On Certain Ternary Cubic-Form Equations
Author(s): J. J. Sylvester
Source: *American Journal of Mathematics*, Vol. 2, No. 4 (Dec., 1879), pp. 357-393
Published by: The Johns Hopkins University Press
Stable URL: https://www.jstor.org/stable/2369490
Accessed: 27-01-2020 17:50 UTC

On Certain Ternary Cubic-Form Equations.

By J. J. Sylvester.

Excursus A. *On the Divisors of Cyclotomic Functions.*

Title 1. *Cyclotomic Functions of the 1st Species.* In the preceding section which should have been termed and will be hereafter referred to as the *Proem* of Chapter I, I stated that the proof of the first batch of theorems on the irresoluble cases of equations in numbers of the form $x^3 + y^3 + Az^3 = 0$, or, as we might say, of the forms of numbers A irresoluble into a pair of rational cubes, depends on the demonstration of the form of the numerical linear divisors of the function $x^3 - 3x + 1$. At the time when this proem went to press I had reduced to a certainty the law of the divisors by numerical verifications without end, but had not obtained a rational demonstration of it, nor was I able to find such or even a statement of the law itself in any of the current text-books, such as Gauss, Legendre, Bachmann, Lejeune-Dirichlet or Serret. I was therefore compelled to seek out a demonstration for myself, and in so doing was unavoidably led to consider the general theory of the species of *cyclotomic* (*Kreistheilung*) functions of which the cubic functions above written is an example of what may be called the second species and incidentally also the theory of the simpler or first species which, although discussed ever since the time of Euler, appears to me to remain still in a somewhat cloudy and incomplete condition. As this inquiry extends beyond the strict needs of the subject which called it forth, I entitle it an *excursus*. It will be necessary for me eventually to introduce another and still more important excursus or lateral digression on certain consequences of the Geometrical Theory of Residuation, which theory itself also took its rise in and is required for the purposes of the arithmetical theory which forms the subject of the entire memoir.

If fx is any rational integral function of the order ω in its variable, we know that in respect to a prime number p as modulus fx regarded as the subject of a congruence cannot have more than ω distinct real roots. If we take p^j as modulus, certain conditions increasing in number with the value of j, will have to be satisfied in order that fx may have a superfluity (*i. e.* more than ω) of real roots.

One condition, the universal *sine quâ non*, will serve for the object I have in view, so that it will be sufficient to make $j = 2$. Obviously when this superfluity exists two of the roots must differ by a multiple of p since otherwise there would be a superfluity of roots *quâ* the first power of p as modulus. If then a and $a + \lambda p$ where $\lambda < p$ be two of the roots, we have $fa \equiv 0$ and $fa + \lambda f'a \,.\, p + Rp^2 \equiv 0 \text{ mod. } p^2$. Hence $fa \equiv 0$ and $f'a \equiv 0 \text{ mod. } p$, so that $fa + \lambda p = 0$ and $f'a + \mu p = 0$.

Applying the dialytic method to eliminate a it is obvious that the resultant of these two equations will differ only by a multiple of p from that of fa and $f'a$, *i. e.* from the arithmetical discriminant of fa (I use the term arithmetical to distinguish it from the algebraical discriminant in obtaining which latter fx is supposed to be affected with binomial numerical coefficients $\omega, \frac{\omega \,.\, \omega - 1}{2}, \ldots$ and the factor ω to be struck out from each of the two equations $\frac{df(x,1)}{dx} = 0, \quad \frac{df(x,1)}{d1} = 0\Big)$.

We see then that a rational integer function (the subject of a congruence) cannot have a superfluity of roots in respect to the power of a prime p^j as modulus, unless the strict (arithmetical) discriminant of the function contains p.

It is necessary for the purpose I have in view to express the strict relation between the arithmetical discriminant of a function Δfx and the product of the squares of the differences of its roots $\zeta^2 fx$. I shall for greater simplicity suppose that the initial coefficient of fx is unity, as it is in the cases with which we shall have to deal.

We know that $\Delta f = \mu \zeta^2 f$ where μ is a function of n the order of f, so that to determine μ we may specialize f in any manner we please, provided the order is maintained. Let $fx = x^n - 1$. Then it is easily proved that, making $\rho = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$,

$$(-)^{n\frac{n-1}{2}} \zeta^2 f = (\rho^n - 1)^{(n-1)\frac{n}{2}} \,.\, n^n,$$

so that $$\zeta^2 f = (-)^{\frac{(n-1)(n-2)}{2}} \,.\, n^n,$$

and $$\Delta f = (-)^{n-1} \,.\, n^{2n-2}.$$

Hence $$\Delta f = (-)^{(n-1)\frac{n}{2}} \,.\, n^{n-2} \zeta^2 f *$$

*As regards the application to be made of this result it was of course not necessary to determine the index of the power to which $(-)$ is raised, but it was hardly worth while to leave it undetermined.

expresses the universal relation between the arithmetical discriminant and the squared product of the root-difference of a function. If we had been dealing with the algebraical discriminant, it would have been necessary to replace n^{n-2} by n^{-n} in the above equation. It is furthermore to be observed that the discriminant is fixed in its sign by the condition that the term containing the highest power of the product of the expressed coefficients is to be taken positively.

So again it will be seen presently to be necessary to ascertain the strict relation between the resultant of two functions of degrees r, s and the product of the differences between the several roots ρ of the one and the several roots σ of the other of them, or, as we may say, between $R_{r,s}$ and $D_{\rho,\sigma}$, where if we choose to pay attention to algebraical signs that of $R_{r,s}$ may be understood to mean the resultant so taken that the term containing the highest power of the coefficient in the r-degreed function is positive and $D_{\rho,\sigma}$ to mean the product of the rs differences $(\rho - \sigma)$.

I shall again, for greater simplicity, suppose the initial coefficients of each of the two functions to be unity.

We know that $R_{r,s} = \mu D_{\rho,\sigma}$ where μ is a function of r and s exclusively. To determine it we may take x^r and $x^s + 1$ as the two functions, it will be found without difficulty that

$$R_{r,s} = 1^* \text{ and } D_{\rho,\sigma} = \left(-(-1)^{\frac{1}{s}}\right)^{rs} = (-)^{rs+r}.$$

Hence we have universally $R_{r,s} = (-)^{rs+r} D_{\rho,\sigma}$.

This seems to be the proper place to ascertain (what will be needed for future purposes) how far or under what qualifications the reciprocal connexion of the two facts: 1. Of two functions in x having a common root. 2. Of their resultant being zero, admits of being extended to roots of congruences in respect to a prime-number modulus.

Suppose fx, gx to be two in all respects (numerically† as well as algebraically) integer rational functions of the degrees i, j in x, then by eliminating dialytically $(i + j - 1)$ powers of x between

$$fx,\ xfx,\ x^2fx \ldots x^{j-1}fx,\quad gx,\ xgx,\ \ldots x^{i-1}gx,$$

*Thus *ex gr.* let $r = 4$, $s = 2$. Then $R_{r,s}$ is the dialytic resultant of

$$\begin{array}{ccccccccc} x^5 & & & & & & & & \\ & x^4 & & & & & & & \\ x^5 & & + x^3 & & & & & & \\ & x^4 & & + x^2 & & & & & \\ & & x^3 & & + x & & & & \\ & & & x^2 & & + 1 & & & \end{array}$$

which is obviously equal to unity.

†By which I mean that the coefficients are exclusively integer numbers.

we may obtain the equation $\lambda x fx + \mu x gx = Rx^q$ (q having any integer value from 0 to $i+j-1$) where R is the resultant of f, g and λx, μx are in all respects integer functions of x of degrees $j-1$ and $i-1$ in x whose values depend on the value of q. If, then, fx and gx are simultaneously zero for some value of x, we must universally have $R=0$ even if x should be zero, for thus we might make $q=0$.

But this equation will not suffice to show that fx and gx will simultaneously vanish for some value of x, provided that $R=0$ for every value of x which makes fx vanish, might, as far as this equation discloses, (and for all values of g), have the effect of making μx vanish.* We may, however, prove the fact in question, on a certain hypothesis to be presently stated, by availing ourselves of the knowledge that R is, to a *numerical factor près*, the product of the differences between the roots of f and those of g.

The hypothesis I make is that $fx \equiv 0 \bmod p$ is a congruence *all whose roots are real;* in this case I shall show that if the resultant R of fx and gx satisfies the congruence $R \equiv 0 \bmod p$ (*i. e.* if R contains p) then gx must have at least one real root in common with fx *quâ* modulus p.

From the congruence of $fx \equiv 0 \bmod p$ we may, by a well known principle, infer the existence of an equation $Fx = fx + p\phi x = 0$ whose roots are the same as those of the congruence above written, and the dialytic method of elimination renders it self-evident that the resultant of Fx and gx will differ only by a multiple of p from that of fx and gx, and will, therefore, be a multiple of p.

If, then, we call the roots of Fx (all real by hypothesis) $a_1, a_2, \ldots a_i$, we shall have $ga_1 . ga_2 . ga_3 \ldots ga_i \equiv 0 \bmod p$, and, as all the factors on the left hand side of the equation are real, one of them must contain p. Hence, if $R(fx, gx) \equiv 0 \bmod p$, and $fx \equiv 0 \bmod p$ *has all its roots real*, one of these roots must belong also to the congruence $gx \equiv 0 \bmod p$.

Going back now to what precedes this investigation, let us determine strictly the relation between the arithmetical discriminants and resultant of two functions in x and the discriminant of their prodnct.

Let ω, ω_1 be the degrees in x of two altogether integer functions fx, f_1x, and suppose $Fx = fx . f_1x$. Then obviously $\zeta^2 Fx = \zeta^2 fx . \zeta^2 f_1x . (D(fx, f_1x))^2$. Hence $\omega^{\omega-2} . \omega_1^{\omega_1-2} \Delta Fx = (\omega+\omega_1)^{\omega+\omega_1-2} f\Delta x . \Delta f_1x (R(fx, f_1x))^2$.

* I think it would not be incorrect to say that *in all cases* the fact of the resultant of two functions of x containing a prime number raises a strong presumption that the functions have a common congruence root in respect to that number.

If, then, p any prime number is contained in Δfx, and ω, ω_1 are each less than p, p will necessarily be contained in ΔFx. And as a particular case of this theorem, if p were contained in the discriminant of any factor of $x^{p-1}-1$ it would be contained in the discriminant of $x^{p-1}-1$, *i. e.* in a power of $(p-1)$, which is impossible. Hence, by a preceding theorem, no factor of $x^{p-1}-1$, regarded as the subject of a congruence, can contain *a superfluity* of real roots (*i. e.* more real roots than there are units in its degree) in respect to the modulus p^j.

It is easy to show, although I do not find it distinctly stated in any of the current text-books, that $x^{p-1}-1 \equiv 0 \bmod. p^j$ has $p-1$ real roots.

For let $x = y^{p^{j-1}}$. Then the congruence becomes

$$y^{p^{j-1}.(p-1)}-1 \equiv 0 \bmod. p^j,$$

where $p^{j-1}.(p-1)$ is what is commonly designated as the ϕ function of p^j, the number of numbers less than p^j and prime to it, (the so-called ϕ function of any number I shall here and hereafter designate as its τ function and call its Totient). This last congruence by Fermat's extended theorem has all its roots real. It is easy to see that they will consist of $(p-1)$ groups, each group containing p^{j-1} numbers for which the value of x *quâ* modulus p^j will be the same, but different for numbers belonging to two different groups. For let y_1 be any of the y roots, and $y_2^{p^{j-1}}-y_1^{p^{j-1}} \equiv 0 \bmod. p^j$. Then *quâ* mod. p, $y_2^{p^{j-1}} \equiv y_2$ and $y_1^{p^{j-1}} \equiv y_1$, because $p^{j-1}-1$ contains $p-1$.

All the values of y_2 will, therefore, be comprised in the series

$$y_1,\ y_1+p,\ y_1+2p,\ \ldots\ y_1+(p^{j-1}-1)\,p,$$

and

$$(y_1+\lambda p)^{p^{j-1}} = y_1^{p^{j-1}}+p^{p^j}.\,Q.$$

Hence the p^j terms of the series (and no other values of z) all satisfy the congruence

$$z^{p^{j-1}}-y_1^{p^{j-1}} \equiv 0 \bmod. p^j.$$

Hence $x = y^{p^{j-1}}$ has $(p-1)$ distinct real values *quâ* p^j or there are $(p-1)$ real roots to the congruence $x^{p-1}-1 \equiv 0 \bmod. p^j$. Hence, if fx is any factor of $x^{p-1}-1$, $fx \equiv 0$ [mod. p^j] will have all its roots real.

For let $fx.f_1x = x^{p-1}-1$.

Then since $x^{p-1} \equiv 0 \bmod. p^j$ has all its roots real, and fx and f_1x have no congruence root *quâ* mod. p in common * if $fx \equiv 0$ to the modulus p^j has not *its full quota*, f_1x will have a *superfluity* of roots, but this has been shown to be impossible.

* For if this were the case two factors of $x^{p-1}-1$ *quâ* mod. p having two roots in common $x^{p-1}-1$ would not have its full quota of roots.

Now, let $p = mk + 1$. Then $x^k - 1$ is a factor of $x^{p-1} - 1$. Let $\chi_k x$ be the factor of $x^k - 1$, which contains all its primitive roots; this is what I term a *cyclotomic function of the first species* to the index k. $\chi_k x$ being a factor of $x^k - 1$ is a factor of $x^{p-1} - 1$, and will therefore, by what has just been shown, have all its roots real *quâ* the modulus p^j.

