the given, and as $h_1(x)f_1(x,y)$ is a multiple of this element, drop it from the system.

If further $g(x) = g_1(x)\,g_2(x)$ and if $g_1(x)$ and $g_2(x)$ have no common divisor, we may by the algorithm of the greatest common divisor determine two functions $\bar{g}_1(x)$ and $\bar{g}_2(x)$ which belong to the fixed realm of rationality and which satisfy the identical relation

$$g_1(x)\,\bar{g}_1(x)+g_2(x)\,\bar{g}_2(x) = 1.$$

As a consequence of this the system $[g(x), f_1(x,y), f_2(x,y)]$ is equivalent to the product of the two systems

$$[g_1(x), f_1(x,y), f_2(x,y)] \text{ and } [g_2(x), f_1(x,y), f_2(x,y)].$$

We have then to consider the systems of the forms

$$[p(x)^n, p(x)^{n_1}f_1(x,y), p(x)^{n_2}f_2(x,y)],$$

where $p(x)$ is an irreducible integral function in x and the integers n_1 and n_2 are divisors of the integer n. The reduction of these systems may be performed in precisely the same manner as the systems which are treated in this Journal, Bd. 119, p. 153 *et seq.*, with the condition here that we admit into the realm of rationality integral functions in x and y with rational coefficients.

We have finally to consider systems of the form

$$[m, f_1(x,y), f_2(x,y)]$$

where the integer m is a linear function of the two elements $f_1(x,y)$ and $f_2(x,y)$ the coefficients being quantities of the realm of integrity $[1, x, y]$.

By processes already repeatedly employed the reduction of this system may be reduced to the reduction of systems of the form

$$[p^n, p^{n_1}f_1(x,y), p^{n_2}f_2(x,y)]$$

where p is a prime integer, and the integers n_1, n_2 divisors of the integer n. We may further assume that the coefficients of the highest power of both the elements $f_1(x,y)$ and $f_2(x,y)$ when expanded in descending powers of either x or y are either unity or powers of p, while the other coefficients have all been reduced with respect to a definite power of p as a modulus. But we are not able to carry the reduction further unless we admit into the realm of rationality rational functions of one of the variables, and then the reduction may be performed in the same way as the systems just mentioned above.

Modular Systems whose elements are functions of three variables.

Consider first the system

$$[p,\ g(x),\ f(x,y),\ N|h(x,y,z)|],$$

where p is a prime integer, $g(x)$ is an irreducible integral function in x (mod. p) with integral coefficients and $f(x,y)$ is an irreducible integral function in x,y (modd. p, $g(x)$) with integral coefficients. The functions $h_1(x,y,z)$, $h_2(x,y,z)$, ... belong to the realm of integrity $[1, x,y,z]$ and when expanded in descending powers of z have the form.

$$h(x,y,z) = a_0(x,y)z^n + a_1(x,y)z^{n-1} + \cdots + a_n(x,y),$$

the functions $a_0(x,y)$, $a_1(x,y)$, ..., $a_n(x,y)$ belonging to the realm of integrity $[1, x,y]$.

We may find two integral functions with integral coefficients $\bar{a}_0(x,y)$ and $\bar{f}(x,y)$ such that

$$a_0(x,y)\,\bar{a}_0(x,y) + f(x,y)\,\bar{f}(x,y) = k(x),$$

where $k(x)$ is an integral function in x with integral coefficients and is not congruent to zero (modd. p, $g(x)$). Of course, those coefficients of $h(x,y,z)$ which contain $f(x,y)$ as a factor (modd. p, $g(x)$) are supposed to have been dropped from the discussion.

We may further determine two integral functions with integral coefficients $\bar{g}(x)$, $\bar{k}(x)$ so that

$$k(x)\bar{k}(x) + g(x)\bar{g}(x) = c,$$

where c is a constant and $\not\equiv 0$ (mod. p), and therefore finally we may determine two constants $\bar{p}$ and $\bar{c}$ which satisfy the expression

$$c\bar{c} + p\bar{p} = 1.$$

From this it follows, since the equivalence of the modular system is not altered (cf. p. 269) when we replace an element $h(x,y,z)$ by this element multiplied by any one of the system of incongruent residues (modd. p, $g(x)$, $f(x,y)$), that instead of the function $h(x,y,z)$ we may determine a function $H(x,y,z)$ in which the coefficient of the highest power of z is unity while the other coefficients have been reduced (modd. p, $g(x)$, $f(x,y)$). We call $H(x,y,z)$ the reduced element of $h(x,y,z)$.

Replacing then the elements $h(x,y,z)$ by their reduced elements $H(x,y,z)$, which we suppose have been arranged in the modular system according to their highest powers in z, the largest coming first, we derive by division the expression

$$H_1 = Q_1 H_2 + R_1,$$

where Q_1 and R_1 are quantities belonging to the realm $[1, x, y, z]$. We may consequently omit H_1 from the system, if to it we add the element R_1. Let H_3 be the reduced element of R_1.

