39.

ON CERTAIN TERNARY CUBIC-FORM EQUATIONS.

[*American Journal of Mathematics*, II. (1879), pp. 280—285, 357—393; III. (1880), pp. 58—88, 179—189.]

CHAPTER I. *On the Resolution of Numbers into the sums or differences of Two Cubes.*

SECTION 1.

M. LUCAS has written to inform me that in some one or more of a series of memoirs commencing with 1870, or elsewhere, the Reverend Father Pépin has made considerable additions to my published theorems * on the classes of numbers irresoluble into the *sum or difference* † of two rational cubes.

Using p, q to denote primes of the forms $18n+5$, $18n+11$, besides the 6 forms published by me, M. Pépin has found 10 other general classes of irresoluble numbers, the total number (as I understand from M. Lucas) known to the Reverend Father being as follows:

$$p,\quad q^2,\quad p^2,\quad q,\quad 2p,\quad 2q^2,\quad 4p^2,\quad 4q,$$
$$9p,\quad 9q^2,\quad 9p^2,\quad 9q,\quad 25p,\quad 25q^2,\quad 5p^2,\quad 5q,$$

but the last four of these classes are special cases only, of three out of the four more general irresoluble classes pq, p^2q^2, $p_1p_2^2$, $q_1q_2^2$, where p_1, p_2 are any two numbers of the p class and q_1, q_2 any two of the q class. On making $p=5$ in the first two of these, and $p_1=5$, $p_2=p$, or $p_2=5$, $p_1=p$, in the third, Father Pépin's last four classes result. It is also true that the numbers in my four additional general classes respectively multiplied by 9 are still irresoluble. Hence the number of known classes of numbers (depending on p and q) irresoluble into the sum or difference of cubes may be arranged as follows:

$$p,\quad q,\quad p^2,\quad q^2,\quad pq,\quad p^2q^2,\quad p_1p_2^2,\quad q_1q_2^2,$$
$$9p,\quad 9q,\quad 9p^2,\quad 9q^2,\quad 9pq,\quad 9p^2q^2,\quad 9p_1p_2^2,\quad 9q_1q_2^2,$$
$$2p,\quad 4q,\quad 4p^2,\quad 2q^2.$$

[* See Vol. I. of this Reprint, pp. 107—118, and Vol. II. pp. 63, 107.]

† It is well to understand that a number resoluble into the sum is necessarily also resoluble into the difference of two positive cubes and *vice versâ*.

Moreover, I have ascertained the truth of the following two theorems of a somewhat different character:

1st. Let ρ, ψ, ϕ denote prime numbers respectively of the forms $18n+1$, $18n+7$, $18n+13$ and suppose ρ, ψ, ϕ to be *not* of the form f^2+27g^2 and consequently *not* to possess the cubic residue 2, then I say that all the numbers comprised in any one of the eight classes

$$2\rho, \quad 4\rho, \quad 2\rho^2, \quad 4\rho^2, \quad 2\psi, \quad 4\psi^2, \quad 4\phi, \quad 2\phi^2$$

are irresoluble into the sum of two cubes *.

2nd. Provided 3 is not a cubic residue to ν† [where ν, any $6n+1$ prime, is the same as ρ, ϕ, ψ taken collectively], 3ν and $3\nu^2$ are similarly irresoluble.

With the aid of these theorems and certain special cases of irresolubility noticed by Father Pépin, communicated to me by M. Lucas, supplemented by calculations of M. Lucas and my own as regards the non-excluded numbers, it follows (*mirabile dictu*) that of the first 100 of the natural order of numbers, there is only a single one, namely, 66, of which it cannot at present be affirmed with certitude either that it is or is not resoluble into the sum of two cubes, and of which, in the former case, the resolution cannot be exhibited.

The proof of these statements, and the resolutions into cubes in their lowest terms, when they exist, will be given in the next number of the *Journal*. For the present I limit myself to noticing (what I much regret not to have done before the paper was printed) a statement of M. Lucas which is capable of being misunderstood and might give rise to an erroneous conception.