Hence a cyclotomic function of the 1st species to the index k contains, as a divisor, any power of any prime number of the form $mk + 1$, and, moreover, if ω is its degree, (where ω represents the *totient* of k), $(mk + 1)^j$ will be an ω-fold divisor of the function, *i. e.* will be a divisor thereof corresponding to ω distinct values of the variable of the function, *i. e.* values incongruent with one another *quâ* the modulus p^j.

The divisors of the cyclotomic function to index h may be divided into two classes, viz: divisors which do not divide the index, which may be called superior or extrinsic divisors, and divisors which divide at the same time the function and its index which may be termed inferior or intrinsic divisors. I shall begin with showing that any prime number extrinsic divisor diminished by unity must contain the index, *i. e.*, that if p is an extrinsic divisor and k the index, we must have $p = mk + 1$ which is a reciprocal proposition to the one just established.

If possible let p, any prime such that $p - 1$ does not contain k nor k contain p, be a divisor of the cyclotomic function of the first species $\chi_k x$. And let δ be the greatest common divisor of $p - 1$ and k. Then we shall have $x^\delta - 1 \equiv 0 \bmod. p$. But we have also $\chi_k x \equiv 0 \bmod. p$. Hence the resultant of $x^\delta - 1$ and $\chi_k x$ must contain p, but $\frac{x_k - 1}{x^\delta - 1}$ contains $\chi_k x$; *à fortiori* therefore the resultant of this and $x^\delta - 1$ will contain p. But this resultant is evidently equal to the value of $\frac{x^k - 1}{x^\delta - 1}$ (where $x^\delta = 1$) raised to the power δ, *i. e.* $= \left(\frac{k}{\delta}\right)^\delta$ and therefore, *ex-hypothesi*, does not contain p.

It has thus been proved that every extrinsic divisor of $\chi_k x$ can only be of the form $mk + 1$.

Next let $k = k_1 p^j$ (k_1 being prime to p) and suppose p to be a divisor of $\chi_k x$.

Then p is a divisor of $(x^{p^j})^{k_1} - 1$ and, therefore, by what has been shown, must be of the form $mk_1 + 1$, unless $x^{p^j} - 1$ contained p in which case since $p^j - 1$ is divisible by $p - 1$, $x - 1$ must contain p and consequently p will be a divisor of $\chi_k 1$.

To find the value of $\chi_k 1$ we may proceed as follows:

Let $k = a^\alpha . b^\beta . c^\gamma . d^\delta . e^\varepsilon$. Then the totient of k is

$$a^{\alpha-1} . b^{\beta-1} . c^{\gamma-1} . d^{\delta-1} . e^{\varepsilon-1} \left\{ \begin{matrix} \alpha\beta\gamma\delta\varepsilon + \Sigma\alpha\beta\gamma + \Sigma\alpha \\ -\Sigma\alpha\beta\gamma\delta - \Sigma\alpha\beta - 1 \end{matrix} \right\},$$

and if we write this $L + M + N - P - Q - R$

$$\chi_k x = \frac{(x^L - 1)(x^M - 1)(x^N - 1)}{(x^P - 1)(x^Q - 1)(x^R - 1)},$$

and so in general the expression for $\chi_k x$, however many the distinct prime factors of k, imitates and follows *pari passu* the expression for the totient of k; and if $L, M, N, \ldots$ be the positive terms and $P, Q, R, \ldots$ be the negative ones in the algebraical representation of that totient by the common theory of vanishing fractions, shows that $\chi_k 1 = \frac{L . M . N \ldots}{P . Q . R \ldots}$. There are two cases:

1°. When k contains i distinct prime factors, where $i > 1$. In that case supposing a to be one of them and α its index, the index of a in $L . M . N \ldots$ will be

$$\alpha \left\{ 1 + \frac{(i-1)(i-2)}{1.2} + \frac{(i-1)(i-2)(i-3)(i-4)}{1.2.3.4} + \ldots \right\}$$

and in $P . Q . R \ldots$.

$$\alpha \left\{ (i-1) + \frac{(i-1)(i-2)(i-3)}{1.2.3} \ldots \right\},$$

so that the index in the quotient is $\alpha (1-1)^{i-1}$, *i. e.* is zero. And so for $b, c, \ldots$. Hence $\chi_k 1 = 1$.

2°. When $i = 1$ and $k = a^\alpha$, the value of $\chi_k x = \frac{x^{a^\alpha} - 1}{x^{a^{\alpha-1}} - 1}$, and consequently $\chi_k 1 = a$. Hence, when $k = k_1 p^j$, and k_1 is not unity, p, if a divisor of $\chi_k x$, must be of the form $mk_1 + 1$. Moreover, the case of $k_1 = 1$ offers no exception to this conclusion, inasmuch as when $k_1 = 1$, p, (like every other number) comes under the form $mk_1 + 1$.

It now remains to show the converse that if $k = k_1^{p^j}$ and $p = mk_1 + 1$, p will be a divisor of $\chi_k x$.

For the sake of greater simplicity, we may consider apart the case where $k = p^j$. Here $\chi_k x = \frac{x^{p^j} - 1}{x^{p^{j-1}} - 1} = 1 + x^{p^{j-1}} + x^{2p^{j-1}} + \ldots + x^{(p-1)p^{j-1}}$, which, (to modulus p) $\equiv 1 + x + x^2 + \ldots + x^{p-1} \equiv \frac{x^p - 1}{x - 1}$, and, therefore, can only contain p, if $x^p - 1$, and, consequently, $x - 1$ contains it. Hence, the only root of $\chi_k x \equiv 0$ [mod. p], for this case is $x = 1$.

Moreover, only p itself, and no higher power of p, can be a divisor of the cyclotomic function in question, because

$$\frac{(1+\lambda p)^{p^j}-1}{(1+\lambda p)^{p^{j-1}}-1} = \frac{\lambda p^{j+1}+\ldots}{\lambda p^j+\ldots} = p + Bp^2 + Cp^3 + \ldots + Lp^{(p-1)p^{j-1}}$$

does not contain p^2.*

To save unnecessary fatigue of attention, about a small matter, to my readers and myself, I will take, as a representative of the general case, $k = k_1 p$, $k_1 = abc$, $p = mk_1 + 1$; it will easily be verified that the increase of the number of distinct prime factors a, b, c, or the affection of them or of p with indices, will in no manner affect the course of the demonstration or the validity of the conclusion.

In the above *special case*

$$\chi_k x = \frac{(x^{abcp}-1)(x^{ab}-1)(x^{ac}-1)(x^{bc}-1)(x^{ap}-1)(x^{bp}-1)(x^{cp}-1)(x-1)}{(x^{abc}-1)(x^{abp}-1)(x^{acp}-1)(x^{bcp}-1)(x^a-1)(x^b-1)(x^c-1)(x^p-1)}.$$

Let now $x^{k_1}-1=0$, so that $x^p = x$. Then obviously $\chi_k x = \frac{x^{abcp}-1}{x^{abc}-1} = p$. Hence the resultant of $\chi_{k_1} x$ and $\chi_k x$ is $p^{\tau(k_1)}$ (τk_1 meaning the totient of k_1). Consequently since $\chi_{k_1} x \equiv 0$ [mod. p] has all its roots real, one root at least of $\chi_k x \equiv 0$ [mod. p] will be a root of the preceding congruence.

It will be noticed that if instead of $\chi_{k_1} x$ we took $\chi_{k'_1} x$ where k'_1 is a factor of k_1 it would not be true that the resultant of it and $\chi_k x$ would contain p.

For example, if $k'_1 = ab$ and $x^{k'_1}-1=0$ we should have

$$\chi_k x = \frac{x^{abcp+1}-1}{x^{abc}-1}\cdot\frac{x^{ab}-1}{x^{abp}-1} = \frac{p}{p} = 1.$$

Or again if $k'_1 = a$ and $x^{k'_1}-1=0$ we should have

$$\chi_k x = \frac{x^{abcp}-1}{x^{abc}-1}\cdot\frac{x^{ab}-1}{x^{abp}-1}\cdot\frac{x^{ac}-1}{x^{acp}-1}\cdot\frac{x^{ap}-1}{x^a-1} = p_1\frac{1}{p}\cdot\frac{1}{p}\cdot p = 1$$

as before. So that the resultant instead of being p would, in each case, be 1, and consequently $x^k-1\equiv 0$ [mod. p] and $x^{k'_1}-1\equiv 0$ [mod. p] could not have a root in common. And so in general it may be shown that if $k = k_1 p^j$ and $k'_1 = \frac{k_1}{\delta}$ the resultant of $x^{k'_1}-1$ and $\chi_k x$ is 1, except when $\delta = 1$ in which case it is p.

Hence the roots of $\chi_k x \equiv 0$ [mod. p] are to be sought not among all the roots of $x^{k_1}-1\equiv 0$ [mod. p], but exclusively among only such of them as belong to the congruence $\chi_{k_1} x \equiv 0$ [mod. p].

* When $p=2$ and $j=1$ the third term will not be of a higher power in p than the second term in the development of the numerator, so that the conclusion ceases to hold; as ought to be the case for the cyclotomic of the 1st species to the index 2, viz: $x+1$ will obviously contain every power of 2 as a divisor.

We have seen that if p, a prime number, is an extrinsic divisor of a cyclotomic function to the index k, any power of p is also a divisor of the function. On the contrary, if p is an intrinsic divisor it will appear that p^2 cannot (and consequently no higher power of p than the 1st, can) be a divisor. For if x satisfies the congruence $\chi_{k_1}x \equiv 0$ [mod. p] we must have $x^{k_1} = 1 + \lambda p$ and $x^p = x^{mk_1}.x = (1 + mp)\,x$, where m represents a series of ascending powers of p. Hence

$$\chi_k x = \frac{x^{k_1 p}-1}{\chi^{k_1}-1}\cdot\frac{x^{ab}-1}{x^{abp}-1}\cdot\frac{x^{ac}-1}{x^{acp}-1}\cdot\frac{x^{bc}-1}{x^{bcp}-1}\cdot\frac{x^{ap}-1}{x^{a}-1}\cdot\ldots,$$

where the first factor, being equal to $x^{k_1(p-1)} + x^{k_1(p-2)} + \ldots + 1$, will be of the form $p\,(1 + Pp)$, P being a series containing only positive powers of p. Again,

$$\frac{x^{ab}-1}{(1+Qp)\,x^{ab}-1} = 1 + \frac{Qpx^{ab}}{1-x^{ab}} + \frac{Q^2p^2x^{2ab}}{(1+x^{ab})^2} + \ldots = 1 + Q_1 p$$

where Q_1 is an infinite series containing positive powers only of p and x.

In like manner $\dfrac{x^{ap}-1}{x^a-1} = \dfrac{(1+Rp)\,x^a-1}{x^a-1} = 1 + R_1 p$ where R_1 (like R) is an infinite series of positive powers of p and x, and so for each separate factor.

On multiplying the product of these infinite series by $p\,(1 + Pp)$, we shall necessarily obtain a finite series of the form $p\,(1 + Gp)$. Consequently, the cyclotomic function will divide by p but not by p^2. And we might have used this method exclusively to have established the fact of the first power of p, under the conditions presupposed, being a divisor of the function. This method serves also to establish directly that *every* root of $\chi_{k_1}x \equiv 0$ is a root of the congruence $\chi_k x \equiv 0$ [mod. p]. And we thus see that the intrinsic divisor, when it exists, is a τk_1-fold divisor of the cyclotomic function.

When k is the index to a cyclotomic function, and $k = k_1 p^j$, where p is a prime not contained in k, let us agree to call k_1 the sub-index to p. Then, from what precedes, we may draw the conclusion that a cyclotomic function of the first species has never more than one intrinsic divisor, which, if it exists, is the greatest prime number contained in the index, but is such only in the case when diminished by unity, it contains its own sub-index, (a conclusion necessarily satisfied when the index is a prime, for then its sub-index is unity), and, moreover, that the first power only of such intrinsic divisor, when it exists, is a divisor of the function.

It being true and capable of easy demonstration, that when a rational integer function contains, as a divisor, each of two numbers prime to one

another, their product will also be a divisor of the function, it follows that any number, each of whose prime factors, diminished by unity, contains the index and also every such number multiplied by the highest prime number which is contained in the index (provided that when diminished by unity that prime contains its own sub-index) is a divisor of a cyclotomic function of the first species. This, as I have said, is only another name for that irreducible factor of a binomial $x^k - 1$ whose degree in x is the *totient* of k.

When the cyclotomic function of any species is made homogeneous by the introduction of a second variable y, relatively prime to x, it becomes a form, (in the technical sense of the word), and may then very conveniently be designated a *cyclo-quantic.*

Title 2. *Cyclotomic Functions of the Second Species* (*Conjugate Class*).* I pass on to the theory of the divisors of the function which has for roots the sum of the binomial (*zweigliedrig*) groups of the primitive roots of $x^k - 1$, or, in other words, all the distinct values, $\frac{1}{2}\tau(k)$ in number, of $2\cos\frac{\lambda\tau}{k}$ where λ is any number less than $\frac{k}{2}$ and prime to k.