Continuing the process we have

$$H_2 = Q_2 H_3 + R_2,$$
$$\ldots\ldots\ldots\ldots$$

Proceding in this way, since the degrees of the functions in z that we adjoin to the system, are being continuously decreased without becoming negative, we must finally have

$$H_{\nu-2} = Q_{\nu-2} H_{\nu-1} + R_{\nu-2},$$
$$H_{\nu-1} = Q_{\nu-1} H_{\nu},$$

where H_ν is the reduced element of $R_{\nu-2}$.

If in this reduction it happened that $R_{\nu-2}$ was of the zero degree in z, and was not congruent to zero (modd. p, $g(x)$, $f(x,y)$), then it would be possible to determine two functions of the realm $[1, x, y]$, $\bar{R}_{\nu-2}$ and $\bar{f}$ so that

$$R_{\nu-2}\bar{R}_{\nu-2} + f\bar{f} = L(x),$$

where $L(x)$ belongs to the realm $[1, x]$ and $\not\equiv 0$ (modd. p, $g(x)$); we may consequently find belonging to the realm $[1, x]$ two functions $\bar{L}(x)$ and $\bar{g}(x)$ such that

$$L(x)\bar{L}(x) + g(x)\bar{g}(x) = c,$$

in which expression the integer $c \not\equiv 0 \pmod{p}$. We may finally find two integers $\bar{c}$ and $\bar{p}$ satisfying the identity

$$c\bar{c}+p\bar{p} = 1.$$

From this it is seen that unity becomes an element of the system, and therefore the system is a unit-system.

If then our system is not a unit-system, we may determine the element H_ν, which is a divisor of both the elements H_1 and H_2 (modd. p, $g(x)$, $f(x,y)$) and we may therefore replace these elements by the one element $H_\nu(x,y,z)$.

Proceeding in the same way it is seen (in case the system is not a unit-system) that we may replace all the elements $H_1, H_2, \ldots$ by the one element H, which may be regarded as the greatest common divisor of these elements (modd. p, $g(x)$, $f(x,y)$).

Our system reduces then to the form

$$[p,\ g(x),\ f(x,y),\ H(x,y,z)].$$

We consider next the system

$$[p,\ g(x),\ f(x,y),\ N\{h(x,y,z)\}],$$

in which $f(x,y) \equiv f_1(x,y)f_2(x,y) \pmod{p,\ g(x)}$ and where $f_1(x,y)$ and $f_2(x,y)$ are irreducible with respect to these moduli. It is seen at once that

$$[p,\ g(x),\ f(x,y),\ N\{h(x,y,z)\}] \sim [p,\ g(x),\ f_1(x,y),\ N\{h(x,y,z)\}]\ [p,\ g(x),\ f_2(x,y),\ N\{h(x,y,z)\}].$$

It remains then to consider modular systems having the forms following:

Take first the system

$$[p,\ g(x),\ f(x,y)^2,\ f(x,y)N\{h(x,y,z)\},\ N\{k(x,y,z)\}],$$

where the function $f(x,y)$ is irreducible (modd. p, $g(x)$).

It may be shown as on p. 275 that this system takes the form

$$[p,\ g(x),\ f(x,y)^2,\ f(x,y)H(x,y,z),\ K(x,y,z)].$$

If further we write

$$[p,\ g(x),\ f(x,y),\ H(x,y,z),\ K(x,y,z)] \sim [p,\ g(x),\ f(x,y),\ L(x,y,z)],$$

it is seen that $f(x,y)L(x,y,z)$ may be added to the system (a.) and then $f(x,y)H(x,y,z)$ may be dropped from this system. It also follows from this latter system that

$$K(x,y,z) = pA+gB+fC+LD,$$

where A, B, C, D are quantities belonging to the realm of integrity $[1, x, y, z]$, and so we may therefore write our system in the form

$$[p,\ g(x),\ f(x,y)^2,\ f(x,y)\,L(x,y,z),\ f(x,y)\,C(x,y,z)+L(x,y,z)\,D(x,y,z)].$$

In the same way

$$[d,\ g(x),\ f(x,y)^3,\ f(x,y)^2 N\{h(x,y,z)\},\ f(x,y) N\{k(x,y,z)\},\ N\{l(x,y,z)\}]$$
$$\backsim [p,\ g(x),\ f(x,g)^3,\ f(x,y)^2 H(x,y,z),\ f(x,y) K(x,y,z),\ L(x,y,z)],$$

etc.

The systems in which the prime integer p, or the function $g(x)$ occurs to powers higher than the first are reduced in exactly the same manner as those already discussed for modular systems in which the elements involve only two variables.

If instead of the systems of the above form, we take the system

$$[N\{h(x,y,z)\}],$$

then, since the elements $h_1(x,y,z)$, $h_2(x,y,z)$, ... have no common divisor, it is in general possible to determine belonging to the realm $[1, x, y, z]$ functions $\bar{h}_1(x,y,z)$, $\bar{h}_2(x,y,z)$, ... such that

$$\text{(a.)} \qquad h_1(x,y,z)\,\bar{h}_1(x,y,z)+h_2(x,y,z)\,\bar{h}_2(x,y,z)+\cdots = f(x,y),$$

where $f(x,y)$ is a function belonging to the realm $[1, x, y]$.