It is where this distinguished contributor to our *Journal* speaks of deriving from one rational point on a cubic curve (defined by a cubic equation with integer coefficients) another by means of its intersections with a

* The exclusion of 2 as a cubic residue blocks out the possibility of the "distribution of the amplitude"; the form p^2+27q^2 blocks out the possibility of a solution in which x^2-xy+y^2 has a common factor with the amplitude, and thereby imposes upon the equation containing x, y, z (were it soluble in integers) the necessity of repeating itself perpetually with smaller numbers, which of course is impossible. But the two conditions thus separately stated are in fact mutually implicative, every number of the form f^2+27g^2 having 2 for a cubic residue and *vice versâ* every number of the form $6n+1$ to which 2 is a cubic residue being of the form f^2+27g^2. The sole condition, therefore, in order that a number coming under any of the eight categories in the text shall be known at sight to be irresoluble into the sum of two cubes, is that its variable part shall not be of the form p^2+27q^2, that is, shall not be 31, 43, 91, 109, 127, 157, 223, 229, 247, etc.

† If I am not mistaken this is tantamount to the proviso that ν shall not be of the form $f^2 \pm 9fg+81g^2$. It is worth noticing that the above quantity multiplied by 3, say $3N$, is equal to $\frac{(9g \mp f)^3+(18g \pm f)^3}{27g}$, so that when g is a cube number N is immediately resoluble. The initial values of N will be found to be 61, 67, 73, 103, 151, 193, 271, 367, 547, etc., for each of which, up to 367 inclusive, $g=1$ or $g=-1$, so that their products by 3 are immediately resoluble.

conic drawn through five consecutive points situated at the given rational one; but, in fact, it follows from my theory of *residuation* that this point is collinear with the given point and its second tangential: just as a ninth point in which the cubic would be met by any other cubic passing through *eight* consecutive points situated at the given point would be the third tangential to the latter *.

Hence M. Lucas' third method amounts only to a combination of the other two; and in fact there is *but one single scale* of rational derivatives from any given point in a general cubic, the successive terms of which expressed in terms of the coordinates of the primitive are of the orders 1, 4, 16, 25, 49, ... the squares of the natural numbers with the multiples of 3 omitted †.

Scholium.

I term *lmn* the *amplitude* of the equation $lx^3 + my^3 + nz^3 = 0$, and if A cannot be broken up in any way into factors l, m, n, such that

$$lx^3 + my^3 + nz^3 = 0$$

shall be soluble in integers, I call the amplitude A of the equation

$$x^3 + y^3 + Az^3 = 0$$

undistributable.

When A is of the form $\dfrac{x^3 - 3x^2y + y^3}{3z^3}$, the equation $x^3 + y^3 + Az^3 = 0$ is always soluble, and when this equation is soluble, then, provided that its amplitude is undistributable and contains no prime factor of the form $6i + 1$, the equation $x^3 - 3x^2y + y^3 = 3Az^3$ must be soluble in integers, which cannot be the case when A contains any factor other than 3, or of the form $18i \pm 1$, inasmuch as *the cubic form* $x^3 - 3x \pm 1$ *contains no factors other than* 3 *or of the form* $18i \pm 1$.

* I make the important additional remark that at those special points of the cubic where this ninth point (sometimes elegantly called the subosculatrix) coincides with the point osculated, the scheme of rational derivatives returns upon itself, and instead of an infinite number there will be only two rational derivatives to such point. That is to say the infinite scheme becomes a system of 3 continually recurring points. The general theory of the special points which have only a finite number of rational derivatives will be given in the next number of the *Journal*.