Such a function, in which the coefficient of the highest power of the variable is supposed to be unity, I call a cyclotomic function, or simply a cyclotomic, of the second species and conjugate class to the index k. It may be found most readily by dividing the corresponding one of the first species, whose variable say is x, by $x^{\frac{1}{2}\tau(k)}$, substituting u for $x + \frac{1}{x}$, and applying for successive values of m the trigonometrical formula for expressing $\cos m\theta$ in terms of powers of $\cos\theta$, except when the index is a prime number, in which case the function in u is given more expeditiously at once by the well-known formula

$$u^m + u^{m-1} - \frac{m-1}{1}u^{m-2} - \frac{m-2}{1}u^{m-3} + \frac{(m-2)(m-3)}{1.2}u^{m-4} + \frac{(m-3)(m-4)}{1.2}u^{m-5} - \ldots,$$

which last coefficient, in the French edition of the Disq. Arith., 1807, it may be worth noting, is written erroneously $\frac{(m-1)(m-4)}{1.2}$.

I have thought it would be useful and convenient for many of my readers to be able to see before them the functions of the two sorts, and I accordingly annex a table of their values for all indices up to 36 inclusive.

* When, in the matter comprehended under this title, by inadvertence, cyclotomic functions of the second species are spoken of without a qualification annexed, it is to be understood, in all cases, that only those of the conjugate class or, in other words, those whose roots are all real, are intended. For brevity I shall usually call this class of functions cyclotomics of the second *sort.*

To the index 1 or 2, the cyclotomic of the second species has no existence. Those of the first species to the index 1 or 2, and of the second to the index 3, 4 or 6 are linear, and of course as forms, have no arithmetical properties, but contain every number as a divisor, linear forms being, as it were, the protoplasm out of which the higher forms are organized.

Table of Cyclotomic Functions of the first species and the conjugate class of the second species for all values of the index from 1 *to* 36 *inclusive.*

Index.	1st Species.	2d Species, Conjugate Class.
1	$x-1$	
2	$x+1$	
3	x^2+x+1	$u+1$
4	x^2+1	u
5	$x^4+x^3+x^2+x+1$	u^2+u-1
6	x^2-x+1	$u-1$
7	$x^6+x^5+x^4+x^3+x^2+x+1$	u^3+u^2-2u-1
8	x^4+1	u^2-2
9	x^6+x^3+1	u^3-3u-1
10	$x^4-x^3+x^2-x+1$	u^2-u+1
11	$x^{10}+x^9+\ldots+x+1$	$u^5+u^4-4u^3-3u^2+3u+1$
12	x^4-x^2+1	u^2-3
13	$x^{12}+x^{11}+\ldots+x+1$	$u^6+u^5-5u^4-4u^3+6u^2+3u-1$
14	$x^6-x^5+x^4-x^3+x^2-x+1$	u^3-u^2+2u+1
15	$x^8-x^7+x^5-x^4+x^3-x+1$	$u^4-u^3-4u^2+4u+1$
16	x^8+1	u^4-4u^2+2
17	$x^{16}+x^{15}+\ldots+x+1$	$u^8+u^7-7u^6-6u^5+15u^4+10u^3-10u^2-4u+1$
18	x^6-x^3+1	u^3-3u+1
19	$x^{18}+x^{17}+\ldots+x+1$	$u^9+u^8-8u^7-7u^6+21u^5+15u^4$ $+10u^3-10u^2+5u+1$
20	$x^8-x^6+x^4-x^2+1$	u^4-5u^2+5
21	$x^{12}-x^{11}+x^9-x^8+x^6-x^4$ $+x^3-x+1$	$u^6-u^5-6u^4+6u^3+8u^2-8u+1$
22	$x^{10}-x^9+\ldots-x+1$	$u^5-u^4-4u^3+3u^2-3u+1$
23	$x^{22}+x^{21}+\ldots+x+1$	$u^{11}+u^{10}-10u^9-9u^8+36u^7+28u^6-56u^5$ $-35u^4+35u^3+15u^2-6u-1$
24	x^8-x^4+1	u^4-4u^2+1
25	$x^{20}+x^{15}+x^{10}+x^5+1$	$u^{10}-10u^8+35u^6+u^5-50u^4-5u^3+25u^2-5u-1$

Index.	1st Species.	2d Species, Conjugate Class.
26	$x^{12}-x^{11}+\ldots-x+1$	$u^6-u^5-5u^4+4u^3+6u^2-3u-1$
27	$x^{18}-x^9+1$	$u^9-9u^7+27u^5-30u^3+9u-1$
28	$x^{12}-x^{10}+x^8-x^6+x^4-x^2+1$	$u^6-7u^4+14u^2-7$
29	$x^{28}+x^{27}+\ldots+x+1$	$u^{14}+u^{13}-13u^{12}-12u^{11}+66u^{10}+55u^9-165u^8-120u^7+210u^6+126u^5-126u^4-56u^3+28u^3+7u-1$
30	$x^{16}-x^{14}+x^{10}-x^8+x^6-x^2+1$	$u^8-9u^6+26u^4-26u^2+1$
31	$x^{30}+x^{29}+\ldots+x+1$	$u^{15}+u^{14}-14u^{13}-13u^{12}+78u^{11}+66u^{10}-220u^9-165u^8+330u^7+210u^6-252u^5-126u^4+84u^3+28u^2-4u-1.$
32	$x^{16}+1$	$u^8-8u^6+20u^4-16u^2+2$
33	$x^{20}-x^{19}+x^{17}-x^{16}+x^{14}-x^{13}+x^{11}-x^{10}+x^9-x^7+x^6-x^4+x^3-x+1$	$u^{10}-u^9-10u^8+10u^7+34u^6-34u^5-43u^4+43u^3+12u^2-12u-1$
34	$x^{16}-x^{15}+x^{14}-\ldots+x^2-x+1$	$u^8-u^7-7u^6+6u^5+15u^4-10u^3-10u^2+4u+1$
35	$x^{24}-x^{23}+x^{19}-x^{18}+x^{17}-x^{16}+x^{14}-x^{13}+x^{12}-x^{11}+x^{10}-x^8+x^7-x^6+x^5-x+1$	$u^{12}-u^{11}-12u^{10}+11u^9+54u^8-43u^7-113u^6+71u^5+110u^4-46u^3-40u^2+8u+1$
36	$x^{12}-x^6+1$	$u^6-6u^4+9u^3-3$

A very good test (or, in most cases, pair of tests) of the correctness of the figures is to write $u=\pm 2^*$ corresponding to $x=\pm 1$ and see if the values for the same index agree. Our interest will presently be concentrated on the single entry in the right hand column, that which expresses the conjugate class of the second species of cyclotomic to the index 9, but the function for the neighboring case of the index 8 is worthy of arresting the reader's attention for a moment, inasmuch as the general theory of cyclotomic divisors applied to it will be seen to supply an instantaneous proof that all prime numbers of the form $8n\pm 1$, and no other prime numbers have 2 for a quadratic residue.†

It is hardly necessary to observe that, when the index is a prime number, it may be duplicated without affecting the character of either set of functions, the only effect produced thereby being the entirely unimportant one of a change in the sign of the variable.

* And a further double test is given by taking $u=0$, $x=2$, as we ought to find $\chi i=2^{\frac{1}{2}\tau k}\psi 0$.

† So, under the third Title, it will be found that u^2+2 is a *non-conjugate* cyclotomic of the second species to the index 8, of which, according to the general cyclotomic law, the odd prime divisors are of the form $8m+1$ or $8m+3$.

The formula which I have employed for computing $\cos n\theta$ is that which, beginning with the *highest* power of $\cos\theta$, admits of a uniform scheme of setting down the work, which is not the case when the series is started from the other end. It, and the series used for $\frac{\sin\frac{p\theta}{2}}{\sin\frac{\theta}{2}}$, also required for my purposes, may be obtained by a much simpler method than any I have seen given in the text books as follows.

In general, the denominator of $\frac{1}{a_1} - \frac{1}{a_2} - \ldots \frac{1}{a_u}$, say the procumulant $[a_1, a_2, \ldots a_u] = A_0 - A_1 + A_2$ etc., where A_0 is $a_1 . a_2 . \ldots . a_u$, A_1 is the sum of the quotients of A_0 by any pair of consecutive elements $a_i . a_{i+1}$, A_2 of the quotients of A_0 by the product of any two such pairs as $a_i . a_{i+1} . a_j . a_{j+1}$, and so on. If we call the *number* of such quotients in A_i, $D_i n$, it is obvious that

$$D_{i+1}n = \Sigma_{t=0}^{t=n-2} D_i t .$$

Hence $D_0 n = 1$, $D_1 n = n-1$, $D_2 n = (n-2)\frac{n-3}{2}$, $D_3 n = \frac{(n-3)(n-4)(n-5)}{1.2.3}$, and so on.

On making $a_1 = a_2 = \ldots = a_n = 2\cos\theta$, it will immediately be seen that the procumulant [$2\cos\theta$, $2\cos\theta \ldots$ to n terms] expresses $\frac{\sin(n+1)\theta}{\sin\theta}$, because, calling this u_n, the equation in difference for finding it is

$$u_{n+1} = 2\cos u_n - u_{n-1} \text{ and } u_0 = 1 .$$

Consequently $\frac{\sin(n+1)\theta}{\sin\theta} = (2\cos\theta)^n - n(2\cos\theta)^{n-2} + \frac{(n-1)(n-2)}{2}(2\cos\theta)^{n-4} \ldots .$

Hence $2\cos n\theta = 2\left(\frac{\sin(n+1)\theta}{\sin\theta} - \cos\theta\frac{\sin n\theta}{\sin\theta}\right) = (2\cos\theta)^n - n(2\cos\theta)^{n-2}$

$+ n\frac{n-3}{2}(2\cos\theta)^{n-4} \ldots .$ Also, $\frac{\sin\frac{2n+1}{2}\theta}{\sin\frac{\theta}{2}} = \frac{\sin(n+1)\theta}{\sin\theta} + \frac{\sin n\theta}{\sin\theta} = (2\cos\theta^n)$

$+ (2\cos\theta)^{n-1} - n(2\cos\theta)^{n-2} - (n-1)(2\cos\theta)^{n-4} + \ldots .$*

*This expansion Gauss (Rech. Arith., Paris, 1757, p. 431) suggests deriving by means of the exceedingly awkward and unmanageable process indicated by the formula $\frac{\sqrt{1-\cos n\theta}}{1-\cos\theta}$, $\cos n\theta$ being previously supposed to be expanded in terms of powers of $\cos\theta$. *Quandoque bonus dormitat Homerus.*

Writing u in place of $2\cos\theta$ these are the two expansions which I have used to express $x^n + \frac{1}{x^n}$ and $\frac{x^{\frac{p-1}{2}} - x^{-\frac{p-1}{2}}}{x^{\frac{1}{2}} - x^{-\frac{1}{2}}}$ in terms of powers of $x + \frac{1}{x}$ in calculating the cyclotomics of the 2d sort whose values are given in the preceding table.

Since $(x^{p-1}-1)(x^{p+1}-1) = x^{2p} - x^{p+1} - x^{p-1} + 1$, if, for convenience, we write $x + \frac{1}{x} = u = 2\cos\theta$, it is evident that $\cos p\theta - \cos\theta$, regarded as an algebraical function of $\cos\theta$, will contain all the cyclotomic functions of the second species (conjugate class) whose indices are divisors of $p-1$ or $p+1$ and in addition to these $\left(x - \frac{1}{x}\right)^2$ or $u^2 - 4$ derived from the factor $x^2 - 1$ which is common to $x^{p-1} - 1$ and $x^{p+1} - 1$, but does not give rise to a cyclotomic of this sort until it is squared; $\cos p\theta - \cos\theta$ is thus a product exclusively of cyclotomics of the second sort.

It is well known that $\cos p\theta - \cos\theta \equiv 0 \pmod{p}$ regarded as a congruence in $\cos\theta$ has the p roots $\cos\theta = 0, 1, 2, 3, \ldots \overline{p-1}$, p being supposed to be a prime number.

But more generally the congruence $\cos p^j\theta - \cos p^{j-1}\theta \equiv 0 \bmod p^j$ has its full complement of p^j real roots a theorem, this, which is the analogue of the theorem of Fermat extended to powers of prime numbers put under the form of affirming that $x^{p^j} - x^{p^{j-1}} \equiv 0 \bmod p^j$ has its full complement of real roots; but, as I do not recall seeing the *cosine* theorem for modulus p^j anywhere stated, and as it is wanted for the theory I am developing, and its truth is not obvious, I shall proceed to prove it. For greater simplicity of notation let us begin with the case where $j = 2$. We have then $\cos p^2\theta = (\cos\theta)^{p^2} - p^2\frac{p^2-1}{2}(\cos\theta)^{p^2-2}.(\sin\theta)^2 + \frac{p^2(p^2-1)(p^2-2)(p^2-3)}{1.2.3.4}(\cos\theta)^{p^2-4}.(\sin\theta)^4 \ldots$ and $\cos p\theta = (\cos\theta)^p - p\frac{p-1}{2}(\cos\theta)^{p-2}.(\sin\theta)^2 + \frac{p.(p-1)(p-2)(p-3)}{1.2.3.4}(\cos\theta)^{p-4}.(\sin\theta)^4 \ldots$ where of course all the powers of $(\sin\theta)^2$ are regarded as functions of $\cos\theta$. It will easily be recognized that every coefficient in the first series will be divisible by p^2 with the exception of those terms in which a new multiple of p first makes its appearance among the factors of the denominator, which will lose one power of p; the next coefficient to any such as last named taking up a new factor of p into the numerator, the fraction to which it belongs will recover the lost p and be again divisible by p^2.