In order then to say that the system $[N\{h(x,y,z)\}]$ is reducible to the form $[p, g(x), f(x,y), H(x,y,z)]$, we must assume that the given system contains integers and integral functions of one variable. If we do away with the assumption that there exist integers in the system, we may make the same reductions indicated above, if we change the realm of integrity by admitting into it also rational numbers as well as integers. If further we do away with the restriction that there must be present within the system integral functions of one variable, our reductions are still applicable, if we also admit into the realm of rationality in the place of integers and integral functions of that variable rational numbers and rational functions of the variable.

If, as a special case, the linear form (a.) is

$$h_1(x,y,z)\,\bar{h}_1(x,y,z)+h_2(x,y,z)\,\bar{h}_2(x,y,z)+\cdots = m(x)$$

where $m(x)$ is an integral function in x with integral coefficients, then we may replace the system by the product of several systems in which corresponding to the element $m(x)$ there appears the irreducible function $g(x)$.

or a power of this function. To do this, however, we have to extend the realm of integrity by admitting within it rational numbers.

Suppose then, as on p. 293, that the functions $h_1(x,y,z)$, $h_2(x,y,z)$, ... have the form

$$h(x,y,z) = a_0(x,y)z^n + a_1(x,y)z^{n-1} + \cdots + a_n(x,y),$$

and that we may write

$$a_0(x,y) = a_{00}(y)y^m + a_{01}(x)y^{m-1} + \cdots + a_{0m}(x),$$

then we can find a function $\bar{a}_{00}(x)$ such that

$$a_{00}(x)\bar{a}_{00}(x) \equiv 1 \pmod{g(x)}.$$

We may therefore replace $h(x,y,z)$ by $\bar{a}_{00}(x)h(x,y,z) = H(x,y,z)$, say, where $H(x,y,z)$ when expanded is

$$H(x,y,z) = y^m z^n + A_1(x,y)z^{n-1} + \cdots + A_n(x,y),$$

the functions $A_1(x,y), \ldots A_n(x,y)$ being integral in x and y with rational coefficients. We may consequently perform all the reductions given in this paper, if we further admit into the realm of rationality rational functions of either of the variables y or z.

Geometrically interpreted, the given functions placed = 0 are equations of algebraic surfaces. In that we have taken outside of the system the greatest common divisor of the elements, if there exists one, there is no surface area common to all the surfaces. If there are n elements $h_1(x,y,z)$, $h_2(x,y,z), \ldots h_n(x,y,z)$, it may however happen that $n-1$ of them have a portion of surface area in common. This surface area may intersect the other surface and the projection of the curve thereby produced upon the xy-plane is contained as a factor in the function $f(x,y)$ of formula (a.).

It may further happen that a of these surfaces have a portion of surface area in common, while b others have in common a portion of surface area as also c others, where $a+b+c \leqq n$.

Then it may be that the surface area common to the surfaces (a) are cut by the surface area common to the the surfaces (b) and by the surface area common to the surfaces (c). We may thus derive several such functions $f_1(x,y)$, $f_2(x,y)$, ... as the function $f(x,y)$ in formula (a.). If there is no portion of curve common to all of a certain number of the curves $f_1(x,y) = 0$, $f_2(x,y) = 0$, ..., but if these curves have points of inter-

section or contact, it is always possible to find integral functions in x, y with integral coefficients $\bar{f}_1(x,y)$, $\bar{f}_2(x,y)$, ... such that

$$f_1(x,y)\bar{f}_1(x,y)+f_2(x,y)\bar{f}_2x,y)+\cdots = g(x),$$

where $g(x)$ is an integral function in x with integral coefficients and contains the projections of the points of intersection of the curves upon the x-axis.

Finally, if we can derive systems of points $g(x) = 0$, $g_1(x) = 0$, ..., and if there is no point common to all these systems, we may find functions integral in x with integral coefficients $\bar{g}(x)$, $\bar{g}_1(x)$, ... so that

$$g(x)\bar{g}(x)+g_1(x)\bar{g}_1(x)+\cdots = c,$$

where c is an integer.

If on the other hand we have in our modular system the prime integer p and the irreducible functions $g(x)$ (mod. p) and $f(x,y)$ (modd. p, $g(x)$, then everything (surface area, portion of curve, system of points, etc.) which is common to the modular system $[p, g(x), f(x,y), N\{h(x,y,z)\}]$ is common to the system $[p, g(x), f(x,y), H(x,y,z)]$ where $H(x,y,z)$ is the greatest common divisor (modd. p, $g(x)$, $f(x,y)$) of the elements $h_1(x,y,z)$, $h_2(x,y,z)$, ...

We may say that the surface $H(x,y,z) = 0$ is common to the surfaces $h_1(x,y,z) = 0$, $h_2(x,y,z) = 0$, ... (modd. p, $g(x)$, $f(x,y)$).