† When the cubic is of the form $Ax^3 + Ay^3 + Cz^3 + Mxyz = 0$, where A, C, M are integers, then a rational point of inflection $x=1$, $y=-1$, $z=0$ is known and, in that case, from any other rational point *besides the ordinary ones* derivative rational points of the missing orders 9, 36, 81 can be found, but no others, and so universally if in the general cubic a rational point of inflection and a rational point (a, b, c) are given the scale of rational derivatives will be of the orders 1, 4, 9, 16, ... in a, b, c. This scale will of course be duplex, consisting of a series of points and a second series in which the radii drawn through the points of the first series and the point of inflection again meet the cubic.

This last theorem is a particular case of the following: If k be any integer and $F(x, y)$, the product of factors of the form $\left(x - 2\cos\frac{2\lambda\pi}{k}\, y\right)$, where λ is every number prime to k up to $\frac{1}{2}(k-1)$, then $Fx\ [= F(x, 1)]$ contains no prime factors excepting such as are contained in k or else are of the form $ki \pm 1$ *.

If it could be shown, in analogy with what holds for the quadratic forms Fx which result from making $k = 8, 10, 12$, that the cubic form $x^3 - 3xy^2 \pm y^3$ which results from making $k = 18$ may always be made to represent any prime number of the form $18n \pm 1$ itself, or else its treble (and for our purpose rational numbers would be as efficient as integers), we should then be able to affirm that any prime $18n \pm 1$ or else its nonuple could be resolved into the sum of two cubes. As a matter of fact I have ascertained that every prime number $18n \pm 1$ as far as 537 inclusive (and have no ground for supposing that the law fails at that point) can be represented by

$$x^3 - 3xy^2 \pm y^3$$

or else by its third part with *integer* values of x, y. Moreover, I find that the same thing is true of 17^2, 17.19, 19^2, 17.37, 19.37, 37^2, 17.53, 19.53, 37.53, that is, in fact for all the binary combinations of the natural progression of "r, ρ" numbers 17, 19, 37, 53, 71, 73, 89 (21 in all), as also 17^2, 19^2, 37^2 †. The number of *consecutive* r, ρ primes for which the law has been verified, that is, the number of those not exceeding 537 will be found to be 39, namely, 17, 19, 37, 53, 71, 73, 89, 107, 109, 127, 163, 179, 181, 197, 199, 233, 251, 269, 271, 307, 323, 341, 359, 361, 377, 379, 397, 413, 431, 433, 449, 451, 467, 469, 487, 503, 521, 523, 541, which according to the usual canons of induction would, I presume, be considered almost sufficient to establish the theorem for the case of $k = 9$.

* Thus, by making $k=8$ we learn that $x^2 - 2$ contains no factors except 2 and $8i \pm 1$ and by making $k=16$, that $y^4 - 4y^2 + 2$, none except 2 or $16i \pm 1$, by making $k=9$ that $x^3 - 3x + 1$, by making $k=18$, that $x^3 - 3x - 1$ contain no other factors but 3, or numbers of the form $18n \pm 1$. The theorem, I am aware, is well known for the case where k is a prime number and possibly is so for the general case. The proof of the irresolubility into two cubes of the 20 classes of numbers involving p's and q's, given at page [312], is an instantaneous consequence of the theorem for the case of $k=9$, for which case also there is no shadow of doubt of the theorem being true.

† 53^2 has not yet made its appearance. All the primes of that form themselves occurring in the first six hundred numbers have already occurred in my calculations except 557 and 593. I have worked with the formula $x^3 - 3xy^2 \pm y^3$ [x and y relative primes], giving to x and to y all the values possible from 1 to 36, and intend to extend the table to the limit of 50 or 100. The longer a moderate-sized number is in making its appearance, the longer it is likely to be before it appears, inasmuch as the large numbers of which it is the residuum or balance are becoming continually greater. It may very well then happen that the missing numbers alluded to may transcend all practicable limits of calculation to find them just as would be the case, for certain values of A, with finding values of x, y to satisfy the Pellian equation $x^2 - Ay^2 = 1$, were there not a theoretical method of arriving at them.