The difference, therefore, between the two series *quâ mod.* p^2 will be $(\cos\theta)^{p^2} - (\cos\theta)^p$

$$+\frac{p^2(p^2-1)\ldots(p^2-2p+1)}{1.2\ldots 2p}(\cos\theta)^{p^2-2p}.(\sin\theta)^{2p} - p\frac{p-1}{2}(\cos\theta)^{p-2}(\sin\theta)^2$$

$$+\frac{p^2(p^2-1)\ldots(p^2-4p+1)}{1.2\ldots 4p}(\cos\theta)^{p^2-4p}.(\sin\theta)^{4p} - \frac{p(p-1)(p-2)(p-3)}{1.2.3.4}(\cos\theta)^{p-4}.(\sin\theta)^4$$

. . . . . .

It may be shown that every pair of terms in the above is divisible by p^2 for all real values of $\cos\theta$.

1°. $(\cos\theta)^{p^2} - (\cos\theta)^p$ contains p^2 by Fermat's extended theorem.

2°. *Quâ* p, $(\cos\theta)^{p^2-2p} \equiv (\cos\theta)^{p-2}$ and $(\sin\theta)^{2p} \equiv (\sin\theta)^2$.

Hence *quâ* p^2, the sum of the second pair of terms

$$\equiv p\frac{p-1}{2}\left\{\frac{(p+1)(p-2)(p-3)\ldots(p^2-2p+1)}{2.3\ldots(2p-1)} - 1\right\} \equiv 0$$

$$\equiv p\frac{p-1}{2}\left\{\frac{2.3\ldots(2p-1)}{2.3\ldots(2p-1)} - 1\right\} \equiv 0.$$

3°. *Quâ* p, inasmuch as $p^2-5p+4=(p-1)(p-4)$, $(\cos\theta)^{p^2-4p} \equiv (\cos\theta)^{p-4}$ and $(\sin\theta)^{4p} \equiv (\sin\theta)^4$. Also, $p^n-1 \equiv p-1$, $p^2-2 \equiv p-2$ and $p^2-3 \equiv p-3$. Hence the sum of the 3d pair of terms *quâ* p^2

$$\equiv \frac{p(p-1)(p-2)(p-3)}{1.2.3.4}\left\{\frac{(p^2-4)(p^2-5)\ldots(p^2-4p+1)}{4.5\ldots(4p-1)}\right\} \equiv 0.$$

And so each pair of terms may be proved to be congruous to zero *quâ* p^2.

The same form of demonstration may be shown to apply to the case of the modulus p^j,* and we may regard as proved the important theorem that $\cos p^j\theta - \cos p^{j-1}\theta \equiv 0$ [mod. p^j] contains the maximum number of roots p. It follows that $\cos p\theta - \cos\theta \equiv$ mod. p^j will contain p distinct roots. For, if we make $\theta = p^{j-1}\phi$, the congruence becomes $\cos p^j\phi - \cos p^{j-1}\phi \equiv 0$ mod. p^j, which has p^j roots. These roots will separate into p groups of p^{j-1} each, such $\cos(p^{j-1}\phi)$ will be the same for all the $(\cos\phi)$'s in the same group, but different (*quâ* mod. p^j) for any two belonging to distinct groups. For if $\cos\phi_1$ be one of the values regarded as given, and $\cos(p^{j-1}\phi_2) \equiv \cos(p^{j-1}\phi_1)$ mod. p^j,

$$\left.\begin{aligned}\cos(p^{j-1}\phi_2) &\equiv \cos\phi_2\\ \text{and}\qquad \cos(p^{j-1}\phi_1) &\equiv \cos\phi_1\end{aligned}\right\} \text{mod. } p.$$

* The reader will please bear in mind that in the expansion of $(a+b)^{p^j}$ the number of coefficients in which p enters to the power $j, j-1, \ldots 2, 1, 0$ respectively is $p^j - p^{j-1}, p^{j-1} - p^{j-2}, \ldots p^2 - p, p-1, 2$.

If, then, we form the series

$$\cos\phi_1,\ \cos\phi_1+p,\ \cos\phi_1+2p,\ \ldots\ \cos\phi_1+(p^{j-1}-1)\,p,$$

all the values of $\cos\phi_2$ must be included among the terms of this series. Conversely, if we make $\cos\phi_2=\cos\phi_1+\lambda p$, we shall have

$$\cos p^{j-1}\phi_2-\cos p^{j-1}\equiv 0 \text{ mod. } p^j.$$

For, writing q for p^{j-1},

$$\cos q\phi_2=(\cos\phi_2)^q-q\,\frac{q-1}{2}\,(\cos\phi_2)^{q-2}.(\sin\phi_2)^2+\ldots.$$

If in this development we take the term containing $(\cos\phi_2)^{q-2t}.(\sin\phi_2)^{2t}$, its coefficient will contain q, except in the case where t contains p^i, in which case the coefficient will contain $\frac{q}{p^i}$ but not q, and the index of $(\cos\phi_2)$ and $(\sin\phi_2)^2$ will each contain p^i. Hence, since $\cos\phi_2=\cos\phi_1+\lambda p$, and consequently $(\sin\phi_2)^2$ is of the form $(\sin\phi_1)^2+\Delta p$, it follows that the difference between this term and the corresponding one in the development of $\cos q\phi_1$ will in the one case contain qp and in the other $\frac{q}{p^i}\,p^{i+1}$, in either case therefore it contains $p\,.\,q$, *i. e.* p^j, and consequently making $\cos\phi_2$ equal to any of the p^{j-1} terms of the series, we shall have $\cos(p^{j-1}\phi_2)\equiv\cos(p^{j-1}\phi_1)$ mod. p^j as was to be shown. Hence $\cos p\theta-\cos\theta\equiv 0$ mod. p^j will have p real roots.

Again no algebraical factor of $\cos p\theta-\cos\theta$ can have a *superfluity* of real roots *quâ* mod. p^j, for if it had then by the same reasoning as applied to the cyclotomics of the first species, it would be necessary for p to be contained in the discriminant of $\cos p\theta-\cos\theta$ regarded as a function of $\cos\theta$, but *quâ* mod. p, this is the same as the discriminant of $(\cos\theta)^p-\cos\theta$ in regard to $\cos\theta$ or of x^p-x in regard to x which is the discriminant of $x^{p-1}-1$ multiplied by the squared resultant of x and $x^{p-1}-1$, and is therefore a power of $(p-1)$. Hence every algebraical factor of $\cos p\theta-\cos\theta$ *quâ mod.* p^j contains *its full quota* of real roots, *i, e.* as many roots as there are units in its degree.

If then $p=mk+\varepsilon$, where $\varepsilon=\pm 1$, since $\cos p\theta-\cos\theta$ will contain the cyclotomic of the second sort to the index k, such cyclotomic equivalented to zero [mod. p^j] will have all its roots real, so that $(mk\pm 1)^j$ will be a $\frac{\tau k}{2}$–fold divisor of such function.

As in the case of cyclotomics of the 1st species we may separate the divisors of those of the 2d sort into intrinsic and extrinsic, according as they are or are not divisors of the index.

First, as regards the extrinsic divisors, we may prove that no other prime numbers except those of the form $k \pm 1$ can be divisors of the 2d species of cyclotomics to the index k.

To show this I proceed as follows: $\psi_k u$ is contained algebraically in $\frac{\sin \frac{k}{2}\theta}{\sin \frac{\theta}{2}}$, and *à fortiori* in its square, *i. e.* in $\frac{1-\cos k\theta}{1-\cos\theta}$, so that if $2\cos\theta$ is a value of u, which makes $\psi_k u$ contain p,

$$\cos k\theta \equiv 1 \text{ mod. } p,$$

but also $\cos p\theta \equiv \cos\theta$ mod. p, and if $\frac{\sin p\theta}{\sin\theta} \equiv a + bp$,

$$1 = (\cos\theta)^2 + a^2(1-\cos\theta)^2 + cp,$$

and $(1-a^2)(1-\cos\theta)^2 = cp$, and, therefore, $a = \pm 1$ mod. p, for $\frac{1-\cos k\theta}{1-\cos\theta}$ does not contain $(1-\cos\theta)$, and if $(1-\cos k\theta)$ contains $1-(\cos\theta)^2$, which is only the case when k is even, $\frac{1-\cos k\theta}{1-(\cos\theta)^2}$, does not contain either $1-\cos\theta$ or $1+\cos\theta$, and, therefore, $\psi_k u$, which, in that case, is contained in $\frac{1-\cos k\theta}{1-(\cos\theta)^2}$, will not contain either $1-\cos\theta$ or $1+\cos\theta$.

Hence $1-(\cos\theta)^2$ is not zero, and, consequently, $a \equiv \pm 1$, and, therefore, $\frac{\sin p\theta}{\sin\theta} \equiv \pm 1$ mod. p.

Hence, either

$$\left.\begin{aligned} &\cos(p-1)\theta = \cos p\theta \,.\cos + \frac{\sin p\theta}{\sin\theta}(\sin\theta)^2 \equiv (\cos\theta)^2 + (\sin\theta)^2 \equiv 1 \\ \text{or} \quad &\cos(p+1)\theta = \cos p\theta \,.\cos\theta - \frac{\sin p\theta}{\sin\theta}(\sin\theta)^2 \equiv (\cos\theta)^2 + (\sin\theta)^2 \equiv 1 \end{aligned}\right\} \text{mod. } p,$$

and writing $\varepsilon = \pm 1$, we must have

$$\cos(p-\varepsilon)\theta \equiv 1 \text{ mod. } p.$$

If possible, let $(p-\varepsilon)$ not contain k, and δ (less than k) be the greatest common measure of k and $(p-\varepsilon)$.

Let $\lambda(p-\varepsilon) - \mu k = \delta$. Then

$$\left.\begin{aligned} &\cos\lambda(p-\varepsilon)\theta \equiv 1 \qquad \frac{\sin\lambda(p-\varepsilon)\theta}{\sin\theta} \equiv 0 \\ &\cos\mu k\theta \equiv 1 \qquad \frac{\sin pk\theta}{\sin\theta} \equiv 0 \end{aligned}\right\} \text{mod. } p.$$

Hence $\cos \delta\theta \equiv 1 \bmod. p$, and, consequently, the resultant of $\psi_k u$ and $\cos \delta\theta - 1$ in respect to $\cos \theta$ must contain p. But $\psi_k u$, when δ is any divisor of k other than k itself, is an algebraical factor of $\frac{\cos k\theta - 1}{\cos \delta\theta - 1}$ *à fortiori*, therefore, the resultant of this last named function of $\cos \theta$ and of $\cos \delta\theta - 1$ must contain p.

This resultant will be the product of the values of $\frac{\cos k\theta - 1}{\cos \delta\theta - 1}$ for every root of $\cos \delta\theta - 1$, it is therefore the δth power of the value of the vanishing fraction $\frac{\cos \mu\varphi - 1}{\cos \varphi - 1}$ $\left[\text{where } \mu = \frac{k}{\delta}\right]$ when $\cos \phi = 1$, *i. e.* of $\left(\frac{\sin \frac{\mu}{2}\varphi}{\sin \frac{\varphi}{2}}\right)^2$ when $\phi = 0$. The resultant is, therefore, $\left(\frac{k}{\delta}\right)^{2\delta}$, which cannot contain p, since, by hypothesis, p is not contained in k. Hence $p - \varepsilon = mk$, or $p = mk \pm 1$. So that, for the extrinsic divisors, the law, both as regards what numbers are and what are not such divisors, is precisely the same as for the cyclotomics of the first species, except that $mk \pm 1$ takes the place of $mk + 1$.

Next, for the intrinsic divisors. Suppose p to be any such, and that $k = k_1 p^j$, where k_1 is prime to p. Then p is a divisor of $\cos k_1 (p^j\theta) - 1$, and, therefore, by what has been shown, must be of the form $mk_1 \pm 1$, unless $(\cos p^j\theta - 1)$ contains p, in which case, since

$$\cos p^j\theta = (\cos p^j\theta - \cos p^{j-1}\theta) + (\cos p^{j-1}\theta - \cos p^{j-2}\theta) + \ldots + \cos \theta,$$

$\cos \theta - 1$ must contain p, and, consequently, p must be a divisor of $\psi_k 2$, *i. e.* of $\chi_k 1$, which we have seen is equal to 1, except when $k_1 = 1$. Hence, p must be of the form $mk_1 \pm 1$. To show the converse, that when $k = k_1 p^j$ and $p = mk_1 \pm 1$, p will be a divisor of $\psi_k u$. Taking, first, the case of $k_1 = 1$ or $k = p^j$, $\psi_k u$, for $u = 2$ will be equal to $\chi_k 1$, which, as we have seen, will divide by p, and not by p^2.

To ascertain if there is any other value of u which will make the function divisible by p, I observe that, for this case, $(\psi_k u)^2 = \frac{\cos p^j\theta - 1}{\cos p^{j-1}\theta - 1}$, which is of the form $\frac{\cos \theta - 1 + Lp}{\cos \theta - 1 + lp}$, and if this function contains p, we must obviously have $\cos \theta \equiv 1 \bmod. p$.

Proceeding to the more general case where $k = k_1 p^j$ and k_1 is other than unity, taking as I did for the first species the specimen case $k = k_1 p, k_1 = abc$,

$p = mk_1 \pm 1$, we shall have

$$(\psi_k u) = \frac{(\cos abcp\theta - 1)(\cos ab\theta - 1)(\cos ac\theta - 1)(\cos bc\theta - 1)(\cos ap\theta - 1)(\cos bp\theta - 1)(\cos cp\theta - 1)(\cos\theta - 1)}{(\cos abc\theta - 1)(\cos abp\theta - 1)(\cos acp\theta - 1)(\cos bcp\theta - 1)(\cos a\theta - 1)(\cos b\theta - 1)(\cos c\theta - 1)}.$$

If, now, $\cos k_1\theta - 1 = 0$, and we suppose $\cos\theta$ to be a root of $\psi_k u = 0$, $\cos p\theta = \cos(\pm\theta) = \cos\theta$, $(\psi_k u)^2$ becomes equal to $\frac{\cos pk_1\theta - 1}{\cos k_1\theta - 1} = p$, and paying no attention to the algebraical sign which is immaterial to our object, we shall have $\psi_k u = p$, and the resultant of $\psi_{k_1} u$ and $\chi_k u$ will be $p^{\frac{1}{2}\tau k_1}$, and, consequently, since $\chi^{k_1} u \equiv 0 \bmod p$ has all its roots real, one of them, at all events, will belong to $\chi_k u \equiv 0 \bmod p$, and precisely in like manner, as in the case for cyclotomics of the 1st species, it may be shown that this reasoning ceases to apply if $\cos\theta$, although satisfying $\cos k_1\theta - 1 = 0$, does not satisfy $\chi^{k_1} u = 0$, in which case the resultant, instead of being a power of p, would become unity, so that the value of $\cos\theta$, satisfying $\cos k_1\theta - 1 \equiv 0 \bmod p$, could not be a congruence root of $\chi_k u \equiv 0 \bmod p$. Finally, as for the case of the 1st species, it may be shown that *every* congruence root of $\chi^{k_1} u \equiv 0$ [when $k = k_1 p^j$ and $p = mk_1 \pm 1$] will satisfy the congruence $\chi_k u \equiv 0 \bmod p$, and that only p, and not p^2, will be a divisor of $\chi_k u$, subject, however, to an exception for the case of $p = 2$, when $k = 2$ or $k = 4$, and also for the case of $p = 2$ and $p = 3$ when $k = 6$.* As regards these intrinsic divisors, it is clear that any root must be the highest prime factor of the index unless its subindex is 3, in which case it may be 2. It is obvious, then, that except the index is 6 or 12, the second cyclotomic function can have only one intrinsic divisor. When the index is 6, the function is simply $u - 1$, and contains of course *every power* of 2 and 3, as well as every power of $6i \pm 1$ as a divisor.

Leaving out of consideration the three known cyclotomics, whose indices are 3, 4, 6, and the one just referred to, $u^2 - 3$, whose index is 12, we may combine the results obtained into the statement that any number, each of whose factors, diminished or increased by unity, contains the index, and any such number, multiplied by the highest prime number in the index, provided that that number, when increased or diminished by unity, contains its subindex, and no other numbers but such as satisfies one or the other of these two descriptions, will be a divisor of a non-linear cyclotomic function of the conjugate class of the second species whose index is other than 12. As regards

*I may probably show this in full in a future note. But since the vast and dazzling theory for cyclotomics of all species, with an indefinite number of classes to each species, has loomed into view, I must confess to a certain feeling of impatience as regards working out these small details for a single class of a single species. The inordinately augmented amplitude of the subject calls for some broader method of treatment.

the index 12, any number, whose factors are all of the form $12m \pm 1$, as also the double, treble and sextuple of any such number, will be a divisor of the function.

By way of example let us consider the indices 15, 21, 35.

$\chi_{15}x$ will contain neither 3 nor 5, $\psi_{15}x$ will contain 5 but not 3.

$\chi_{21}x$ will contain 7 but not 3, $\psi_{21}x$ will contain 7 but not 3.

$\chi_{35}x$ will contain neither 5 nor 7, $\psi_{35}x$ will contain neither 5 nor 7.

To find a value of x which make $\psi_{15}x$ contain 5, write $\psi_3 u = u + 1 \equiv 0$ mod. 5, then $u \equiv -1$.

To find values of x which make $\psi_{21}x$ contain 7, write $u + 1 \equiv 0$ mod. 7, then $u \equiv 6$; and to find values of x which make $\chi_{21}x$ contain 7, write $x^2 + x + 1 \equiv 0$ mod. 7, then $x \equiv 2$ or $x \equiv 4$.

On turning to the table p. 367 it will be seen that

$$\psi_{15}(-1) = 1 + 1 - 4 - 4 + 1 = -5,$$

$$\psi_{21}(-1) = 1 + 1 - 6 - 6 + 8 + 8 + 1 = 7,$$

$$\left.\begin{array}{l}\psi_{21}2 = 4096 + 512 + 64 + 8 + 1 \\ \quad - 2048 - 256 - 16 - 2\end{array}\right\} = 4681 - 2322 = 2359 = 7 \,.\, (16 \,.\, 21 + 1),$$

and of course since $\chi_{21}x^2$ contains $\chi_{21}x$ as an algebraical factor, $\chi_{21}4$ will also contain the intrinsic divisor 7 on the general principle that if λ be any number prime to k, $\chi_k x^\lambda$ must contain $\chi_k x$ as an algebraical factor, as admits of easy demonstration.

Also $\psi_{21}6 \equiv \psi_{21}\left(2 + \frac{1}{2}\right) \equiv \chi_{21}2$ [mod. 7] will also contain 7. Lastly, to mod. 5, for $x = 0, 1, 2, 3, 4$

$$\chi_{35}(x) \equiv 1, 1, 1, 1, 1; \quad \psi_{35}(x) \equiv 1, 1, 1, 1, 1;$$

and to mod. 7, for $x = 0, 1, 2, 3, 4, 5, 6,$

$$\chi_{35}(x) \equiv 1, 1, 1, 1, 1, 1, 1; \quad \psi_{35}(x) \equiv 1, 2, 1, 3, 3, 1, 2;$$

so that neither 5 nor 7 is a divisor of either function to index 35.

Title 3. *On Cyclotomic Functions of Any Species and Class.* The cyclotomic functions, called by me, of the second *sort* or conjugate class of the second species discussed under the preceding title, constitute the leading class of a much more general kind of binomial (*zweigliedrig*) cyclotomics, which it would mislead were I to suppress all allusion to.

Suppose k to contain θ distinct odd prime factors, then we know that the number of square roots of unity to the modulus k is 2^θ, except when k is divisible by 4, in which case it is $2^{\theta+1}$, or $2^{\theta+2}$, according as $\frac{k}{8}$ is fractional or integer, or, setting apart unity, the number remaining is $2^\theta - 1$,

$2^{\theta+1}-1$, $2^{\theta+2}-1$ in the three cases respectively. Let $\sqrt{1}$ (one of the totitives to k) denote any *specific one* of these square roots. Then, if we call ρ any primary kth root of unity and make $x=\rho+\rho^{\sqrt{1}}$, we shall obtain a completely integer function of the degree $\frac{1}{2}\tau k$ in x, which may be called a binomial cyclotomic. When k is divisible by 4, one value of $\sqrt{1}$ will be $\frac{k}{2}+1$, and the value of $\rho+\rho^{1+\frac{k}{2}}$ being zero, the cyclotomic function that ought to be, degenerates into a power of x. Hence, when k is not divisible by 4, the number of binomial cyclotomics is $2^{\theta}-1$, when it is divisible by 4, $2^{\theta+1}-2$, or the double of the former value, and when by 8, $2^{\theta+2}-2$.

All these binomial cyclotomics will be found to possess similar properties to those which have been demonstrated under Title 2 concerning their leading class, as the annexed examples will serve to demonstrate, where the odd prime extrinsic factors it will be seen are of the form $mk+1$ or $mk+\sqrt{1}$; that is to say, in respect to the index, are congruous to one or the other of the *primordinal* totitives 1 and $\sqrt{1}$ where the latter quantity has a definite value for each of the cyclotomics in question.

Thus, suppose $k=15$, the square roots of unity (*quâ* 15) are $\pm 1, \pm 4$. Let $\sqrt{1}=4$, and make $x=\rho+\rho^4$, then it will be found that $x^4-x^3+2x^2+x+1$ will contain the four roots of x and all the odd prime divisors of this function are of the form $15m+1, 4$.

Or, again, let $\alpha=\rho+\rho^{11}$, then it will be found that x is a root of the function $x^4+x^3+x^2+x+1$, the prime factors of which, other than 5, are of the form $15m+1, 11$, which is, in effect, the same as the form $5m+1$.

Again, let $k=20$. The values of $\sqrt{1}$ [mod. 20] are $\pm 1, \pm 9$. If we were to put $x=\rho+\rho^{11}$, its value would be zero, but writing $x=\rho+\rho^9$, we shall find it will be the root of x^4+3x^2+1, all the prime factors of which, other than the intrinsic one 5, are of the form $20m+1, 9$.*

We may now proceed to generalize these results by considering cyclotomics of every possible numerosity of grouping for a given index, and of every possible order of conjunction for a given numerosity—in a word, we are brought face to face with the most general theory of ν-nomial cyclotomic functions.†

* If $k=8$ and we take $x=\rho+\rho^3$ it will be a root of x^2+2 of which the odd extrinsic factors will be of the form $8m+1, 3$.

† All the species with their several classes here referred to form but a single genus of cyclotomic functions. The second genus will arise from the subdivision of groups into smaller groups and so on continually.

I have accordingly calculated cyclotomic functions for the cases following:

$k=15$	$\mu=2$	$\nu=4$
$k=21$	$\mu=4$	$\nu=3$
	$\mu=3$	$\nu=4$
	$\mu=2$	$\nu=6$
$k=26$	$\mu=4$	$\nu=3$
	$\mu=2$	$\nu=6$
$k=28$	$\mu=4$	$\nu=12$
	$\mu=2$	$\nu=6$
$k=25$	$\mu=5$	$\nu=4$
$k=33$	$\mu=5$	$\nu=4$
	$\mu=4$	$\nu=5$
	$\mu=2$	$\nu=10$

Understanding by the "totitives" of k the numbers less than k and prime to it, these totitives may be arranged in (among others) the natural groups hereunder written.

Totitives to 15 for $\mu=2$, $\nu=4$

1	4	11	14
2	7	8	13

" to 21 for $\mu=4$, $\nu=3$

1	4	16
2	8	11
5	17	20
10	13	19

" " for $\mu=3$, $\nu=4$

1	8	13	20
2	5	16	19
4	10	11	17

" " for $\mu=2$, $\nu=6$

1	4	5	16	17	20
2	8	10	11	13	19

" to 26 for $\mu=4$, $\nu=3$

1	3	9
5	15	19
7	11	21
17	23	25

Totitives to 26 for $\mu=3$, $\nu=4$

1	5	21	25
3	11	15	23
7	9	17	19

" " 28 for $\mu=4$, $\nu=3$

1	9	25
3	27	19
5	17	13
11	15	23

" " for $\mu=2$, $\nu=6$

1	3	9	19	25	27
8	10	11	17	18	23

" to 25 for $\mu=5$, $\nu=4$

1	7	18	24
2	11	14	23
3	4	21	22
6	8	17	19
9	12	13	16

To save space, I omit the groupings to $k=33$.

If, in any of the above tables, we call the totitives of the several rows,

$$\begin{matrix} \tau_{1,1} & \tau_{1,2} \ldots \tau_{1,\nu} \\ \tau_{2,1} & \tau_{2,2} \ldots \tau_{2,\nu} \\ \ldots\ldots\ldots\ldots \\ \tau_{\mu,1} & \tau_{\mu,2} \ldots \tau_{\mu,\nu} \end{matrix}$$

and if ρ be a primitive root of x^k-1, and we write $R_\theta = \rho^{\tau\theta,1} + \rho^{\tau\theta,2} + \ldots \rho^{\tau\theta,\nu}$, $R_1, R_2, \ldots R_\mu$ will be the roots of a cyclotomic of the νth species to the index k, or, as we may say, the index k and *nome* ν.

The values of the cyclotomic functions may be found most easily by calculating all the values of σ_i (the sum of the ith powers of its roots), from $i=1$ to $i=\mu$ where $\mu=\frac{\tau(k)}{\nu}$.

The value of $X_{k,\nu}$ will then be the sum of the terms not containing negative powers of x in the development of $x^\mu \left\{ e^{-\frac{\sigma_1}{x} - \frac{\sigma_2}{2x^2} - \ldots - \frac{\sigma_\mu}{\mu x^\mu}} \right\}$.

It will, of course, be recognized that the first row of numbers (the primordinal totitives, as we may term them) in any of the foregoing natural

schemes of decomposition of the kth primitive roots of unity into groups are νth roots (not necessarily comprising any primitive root) of unity in respect to the index k as modulus.

The values of the cyclotomics are exhibited in the annexed table.

Index.	Nome.	Cyclotomic function.	Primordinal Totitives.
15	4	$x^2 - x - 1$	1, 4, 11, 14
21	3	$x^4 - x^3 - x^2 - 2x + 4$	1, 4, 6
"	4	$x^3 - x^2 - 2x + 1$	1, 8, 13, 20
"	6	$x^2 - x - 5$	1, 4, 5, 16, 17, 20
26	3	$x^4 - x^3 + 2x^2 + 4x + 3$	1, 3, 9
"	4	$x^3 - x^2 - 4x - 1$	1, 5, 21, 25
28	3	$x^4 - 3x^2 + 4$	1, 9, 25
"	6	$x^2 - 7$	1, 3, 9, 19, 25, 27
25	4	$x^5 - 10x^3 + 5x^2 + 10x + 1$	1, 7, 18, 24
33	4	$x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$*	$\pm 1, \pm 10$
"	5	$x^4 - x^3 - 2x^2 - 3x + 9$	$1, -2, 4, -8, 16$
"	10	$x^2 - x - 8$	$\pm 1, \pm 2, \pm 4, \pm 8, \pm 16$

In each of the above cases calling the index k, its totient $\mu\nu$, the nome ν and the primordinal totitives $\theta_1, \theta_2 \ldots \theta_\nu$, it will be found that all the *odd* extrinsic prime number divisors (*i. e.* primes dividing the function but not its index) are of the form $mk + \theta_1, \theta_2, \ldots \theta_\nu$.