The table of "*special* cases" of irresoluble numbers found by Father Pépin (according to the information most kindly communicated to me by M. Lucas) comprises the numbers

14, 21, 31, 38, 39, 52, 57, 60, 67, 76, 77, 93, 95 *,

all of which I have verified as irresoluble except the number 60, which I accept as such on the erudite and sagacious Father's authority.

Reverting to F, it is hardly necessary to recall that $F(x^2+y^2, xy)$ is the primitive factor of x^k-y^k, and that it is capable of very easy demonstration that this primitive factor contains no prime factors except such as are divisors of k or of the form $ki+1$, the linear divisor $ki-1$ being here excluded. It seems to be very probable that for $k=9$, $F(x, y)$ or else $3F(x, y)$ does represent any prime of the form $18n \pm 1$, and consequently that every such form of prime or else 9 times the same is the sum of two rational cubes †.

This last conjectural theorem, it will be noticed, is not in any real analogy to the theorem that every product of primes of the form $4n+1$, and also the double thereof, is the sum of two *integer* squares; the real analogy is between the fact, of which this theorem is a consequence, that $x^3-3xy^2 \pm y^3$ or its third part represents every number which is a product of primes of the form $18n \pm 1$, and each one of the facts that x^2-2y^2, x^2-5y^2 represent all numbers of the form $8i \pm 1$, $10i \pm 1$ respectively, and that x^2-3y^2 or its third part represents all numbers of the form $12i \pm 1$. On account of its importance to this theory it seems desirable to give a name to the law which governs the prime factors of $F(x, y)$, and I take advantage of the circumstance that $F(x^2+y^2, xy)$ contains prime factors of the form $ki+1$, but not of the form $ki-1$, whilst $F(x, y)$ contains prime factors of either of these forms indifferently, to characterize it as the Law of Twin Prime Factors. Let us suppose the circumference of a circle divided by points into k equal parts, and agree to designate the shorter arc between any two of the points a *primitive* division of the circle in respect to k, provided that no number less than k would be adequate to give rise to an equal length of arc, so that $\frac{2\lambda\pi}{k}$, when λ is prime to k and less than $\frac{k}{2}$, will serve to represent any such division. The assumed Law of Twin Factors (well known, I repeat, for the case of k a prime number and possibly in its extended form likewise) may then be enunciated as follows :

* Of these numbers all except 60, 31, 67, 77, 95 belong to some one or other of the general classes of irresoluble numbers given in the text.

† It may be and probably is true also that $x^3-3xy^2 \pm y^3$ will represent the product or else three times the product of any two primes each of which is of the form r or ρ, and possibly the square or else three times the square of any r or ρ; it cannot possibly represent three times *any cube*, for if it did we should be able to infer that a cube was resoluble into two cubes, which we know is not true.

That function of x whose first coefficient is unity and whose roots are the doubled cosines of all the primitive divisions of the circle in respect to k contains no prime factors except such as are divisors of, or else when increased or diminished by unity, are divisible by k. This may be called again the *Exclusional or Negative Theorem of Twin Factors;* and on the other hand the more extraordinary theorem which asserts (on evidence not yet conclusive) that the function of x above defined, when made homogeneous in x, y, will represent (at all events for the case of $k = 9$) every prime number of the form $ki \pm 1$, or else certain specific multiples of any such number, may be called the *Inclusional or Representational Theorem of Twin Factors.*

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

Title 1. *Cyclotomic Functions of the* 1*st 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 function 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 (that is, 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 $fa + \lambda f'a \,.\, p + Rp^2 \equiv 0 \mod p^2$. Hence $fa \equiv 0$ and $f'a \equiv 0 \mod p$, 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 $f'a$, that is, 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 ω, $\frac{1}{2}\omega(\omega - 1)$, ... and the factor ω to be struck out from each of the two equations $\dfrac{df(x, 1)}{dx} = 0$, $\dfrac{df(x, 1)}{d1} = 0$).

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

expresses the universal relation between the arithmetical discriminant and the squared product of the root-difference of a function. If we had been

* 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.

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

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

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

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

we may obtain the equation $\lambda xfx + \mu xgx = Rx^q$ (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

* Thus, for example, 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.