Here, for the present, I must be content to leave this great theory, or I should be in danger of never finding my way back from it to the original object of the memoir which, although its parent, it transcends in importance; for Bachmann's work, as it seems to me, gives proof, that Cyclotomy is to be regarded not as an incidental application, but as the natural and inherent centre and core of the arithmetic of the future.

Remark on the intrinsic divisors of cyclotomic functions of the 1st species.

It has been seen that if $k = \frac{p-1}{m} p^{j-1} = k_1 p^{j-1}$, $\chi_k x \equiv 0 \; mod.\; p^j$ has all its roots the same as those of $\chi_{k_1} x \equiv 0 \bmod. p$ and does not contain p^2. If, then, we make j successively $0, 1, 2 \ldots j-1$ it will follow that $\chi_{k_1}, \chi_{k_1 p}, \chi_{k_1 p^2}, \ldots \chi_{k_1 p^{j-1}}$ will each contain p, but only in the first power for the same τk_1 values of x. Hence $x^{\frac{(p-1)p^{j-1}}{m}} - 1$, which contains all the above written cyclotomics, will

* The values of $\sigma_2, \sigma_3, \sigma_4, \sigma_5$ in this case follow the noticeable progression 9, 4, 25, 16.

contain p^j, so that $x^{\frac{\tau p^j}{m}} - 1 \equiv 0 \bmod. p^j$ will have $\tau\left(\frac{p-1}{m}\right)$ primitive roots, and it is easy to see that $x^{\frac{k}{n}} - 1$ will not have any congruence root in common with $x^{k_1} - 1$ in respect to the modulus p^j.

The theory of intrinsic divisors, it will thus be seen, contains within itself the whole theory of primitive roots, which I notice because it induces me to withdraw the remark made in a previous foot note that the exact determination of the properties of the intrinsic cyclotomic divisors is a matter of comparatively small importance.

NOTES TO PROEM.

1. *On the rational in- and- exscribed triangle to the cubic curve* $x^3 - 3xy^2 - y^3 + 3z^3 = 0$.

IN the proem it was, under another form of expression, intimated in advance of what will be shown in the second section of this chapter, that the curve $x^3 + y^3 + Az^3 = 0$ has a correspondence with the curve $x^3 - 3xy^2 - y^3 + 3Az^3 = 0$, of such a kind that whenever the second equation has a rational solution, the same must be true of the first, so that (*ex. gr.*) on making $A = 1$, the solubility of $x^3 - 3xy^2 - y^3 + 3z^3 = 0$ in integers implies the like of the equation $x^3 + y^3 + z^3 = 0$. Hence it might, at first sight, be rashly inferred (which is what happened to me when writing the 2d foot-note to page 284 from a sick bed) that since a cube number cannot be broken up into the sum of two others, the former of these last written equations is insoluble in integers. But the fact stares one in the face that it has three solutions in integers, viz:

$$x:y:z :: \quad 1: \quad 1:1$$
$$x:y:z :: -2: \quad 1:1$$
$$x:y:z :: \quad 1: -2:1$$

In general, (except at points of inflexion or at points whose ith tangentials are points of inflexion*), one rational point in a cubic gives rise to an infinite series of rational derivatives, but in this case the three points $1:1:1$, $-2:1:1$, $1:-2:1$ are the angles of a triangle in- and- exscribed to the curve $x^3 - 3xy^2 - y^3 + 3z^3$, and are the only rational points on the curve. Each of them is its own third tangential, so that, at any one of the three, an

* Thus we have the following distinction of cases as regards the algebraically rational derivatives of any point on a cubic curve: 1°. An infinite succession of links. 2°. A finite open chain reducing in the case of inflexions to a single point. 3°. A closed chain with a finite number of links.

infinite number of cubic curves can be made to pass having plethoric, or, so to say, pluperfect contact with each other (9-point contact) and accordingly will not intersect each other in any other point.

To these three points will be found to correspond (as will presently be shown in § 2) points for which x or y is zero in the curve $x^3+y^3+z^3=0$. This perfectly explains the seeming paradox.

The sides of the rational in- and- exscribed triangle are easily seen to be $y-z=0$, $x+y+z=0$, $x-z=0$.

In general, if any cubic be thrown into the form $x^2y+y^2z+z^2x+\lambda xyz$, it will obviously be in- and- exscribed to the triangle x, y, z*. In the present instance, if we write $x-z=u$, $y-z=v$, $x+y+z=-w$, it will be found that the curve $x^3-3xy^2-y^3+3z^3$ becomes simply $uv^2+vw^2+wu^2$, of which the Hessian is the three straight lines $u^3+v^3+w^3-3uvw$. If we take the sides of an equilateral triangle whose area is $\frac{1}{2}\Delta$ for the axes of u, v, w, we shall have $u+v+w=\Delta$, and the three real points of inflexion being in the line $u+v+w$, will pass off to infinity, so that the curve will possess three infinite branches. Writing $\omega=\frac{2\pi}{9}$, each asymptote will cut the sides of the angles of reference in 3 pairs of segments abutting at the several angles, such that the ratio to each other of the segments in the several pairs, taken in regular order, will be (for the three asymptotes respectively),

$$\begin{matrix} \frac{\cos\omega}{\cos 2\omega}, & \frac{\cos 2\omega}{\cos 4\omega}, & \frac{\cos 4\omega}{\cos\omega}, \\ \frac{\cos 2\omega}{\cos 4\omega}, & \frac{\cos 4\omega}{\cos\omega}, & \frac{\cos\omega}{\cos 2\omega}, \\ \frac{\cos 4\omega}{\cos\omega}, & \frac{\cos\omega}{\cos 2\omega}, & \frac{\cos 2\omega}{\cos\omega}. \end{matrix}$$

These ratios, of course, remain the same, for the conjugate cubic $u^2v+v^2w+w^2u$, except that the order of the readings has to be reversed.

According to my departed friend, (of cherished memory), Otto Hesse's dictum, I suppose it may almost be taken for granted without proof, which would obviously be easy, that the two sets of real asymptotes for the conjugate cubics will envelop one and the same conic.

In a future excursus I propose to demonstrate the existence of an infinite number of polygons in- and- exscribable about any given cubic, and to deter-

*For x will touch the cubic at x, y; y at y, z; z at z, x.

mine the number of such polygons for any existent number of sides. Since $uv^2 + vu^2 + uw^2 = 0$ is equivalent to $(2uw + v^2)^2 + (4u^3v - v^4) = 0$, we are able to deduce, from the fact that one cube cannot be the sum of two others, the theorem that the equation $v^4 - 4u^3v = t^2$ has no solution in integers,* (zeros excluded) which seems to me (the way in which it is got, I mean, not the theorem itself) a very surprising inference.

SCHOLIUM. *On triangles and polygons in- and- exscribable to a general cubic.*

The apices of any such triangle must be points which are their own 3d tangentials. Any such point, it may be shown, is completely defined by the condition that two right lines, drawn, the first through it and any one chosen at will, of the 9 points of inflexion, the second through its tangential and some other point of inflexion, shall meet the curve in the same point.

If, then, the cubic be written under its canonical form, and we select the point of inflexion (I), for which $x = 1$, $y = 1$, and through the point $P(x, y, z)$, which is to be its own 3d tangential, and I draw a ray meeting the curve in P', and through P' and Q, the tangential to P, [*i. e.* the point whose coordinates are $x(y^3 - z^3)$, $y(z^3 - x^3)$, $z(x^3 - y^3)$] draw a ray, the point (X, Y, Z), where that ray meets the curve, must be a point of inflexion, and, *vice versa*, if the condition is fulfilled, P is its own 3d tangential.

It will be found that

$$\begin{aligned} X &: -x^6y^3 - y^6z^3 - z^6x^3 + 3x^3y^3z^3 \\ :: Y &: -x^3y^6 - y^3x^6 - x^3z^6 + 3x^3y^3z^3 \\ :: Z &: \quad xyz\,(x^6 + y^6 + z^6 - x^3y^3 - y^3z^3 - z^3x^3), \end{aligned}$$

and we must have $X = 0$ or $Y = 0$ or $\frac{Z}{xyz} = 0$, the factor which figures in Z being disregarded, because it would lead to the 9 points of inflexion, which

*Suppose the equation $u^2v + v^2w + w^2u = 0$ is resoluble in non-zero integers. We may regard u, v, w as having no common measure, as any such, if it existed, could be driven out of the equation by division. Suppose p to be any prime number entering exactly α times into u and β times into v; then writing $u = p^\alpha u_1$, $v = p^\beta v_1$, since w^2u contains p^α, and v^2w, $\beta^{2\beta}$, we must have $\alpha = 2\beta$ and $p^{3\beta}u_1^2v_1 + v_1^2w + w^2u_1 = 0$, and proceeding similarly with each prime common measure of u, v of v, w and of w, u, it is obvious that, calling the greatest common measure of these three pairs δ, ε, θ, we must have $\delta^3u'^2v' + \varepsilon^3v'^2w' + \theta^3w'^2u' = 0$, where u', v', w' have no two of them any common measure. Hence, apart from algebraical sign u', v', w' must be each of them unity, and the above equation may be written $\delta_1^3 + \varepsilon_1^3 + \theta_1^3 = 0$, the same in form as that which gave birth to the equation $\xi^3 - 3\xi\eta^2 + \eta^3 = 0$, of which $u^2v + v^2w + w^2u = 0$ is a transformation. It is worthy also of remark that the two equations $u^2v + v^2w + w^2u = 0$ and $x^3 + y^3 + z^3 = 0$ pass into one another through the medium of the self-reciprocal substitution-matrix

$$\begin{matrix} 1 & 1 & 1 \\ \rho^{\frac{1}{3}} & \rho^{\frac{4}{3}} & \rho^{\frac{7}{3}} \\ \rho^{\frac{2}{3}} & \rho^{\frac{8}{3}} & \rho^{\frac{5}{3}} \end{matrix},$$

where ρ is a primitive cube root of unity.

may be thrown out of account, as for each of them the in- and- exscribed triangle reduces to a point.

Combining each of the above equations taken separately with the equation to the cubic, we see that there will be $3 \times (9+9+6)$, *i. e.* 72 points forming the apices of 24 in- and- exscribed triangles to the cubic. It may be shown further that these 24 triangles consist of 12 pairs of conjugate triangles, every pair being so situated that each is a threefold perspective representation of the other, the three perspective centres being some one of the 12 sets of 3 collinear points of inflexion.*

The 24 in- and- exscribed triangles may therefore be distributed into 4 groups, each containing 3 pairs of conjugate triangles. This theory and the general one of in- and- exscribed polygons with any number of sides to a cubic curve will be treated more fully in a future excursus. It may, however, be remarked here that the equation $\frac{Z}{xyz} = 0$ is equivalent to the two $x^3 + \rho y^3 + \rho^2 z^3 = 0$, and $x^3 + \rho^2 y^3 + \rho z^3 = 0$, so that 18 of the points xyz may be found by solving two cubic equations between x^3, y^3 or y^3, z^3 or z^3, x^3. The remaining 54 may be found by substituting for x, y, z respectively (in the simple equations which express their ratios)

1°.	$x+y+z$	$x+\rho y+\rho^2 z$	$x+\rho^2 y+\rho z$
2°.	$x+y+\rho z$	$x+\rho y+z$	$\rho x+y+z$
3°.	$x+y+\rho^2 z$	$x+\rho^2 y+z$	$\rho^2 x+y+z$

(these substituted values, together with the original values of x, y, z, rep-

---

*ABC, LMN are in threefold perspective when AL, BM, CN; AM, BN, CL; AN, BL, CM meet in three several points. If ABC be taken as the triangle of reference and the coordinates of L, M, N are a, b, c; a', b', c'; a'', b'', c'' respectively, the triple "perspectivische lage" requires only the satisfaction of two conditions, viz: $ab'c'' = bc'a'' = ca'b''$, so that there is nothing between single and triple perspective relation. This statement constitutes a porism. The double condition $ba'c'' = cb'a'' = ac'b''$ of course corresponds to the contrary relation of triple perspective where AM, BL, CN; AL, BN, CM; AN, BM, CL meet in three several points.

Let I, I', I'', J, J', J'', K, K', K'' denote three points of collinear inflexions and P, Q the 3d point collinear with P and Q any two points on the cubic. If Q is the tangential to P, one of the vertices in question, it may be proved that any inflexion I, being assumed, another J may be found such that $IP = JQ$. From this it follows that PQ will satisfy the 10 equations

$$PP = Q$$

$IP = JQ$	$JP = KQ$	$KP = IQ$
$I'P = J'Q$	$J'P = K'Q$	$K'P = I'Q$
$I''P = J''Q$	$J''P = K''Q$	$K''P = I''Q$.

These will necessarily continue to be satisfied when I and J are interchanged, provided that $4P$, Q be written KP and KQ or $K'P$ and $K'Q$ or $K''P$ and $K''Q$, and, consequently, to P, Q, R one in- and- exscript, will correspond another denotable indifferently by KP, KQ, KR, $K'P$, $K'Q$, $K'R$, $K''P$, $K''Q$, $K''R$, which will obviously therefore be in triple *perspectivische lage* with the first named one.

resenting the sides of the 4 triangles which contain 3 points of inflexion on each side).*

We may thus neglect altogether the equations $X=0$, $Y=0$, the values of x, y, z, to which they would lead, being comprised among those resulting from the above method.†

In like manner, as we have found the number of in- and- exscribable triangles, it may be shown that the number of quadrilaterals in- and- exscribable to a cubic is 54, and of p-laterals, when p is a prime number, $8(2^{p-1}-1)(2^{p-2}+1)$. For a k-sided polygon, where k is any number whatever, the rule is as follows. Let

$$\phi x = 8(2^{x-1}-(\overline{1})^{x-1})(2^{x-2}-(\overline{1})^{x-2}),$$

and let the totient of k, (supposed to contain i distinct prime factors) be expressed in the usual manner as the sum of 2^{i-1} positive terms P and the like number 2^{i-1} negative terms Q.

Then it may be proved (for it requires proof) that $\Sigma\phi P - \Sigma\phi Q$ will contain k; the quotient will contain the number of k-sided polygons in- and- exscribable about a cubic.

This theorem does not accord with the formula given by Professor Cayley in the Phil. Tr. for 1871, as quoted in the Math. Fortschr., Vol. III.

The number of triangles in- and- exscribable to a curve whose order is x, whose class is X and whose number of cusps + three times its class is ξ, is there stated to be

$$X^4+(2x^3-18x^2+52x-46)X^3+(\overline{18}x^3+162x^2-420x+221)X^2$$
$$+(52x^3-420x^2+704x+172)X+(x^4-46x^3+221x^2+172x)$$
$$+\xi\{\overline{9}X^2+(\overline{12}x+135)X+(\overline{9}x^2+135x-600)\}.$$

† When the cubic is $x^3+y^3+z^3$, X, Y, Z become $x^9+6x^6y^3+3x^3y^6-y^9, \ldots, xyz(x^6+x^3y^3+y^6)$ $X=0$ then gives $\frac{x^3}{y^3}=t-t^2$ if $t^3-3t+1=0$, *i. e.*, $t=2\cos\frac{2\pi}{9}$, $2\cos\frac{4\pi}{9}$, $2\cos\frac{8\pi}{9}$; calling the three values of $\frac{x^3}{y^3}$ thus obtained $\tau_1\tau_2\tau_4$, one of the two real in- and- exscribed triangles will have at its vertices $\frac{x}{y}, \frac{y}{z}, \frac{z}{x} = \tau_1^{\frac{1}{3}}, \tau_2^{\frac{1}{3}}, \tau_4^{\frac{1}{3}} = \tau_2^{\frac{1}{3}}, \tau_4^{\frac{1}{3}}, \tau_1^{\frac{1}{3}} = \tau_4^{\frac{1}{3}}; \tau_1^{\frac{1}{2}}; \tau_2^{\frac{1}{3}}$ respectively, and the triangle conjugate to it will have at its vertices $\frac{x}{y}, \frac{y}{z}, \frac{z}{x}$ equal to the same three systems of ratios.

† If $x^3+y^3+z^3+3mxyz$ be the given cubic, one set of 9 points will be found from the equation

$$[(1-\rho)y^3+(1-\rho^2)z^3]^3+27m^3(\rho y^6z^3+\rho^2y^3z^6)=0,$$

or

$$y^9-3((1-\rho^2)m^3-\rho^2)y^6z^3-((1-\rho)m^3-\rho)y^3z^6+z^9=0,$$

and the fellow set by interchanging y and z. The disadvantage of this method consists in its leading to equations with imaginary coefficients for finding *inter alia* real roots which the equations $Y=0$ or $Z=0$, being of odd degrees, show must necessarily always exist.

On making $x = 3$, $X = 6$ and $\xi = 18$ we ought to have 24 the number of in- and- exscribable triangles to a general cubic, but on making these substitutions the result will be found to be zero. It is *quite certain*, therefore, that this formula requires some correction which has been overlooked by its illustrious author. For I have actually, in the text, given a cubic and a triangle in- and- exscribable to it, not to add that it is manifestly impossible for a general cubic to refuse to pass under the form $xy^2 + yz^2 + zx^2 + mxyz$.

Before quitting this subject I wish to call attention to the fact that the formula above given for composite numbers is a form deduced from the form ϕk precisely as in the excursus, the expression for $\log \chi_k^x$ was deduced from $\log (x^k - 1)$.* It is clear from general logical considerations that this sort of deduction must be continually liable to occur and a name is imperatively called for to express it as much as one was formerly wanted to express the kind of deduction which leads from an algebraical form to its Hessian. Here the deduction depends on the arithmetical constitution of the subject of the form, and it is a great impediment to the free course of ratiocination not to be able to pass at once, in language and in thought, from the form to its deduct. I intend then in future to call such deduct the *functional totient* of the form, say ϕk, from which it is derived, and to denote it by $(\phi\tau)\, k$. This constitutes a very important gain to arithmetical nomenclature.

I would further call attention to the fact of an arithmetical theorem of some considerable difficulty to demonstrate (by means of Fermat's extended theorem) in the general case as any one, who goes through the process of the proof for the single case of $k =$ the product of two primes, will easily satisfy himself, (I mean the theorem that the *functional totient* of $8(2^{k-1} - (\overline{1})^{k-1})(2^{k-2} - (\overline{1})^{k-2})$ is always divisible by k) should admit of an intuitional proof through the intervention of a pure property of cubic curves without any recourse to concepts drawn from reticulated arrangements, as in the applications of geometry to arithmetic made by Dirichlet and Eisenstein. This example of the possibility of such application (akin to that whereby the binomial theorem is made to prove that $\frac{\pi(m+m')}{\pi m \,.\, \pi m'}$ is an integer) is, as far as I can recall, without a precedent in mathematical history.

*The expression actually there given is for χ_k^x and not its logarithm; using the notation explained above, and calling $\phi k = \log (x^k - 1)$ the cyclotomic of the 1st species to the index k, is $e^{(\phi\tau),k}$.

Postscriptum.

Mr. Franklin obtains my result as follows: The condition that the $(i-1)$th tangential shall lie on the first polar is of the degree $2.4^{i-1}+1$; the number of points on the cubic (exclusive of inflexions) satisfying this condition is $3(2.4^{i-1}+1)-27=24(4^{i-2}-1)$. But the $(i-1)$th tangential will be on the first polar, not only when it is a true antitangential, but also when it is the original point itself or the consecutive point; so that we have to deduct from the above number twice the number of points (exclusive of inflexions) whose $(i-1)$th tangentials are the points themselves; *i. e.* denoting by u_i the number of vertices of in- and- exscribed i-laterals, we have

$$\begin{aligned} a_i &= 24(4^{i-2}-1)-2u_{i-1} \\ &= 24\{2^{2i-4}-2^{2i-5}+\ldots+(-2)^{i-1}-(1-2+2^2-\ldots+(-2)^{i-3}\} \\ &= 8(2^{i-1}+(-1)^{i-2})(2^{i-2}-(-1)^{i-2}), \end{aligned}$$

which will be the number of the vertices, not only of true i-laterals, but also of all the $\frac{i}{\delta}$-laterals, (δ being any divisor of i except i itself) as well. Mr. Franklin further suggests that the discrepancy between this result for $i=3$ and Prof. Cayley's formula may be due to the latter not taking account of the peculiar kind of in- and- exscription in which the curve is in- and- exscribed at the same points. Finally, let us call the *summant* of a number k of the form $a^\lambda.b^\mu.c^\nu$ (a, b, c being primes) the well-known quantity consisting of $(1+\lambda)(1+\mu)(1+\nu)\ldots$ terms which represents the sum of the divisors of k. We may speak of a *functional summant* to ϕk obtained by prefixing ϕ to each monomial term in the *development* of the summant and denote it by $(\phi\sigma)k$. The equation $(\phi\sigma)k=\omega(k)$ has for its solution $fk=(\omega\tau)k$. My method gives at once, for the *functional summant* of u^k (*without exclusion* of inflexions) $(2^k-\tau^k)^2$, and accordingly, the functional totient to this form divided by k is the simplest expression for the number of ex- and- inscribed k-laterals to the cubic. Thus, for $k=1, 2, 3, 4, 5, 6$, that number is 9, 0, 24, 54, 216, 648 respectively.

2. *On 2 and 3 as cubic residues.*

For the benefit of those among my readers in this country who may not have access to the later works on arithmetic, it may be as well to point how with the aid of their Gauss or Legendre they may verify the conditions

which, later on, I shall have need to employ of 2 or 3 being cubic residues to k, a prime of the form $6i+1$. The cyclotomic function of the third degree in the variable to the index k, if we make $4k = m^2 + 27n^2$, is known to be $x^3 + x^2 - \frac{k-1}{2}x - \frac{3k-1+\varepsilon mk}{27}$, where $\varepsilon^2 = \pm 1$ and $m - \varepsilon$ contains 3. Connecting this with the same function formed in the manner in which the cyclotomics in the Excursus under Title 3 have been calculated, calling U the number of solutions of the congruence $1+\beta+\gamma \equiv 0 \pmod{k}$, where β, γ are any two unequal cubic residues to k, and θ the number of solutions (1 or 0) of the congruence $1+2\beta \equiv 0 \pmod{k}$, it will easily be found, by comparing the constant terms in the two expressions, that

$$U + \frac{3\theta}{2} = \frac{k-8+\varepsilon m}{18}.$$

Hence, when $\theta = 1$, *i. e.* when 2 is a cubic residue, m (and therefore also n) must be even, and consequently when $\theta = 0$, or 2 is not a cubic residue, m must be odd, and *vice versâ*.

Again, if we compare the values of the sum of the 4th powers of the roots of the cyclotomic as found by the general method with that deducible from the given function, we shall find

$$V + \frac{2}{3}\mathfrak{S} = \frac{k^2+3k-66-4m\varepsilon k}{162},$$

where V is the number of solutions of the congruence $1+\beta+\gamma+\delta \equiv 0$, plus the number of solutions of the congruence $1+\beta+2\gamma \equiv 0$ (β, γ, δ being cubic residues to k) and $\mathfrak{S}$ the number of solutions of the congruence $1+3\beta \equiv 0 \pmod{k}$, *i. e.* 1 or 0, according as 3 is, or is not, a cubic residue to k.

The numerator is necessarily divisible by 54, but the criterion of $\mathfrak{S}$ being 0 or 1 depends on its being divisible or not by 81. On substituting for k its value in terms of m and n, it will be found that 16 times the numerator to modulus 81 is congruous with 54 times $(n^2-1) + \varepsilon\left\{\left(\frac{m-\varepsilon}{3}\right)^3 - \frac{m-\varepsilon}{3}\right\}$, and consequently is divisible or not by 81 according as n is not, or is, divisible by 3. Hence $\mathfrak{S} = 1$ when n is divisible by 3 and otherwise is 0.

The joint effect of these two results may be translated into the following statement, which is better adapted than the more complete* form of enunciation would be to the purposes of this memoir.

*I mean more complete in the sense of fixing the cubic character in the case of 3 being a non-residue, which is unimportant to the matter in hand.

If $k = f^2 + 3g^2$, *when* $(f \pm g)$ *contains* 9, 3 *is, and* 2 *is not, a cubic residue; when* g *contains* 3, *but not* 9, 2 *is, and* 3 *is not, a cubic residue*; *when* g *contains* 9, 2 *and* 3 *are each of them cubic residues, and in any other case neither* 2 *nor* 3 *is a cubic residue to* k.*

The equation $U + \frac{3\theta}{2} = \frac{3k - 1 + \varepsilon mk}{18}$ contains a complete solution of the interesting question, "How many times, if the cubic residues to a given modulus are set out in a regular ascending series, will consecutive terms differ from one another by a single unit?" When 2 is not a cubic residue, the answer is obviously $2U$, for $1 + \alpha + \beta = n$ gives two sequences, α, $n - \beta$ and β, $n - \alpha$, differing by units. But when 2 is a cubic residue, there will be three extra sequences not contained among the $2U$ just spoken of, viz:

$$1, 2; \quad \frac{k-1}{2}, \frac{k+1}{2}; \quad k-2, \; k-1.$$

Hence, in each case, the number is $2U + 3\theta$, *i. e.* $\frac{k - 8 + \varepsilon m}{9}$, or, if we count in 0 as a residue, $\frac{k + \varepsilon m + 1}{9}$.

SECTION 2.

On certain numbers and classes of numbers that cannot be resolved into the sum or difference of two rational cubes.

Title 1. *Theorem on irresoluble numbers whose prime factors other than* 2 *or* 3 *are of the form* $18n + 5$ *or* $18n + 11$.† I propose to prove the following collective theorem. If A represents any one of the numbers 1, 2, 3, 4, 18, 36 or any number of the form

$$\begin{array}{c} p, \; q, \quad p^2, \; q^2, \\ 9p, \; 9q, \quad 9p^2, \; 9q^2, \\ 2p, \; 4q, \quad 4p^2, \; 2q^2, \\ pq, \; p_1p_2^2, \; q_1q_2^2, \; p^2q^2, \end{array}$$

(where any p means a prime number of the form $18n + 5$, and any q a prime of the form $18n + 11$) A will be irresoluble into the sum of two unequal rational cubes.

*In other words, if $4p = m^2 + 27n^2$ [an equation always possible when $p = 6n + 1$], n divisible by 2 is the necessary and sufficient condition of 2, and n divisible by 3 is the necessary sufficient condition of 3, being a cubic residue to p.