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 $fx \equiv 0 \mod p$ 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 $R \equiv 0 \mod p$ (that is, if R contains p) then gx must have at least one real root in common with fx *quâ* modulus p.

From the congruence of $fx \equiv 0 \mod p$ 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 $ga_1 . ga_2 . ga_3 \ldots ga_i \equiv 0 \mod p$, and, as all the factors on the left hand side of the equation are real, one of them must contain p. Hence, if $R(fx, gx) \equiv 0 \mod p$, and $fx \equiv 0 \mod p$ *has all its roots real*, one of these roots must belong also to the congruence $gx \equiv 0 \mod p$.

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 product.

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 $\omega^{\omega-2} . \omega_1{}^{\omega_1-2} \Delta Fx = (\omega + \omega_1)^{\omega+\omega_1-2} \Delta fx . \Delta f_1x (R(fx, f_1x))^2$.

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 $x^{p-1} - 1$, that is, 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 (that is, more real roots than there are units in its degree) in respect to the modulus p^j.

* 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.

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

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

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

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 $y_2{}^{p^{j-1}} - y_1{}^{p^{j-1}} \equiv 0 \text{ mod. } p^j$. 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

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

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

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, that is, will be a divisor thereof corresponding to ω distinct values of the variable of the function, that is, values incongruent with one another *quâ* the modulus p^j.

* 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.

The divisors of the cyclotomic function to index h may be divided into two classes, namely, 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, that is, 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, that is, $= \left(\frac{k}{\delta}\right)^\delta$ 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 $k = a^\alpha . b^\beta . c^\gamma . d^\delta . e^\epsilon$. Then the totient of k is

$$a^{\alpha-1} . b^{\beta-1} . c^{\gamma-1} . d^{\delta-1} . e^{\epsilon-1} \begin{Bmatrix} \alpha\beta\gamma\delta\epsilon + \Sigma\alpha\beta\gamma + \Sigma\alpha \\ -\Sigma\alpha\beta\gamma\delta - \Sigma\alpha\beta - 1 \end{Bmatrix},$$

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

(2) When $i=1$ and $k=a^\alpha$, the value of $\chi_k x = \dfrac{x^{a^\alpha}-1}{x^{a^{\alpha-1}}-1}$, 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 $k=k_1p^j$ 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 $\chi_k x = \dfrac{x^{p^j}-1}{x^{p^{j-1}}-1} = 1+x^{p^{j-1}}+x^{2p^{j-1}}+\ldots+x^{(p-1)p^{j-1}}$, which, (to modulus p) $\equiv 1+x+x^2+\ldots+x^{p-1} \equiv \dfrac{x^p-1}{x-1}$, 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, $k=k_1p$, $k_1=abc$, $p=mk_1+1$; 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.

* 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, namely, $x+1$ will obviously contain every power of 2 as a divisor.

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 $p^{\tau(k_1)}$ ($\tau(k_1)$ 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

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

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].

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

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

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 $\frac{x^{ap}-1}{x^a-1} = \frac{(1+Rp)x^a-1}{x^a-1} = 1+R_1p$ 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 $\tau(k_1)$-fold divisor of the cyclotomic function.

When k is the index to a cyclotomic function, and $k = k_1p^j$, 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,

* 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*.

or, in other words, all the distinct values, $\frac{1}{2}\tau(k)$ in number, of $2\cos\frac{2\lambda\pi}{k}$ where λ is any number less than $\frac{1}{2}k$ 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.

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	2nd 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

Index	1st Species	2nd Species, Conjugate Class
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	$x^{20}+x^{15}+x^{10}+x^5+1$	$u^{10}-10u^8+35u^6+u^5-50u^4-5u^3+25u^2-5u-1$
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	$x^{28}+x^{27}+\ldots+x+1$	$u^{14}+u^{13}-13u^{12}-12u^{11}+66u^{10}+55u^9-165u^8$ $-120u^7+210u^6+126u^5-126u^4-56u^3+28u^2$ $+7u-1$
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 neighbouring 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

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

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.