† This theorem includes and transcends all the cases of irresolubility that had been discovered prior to the date of publication of the Proem in the last number of the Journal, with the exception of certain specific numbers whose irresolubility had been determined by the Abbé Pépin.

Lemma. If we decompose A (when it is not a prime) into any factors f, g, h, prime to each other, other than 1, 1, A, the equation $fx^3 + gy^3 + hz^3 = 0$ will be irresoluble in integers.

I prove this by showing that the above equation converted into a congruence to *modulus* 9 is irresoluble in integers.

x^3, y^3, z^3, each of them to this modulus is equivalent to one or the other of the three numbers $\overline{1}$, 0, 1.

$$\begin{array}{llllll} p, p_1, p_2 & \text{to this modulus is} & & \text{equivalent to} & & \overline{4} \\ q, q_1, q_2 & " & " & " & " & 2 \\ p^2, p_1^2, p_2^2 & " & " & " & " & \overline{2} \\ q, q_1^2, q_2^2 & " & " & " & " & 4, \end{array}$$

and on inspection, it will easily be verified that the limited linear congruence $f\lambda + g\mu + h\nu \equiv 0$ [mod. 9], where λ, μ, ν must each be picked out of the three numbers $\overline{1}$, 0, 1, has no solution.

Hence, if $fx^3 + gy^3 + hz^3 = 0$ and $f.g.h = A$, and x, y, z are supposed to be prime to each other, two of the quantities f, g, h will be unities and the third equal to A.

Let, now, $x^3 + y^3 + Az^3 = 0$ be supposed soluble in integers. Then, since A contains no $6n + 1$ prime, we must have

$$\left.\begin{array}{l} x + y = A\zeta^3 \\ x^2 - xy + y^2 = \omega^3 \\ z = -\zeta\omega \end{array}\right\} \text{when } x+y \text{ does not contain 3,}$$

and

$$\left.\begin{array}{l} x + y = 9A\zeta^3 \\ x^2 - xy + y^2 = 3\omega^3 \\ z = -3\zeta\omega \end{array}\right\} \text{when } x+y \text{ contains 3.}$$

If $x + y$ is even, since $x^2 - xy + y^2 = \left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2$, we must have $\frac{x+y}{2} + \sqrt{-3}\,\frac{x-y}{2} = (\xi + \sqrt{-3}\eta)^3$, when $x + y$ does not contain 3, and $\frac{x-y}{2} + \sqrt{-3}\,\frac{x+y}{6} = (\xi + \sqrt{-3}\eta)^3$, when $x + y$ contains 3. In the one case $\frac{x+y}{2} = \xi^3 - 9\eta^3$, $\frac{x-y}{2} = 3\xi^2\eta - 3\eta^3$, and in the other $\frac{x-y}{2} = \xi^3 - 9\eta^2\xi$, $\frac{x+y}{6} = 3\xi^2\eta - 3\eta^3$.

In the one case, then, $2\xi(\xi - 3\eta)(\xi + 3\eta) = A\zeta^3$, and in the other $2\eta(\xi - \eta)(\xi + \eta) = A\zeta^3$. In either case, therefore, there is an equation-system

of the form $\rho\sigma\tau = -A\zeta^3$, $\rho+\sigma+\tau=0$, to be satisfied; therefore, disregarding permutations of ρ, σ, τ, we must have

$$\rho = fx_1^3, \quad \sigma = gy_1^3, \quad \tau = hz_1^3$$
$$f.g.h = A, \quad x_1y_1z_1 = -\zeta$$
$$fx_1^3 + gy_1^3 + hz_1^3 = 0,$$

and consequently by the Lemma $x_1^3 + y_1^3 + Az_1^3 = 0$ (or the same equation with x_1, y_1, z_1 interchanged) where $x_1y_1z_1$ is a factor of z.

Continuing the same process perpetually, as long as the new x and y have the same parity, each new x, y, z being contained in the immediately preceding z, must perpetually decrease, and if the process could be indefinitely continued, x and y must each evidently become unity, since otherwise z could go on decreasing without limit. This could only happen when $A=2$, and even then is excluded by the condition that the cubes are to be unequal as well as rational.* Hence, if the proposed equation is soluble at all, it must contain solutions in which x and y are one even and the other odd.

On this hypothesis, let us consider separately case (1), where $x+y$ does not, and case (2) where $x+y$ does contain 3.

Case (1). Here $(x+y)^2+3(x-y)^2=4(L^2+3M^2)=4\omega^3$, and all the solutions of this equation are necessarily included in those of the system $L^2+3M^2=\omega^3$, $x+y=L+3M$, $x-y=L-M$.

Hence $x+y=\xi_1^3+9\xi_1^2\eta_1-9\eta_1^2\xi_1-9\eta_1^3=A\zeta^3$. On making $\xi_1=\xi-3\eta_1$, this becomes $\xi^3-36\xi\eta_1^2+72\eta_1^3=A\zeta^3$, or, making $\eta'=6\eta_1$, $3\xi^3-3\xi\eta'^2+\eta'^3=3A\zeta^3$, which, on writing $\eta'=\eta+\xi$, becomes $\eta^3-3\eta\xi^2+\xi^3=3A\zeta^3$, where A unless it is unity contains at least one factor that is not of the form $18n\pm1$, or else (in the case when $A=3$) the square of 3. Hence, by virtue of the cyclotomic law for index 9, species 2 (conjugate class) (see Table, p. 367), the above equation is insoluble in integers.†

*To prove this. Let ξ, η, ζ be the system of variables, for which $\xi=1$, $\eta=1$ and x, y, z the system immediately preceding it. Then we have $A=2$, $\xi=1$, $\eta=1$, $\zeta=-1$, and either $x-y=0$, or $x+y=0$. The latter of these equations would imply $z=0$ and the former $x:y:z::1:1:-1$, and so continually until we fall back on the original equation in x, y, z. Hence the only possible resolution of 2, if $x+y$ is even, is into two equal cubes.

†$3A$ not containing any cube, ξ and $3A$ must be prime to each other, since otherwise η, ξ, ζ would have a common measure. Hence we may make $\eta=\xi\mu-3A\lambda$, and, consequently, $(\mu^3-3\mu+1)\xi^3\equiv 0 \mod 3A$, and, therefore, $\mu^3-3\mu+1$ must contain $3A$.

This conclusion would not hold if $3A$ were of the form A_1B^3 where A_1 contained no cube. We could then only infer $\mu^3-3\mu+1\equiv 0 \mod A_1$. Thus, in the case of $A=9$, $3A=B^3$, and our inference would become $\mu^3-3\mu+1\equiv 0 \mod 1$, which, of course, is satisfied, and, accordingly, 9 ought to be resoluble into two cubes, as it obviously is, viz: into 1 and 8. Thus, the equation $x^3-3xy^2+y^3=3Az^3$, when $A=9$ has an infinite number of solutions when $A=3$ has no solution, and when $A=1$ has just 3 solutions.

Case (2). Here, using L and M in the same sense as above, $\frac{x+y}{3} = L - M$ and $x-y = L+3M$ or $\xi_1^3 - 3\xi_1^2\eta_1 - 9\xi_1\eta_1^2 + 3\eta_1^3 = 3A\zeta^3$. Here writing $2\eta_1 = -\xi$, $\xi_1 = \eta + 2\xi$, the equation becomes $\eta^3 - 3\eta\xi^2 + \xi^3 = 3A\zeta^3$, and is insoluble in integers as before. Hence, since by hypothesis $x+y$ is not even, and it has been shown that it cannot be odd, *the number A when not unity is irresoluble into the sum or difference of two unequal rational cubes.**

When A is unity the equation above written becomes $\eta^3 - 3\eta\xi^2 + \xi^3 = 3\zeta^3$, the necessity for discussing what may be avoided by choosing the x, y out of x, y, z (which in this case are indistinguishable) so as to make $x+y$ always even, which is the ordinary and easier method; but it is not without interest to show how the desired conclusion may be arrived at by keeping $x+y$ always odd. This may be done as follows: The equation between ξ, η, ζ, on writing $\eta+\zeta = u$, $\zeta-\xi = v$, $-\eta+\xi+\zeta = w$† becomes $uv^2 + vw^2 + wu^2 = 0$ which, as shown in foot note to p. 383, involves the relations $u = y'^2z'$, $v = z'^2x'$, $w = x'^2y'$ and consequently $x'^3 + y'^3 + z'^3 = 0$ where $x'y'z' = \sqrt[3]{uvw}$.

Let us use in general two or more separate letters enclosed within a parenthesis to denote the absolute value of the *greatest one of them* (their *dominant* as I am wont to call it).

When $x+y$ does not contain 3, $x+y = \zeta^3$, $x^2 - xy + y^2 = (\xi_1^2 + 3\eta_1^2)^3$. Hence $\zeta < 2^{\frac{1}{3}}(x^{\frac{1}{3}}, y^{\frac{1}{3}})(\xi_1, \eta_1) < 3^{\frac{1}{3}}(x^{\frac{1}{3}}, y^{\frac{1}{3}})$. Therefore $(\xi_1, \eta_1, \zeta) < 3^{\frac{1}{3}}(x, y, z)^{\frac{1}{3}}$, and consequently since $\xi = \xi_1 + 3\eta_1$ and $\eta = -\xi_1 + 3\eta_1$, $(\xi, \eta, \zeta) < 4 \cdot 3^{\frac{1}{3}}(x, y, z)^{\frac{1}{3}}$ and therefore $(u, v, w) < 4 \cdot 3^{\frac{4}{3}}(x, y, z)^{\frac{1}{3}}$. Hence $x' \cdot y' \cdot z' < (u, v, w) < 4 \cdot 3^{\frac{4}{3}}(x, y, z)^{\frac{1}{3}}$.

In like manner when $x+y$ does contain 3, from the equations $\xi = -2\eta_1$, $\eta = \xi_1 - \eta_1$, $x+y = 9\zeta^3$, $x^2 - xy + y^2 = 3(\xi_1^2 + 3\eta_1^2)^3$, follow $\zeta < \left(\frac{1}{3}\right)^{\frac{2}{3}}(x, y)^{\frac{1}{3}}$ $(\xi_1, \eta_1) < (x, y)^{\frac{1}{3}}$, $(\xi_1, \eta_1, \zeta) < (x, y, z)^{\frac{1}{3}}$, $(\xi, \eta, \zeta) < (x, y, z)^{\frac{1}{3}}$, $x' \cdot y' \cdot z' < (u, v, w)$ $< 3(x, y, z)^{\frac{1}{3}}$.

In any case therefore $x' \cdot y' \cdot z' < 4 \cdot 3^{\frac{4}{3}}(x, y, z)^{\frac{1}{3}} < 18(x, y, z)^{\frac{1}{3}}$. But the difference between any two cubes except 8 and 1 being greater than 8, the

It may be worth noting that, in general, if $(x, y)^n = Az^n$, and $A = A_1 B^n$, where A_1 contains no nth power of a number $(x, 1)^n$ will contain A_1 as a divisor, provided that the coefficient of x^n in $(x, y)^n$ is prime to A_1. Cases of this inference being drawn of course frequently occur, but the general principle, obvious as it is, I do not recollect to have seen formulated in the text books. It may be made more precise by the statement that any factor of A_1 prime to the coefficient of x^n will be a divisor of $(x, 1)^n$.

* The equations of substitution are: for case 1, $\xi = \xi_1 + 3\eta_1$, $\eta = -\xi_1 + 3\eta_1$; and for case 2, $\xi = -2\eta_1$, $\eta = \xi_1 - \eta_1$.

† From these equations it is obvious that the dominant, *i. e.* the arithmetically greatest of the quantities u, v, w, is less than 3 times the dominant of ξ, η, ζ.

smallest of the numbers x', y', z' cannot be less than 3, and, since neither 3^3+4^3 nor 3^3+5^3 is a cube, it follows that $\frac{x'.y'.z'}{(x',y',z')}>18$, and therefore $(x', y', z') <(x, y, z)^{\frac{1}{3}}$, or the dominant of the quantities x, y, z which satisfy $x^3+y^3+z^3=0$ is continually replaced by another similar dominant less than the cube root of its predecessor, which is impossible.

Hence $x^3+y^3+z^3=0$ is insoluble. Let us see how this is reconcilable with the existence of the 3 rational solutions of $\eta^3-3\eta\xi^2+\xi^3=3A\zeta^2$, viz: $\xi, \eta, \zeta = \bar{1}, 1, 1$ or $2, 1, 1$ or $1, 2, \bar{1}$ respectively.

In case (1) $\xi=\xi_1+3\eta_1 \quad \eta=-\xi_1+3\eta_1$ $\xi, \eta = \bar{1}, 1$ gives $\eta_1=0$ $\xi, \eta = 2, 1$ gives $\eta_1=-\xi_1$ $\xi, \eta = 1, 2$ gives $\eta_1=\xi_1$. In each instance therefore $M=3\eta_1(\xi_1^2-\eta_1^2)=0$ and consequently $x+y=L=x-y$ and $y=0$.

In case (2) $\xi=-2\eta_1 \quad \eta=\xi_1-\eta_1$ $\xi, \eta = \bar{1}, 1$ gives $\xi_1=3\eta_1$ $\xi, \eta = 2, 1$ gives $\xi_1=-3\eta_1$ and $\xi, \eta = 1, 2$ gives $\xi_1=0$.

In each instance therefore $L=\xi_1(\xi_1^2-9\eta_1^2)=0$ and therefore $x=0$. Thus the rational solutions of the equation in ξ, η, ζ in both cases correspond to rational but futile solutions of the equation in x, y, z.

[To be continued.]