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 $\dfrac{\sin\frac{p\theta}{2}}{\sin\frac{\theta}{2}}$, 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 $\dfrac{1}{a_1 - \dfrac{1}{a_2 - \ldots \dfrac{1}{a_n}}}$, say the procumulant $[a_1, a_2, \ldots a_n] = A_0 - A_1 + A_2$ etc., where A_0 is $a_1 . a_2 \ldots . a_n$, 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 $D_0 n = 1$, $D_1 n = n-1$, $D_2 n = (n-2)\dfrac{n-3}{2}$, $D_3 n = \dfrac{(n-3)(n-4)(n-5)}{1.2.3}$, 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 $\dfrac{\sin(n+1)\theta}{\sin\theta}$, 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 $2\cos n\theta = 2\left(\dfrac{\sin(n+1)\theta}{\sin\theta} - \cos\theta\dfrac{\sin n\theta}{\sin\theta}\right) = (2\cos\theta)^n - n(2\cos\theta)^{n-2}$

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

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

* 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 $8m+3$.

† This expansion Gauss (*Rech. Arith.*, Paris, 1757, p. 431) suggests deriving by means of the

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 2nd 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 $\cos\theta = 0, 1, 2, 3, \ldots (p-1)$, p being supposed to be a prime number.

But more generally the congruence $\cos p^j\theta - \cos p^{j-1}\theta \equiv 0 \pmod{p^j}$ 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 $x^{p^j} - x^{p^{j-1}} \equiv 0 \pmod{p^j}$ 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

---

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.*

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

$$(\cos\theta)^{p^2} - (\cos\theta)^p$$

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

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

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

.....

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

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

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

(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 3rd pair of terms *quâ* p^2

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

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 $\cos p\theta - \cos\theta \equiv 0$ 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,

* 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, $j-1$, ... 2, 1, 0 respectively is $p^j - p^{j-1}$, $p^{j-1} - p^{j-2}$, ... $p^2 - p$, $p - 1$, 2.

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,

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

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

$$\cos p^{j-1}\phi_2 - \cos p^{j-1}\phi_1 \equiv 0 \text{ mod. } p^j.$$

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 $p\,.\,q$, that is, 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, that is, as many roots as there are units in its degree.

If then $p = mk + \epsilon$, where $\epsilon = \pm 1$, 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 $\frac{1}{2}\tau(k)$-fold divisor of such function.

As in the case of cyclotomics of the 1st species we may separate the divisors of those of the 2nd 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 2nd species of cyclotomics to the index k.

To show this I proceed as follows: $\psi_k u$ is contained algebraically in $\dfrac{\sin \frac{k}{2}\theta}{\sin \frac{\theta}{2}}$, and *à fortiori* in its square, that is, in $\dfrac{1-\cos k\theta}{1-\cos\theta}$, 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 $\dfrac{\sin p\theta}{\sin\theta} \equiv a + bp$,

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

and $(1-a^2)(1-\cos\theta)^2 = cp$, and, therefore, $a = \pm 1$ mod. p, for $\dfrac{1-\cos k\theta}{1-\cos\theta}$ 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, $\dfrac{1-\cos k\theta}{1-(\cos\theta)^2}$, does not contain either $1-\cos\theta$ or $1+\cos\theta$, and, therefore, $\psi_k u$, which, in that case, is contained in $\dfrac{1-\cos k\theta}{1-(\cos\theta)^2}$, 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, $\dfrac{\sin p\theta}{\sin\theta} \equiv \pm 1$ mod. p.

Hence, either

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

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

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

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

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

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

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 $\dfrac{\cos k\theta - 1}{\cos \delta\theta - 1}$ *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 $\dfrac{\cos k\theta - 1}{\cos \delta\theta - 1}$ for every root of $\cos \delta\theta - 1$, it is therefore the δth power of the value of the vanishing fraction $\dfrac{\cos \mu\phi - 1}{\cos \phi - 1}$ $\left[\text{where } \mu = \dfrac{k}{\delta}\right]$ when $\cos \phi = 1$, that is, of $\left(\dfrac{\sin \frac{\mu}{2}\phi}{\sin \frac{\phi}{2}}\right)^2$ when $\phi = 0$. The resultant is, therefore, $\left(\dfrac{k}{\delta}\right)^{2\delta}$, which cannot contain p, since, by hypothesis, p is not contained in k. Hence $p - \epsilon = mk$, 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 $\psi_k 2$, that is, 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, $(\psi_k u)^2 = \dfrac{\cos p^j\theta - 1}{\cos p^{j-1}\theta - 1}$, which is of the form $\dfrac{\cos \theta - 1 + Lp}{\cos \theta - 1 + lp}$, 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 $\dfrac{\cos pk_1\theta - 1}{\cos k_1\theta - 1} = p$, 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 satisfy 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 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.

* 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.

To find a value of x which makes $\psi_{15}x$ 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. [327] 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†.

I have accordingly calculated cyclotomic functions for the cases following:

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

* 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.

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

„ „ for $\mu = 3$, $\nu = 4$

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

„ to 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,

$$\tau_{1,1},\ \tau_{1,2} \cdots \tau_{1,\nu}$$
$$\tau_{2,1},\ \tau_{2,2} \cdots \tau_{2,\nu}$$
$$\cdots\cdots\cdots\cdots$$
$$\tau_{\mu,1},\ \tau_{\mu,2} \cdots \tau_{\mu,\nu}$$

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 $\mu = \dfrac{\tau(k)}{\nu}$.

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	$x^5-x^4-4x^3+3x^2+3x-1$*	±1, ±10
„	5	$x^4-x^3-2x^2-3x+9$	1, -2, 4, -8, 16
„	10	x^2-x-8	±1, ±2, ±4, ±8, ±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 (that is, primes dividing the function but not its index) are of the form $mk+\theta_1, \theta_2, \ldots \theta_\nu$.

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

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 1*st 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 $\chi_{k_1} x \equiv 0$ mod. p and does not contain p^2. If, then, we make j successively 0, 1, 2 ... $j-1$ it will follow that

$$\chi_{k_1},\ \chi_{k_1 p},\ \chi_{k_1 p^2},\ \cdots\ \chi_{k_1 p^{j-1}}$$

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 contain p^j, so that $x^{\frac{\tau p^j}{m}} - 1 \equiv 0$ mod. 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 footnote 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, for example, 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 2nd footnote to page [316] 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, namely,

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

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 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 three 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),

$$\frac{\cos\omega}{\cos 2\omega}, \frac{\cos 2\omega}{\cos 4\omega}, \frac{\cos 4\omega}{\cos\omega},$$
$$\frac{\cos 2\omega}{\cos 4\omega}, \frac{\cos 4\omega}{\cos\omega}, \frac{\cos\omega}{\cos 2\omega},$$
$$\frac{\cos 4\omega}{\cos\omega}, \frac{\cos\omega}{\cos 2\omega}, \frac{\cos 2\omega}{\cos\omega}.$$

* 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.

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

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 determine the number of such polygons for any existent number of sides. Since $wv^2 + vu^2 + uw^2 = 0$ 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 3rd 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 3rd tangential, and I draw a ray meeting the curve in P', and through P' and Q, the tangential to P, [that is, 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 versâ*, if the condition is fulfilled, P is its own 3rd tangential.

* 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, $p^{2\beta}$, 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 $\delta^3u'^2v' + \epsilon^3v'^2w' + \theta^3w'^2u' = 0$, 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 $\delta_1^3 + \epsilon_1^3 + \theta_1^3 = 0$, 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.

It will be found that

$$X: -x^6y^3 - y^6z^3 - z^6x^3 + 3x^3y^3z^3$$
$$:: Y: -x^3y^6 - y^3z^6 - z^3x^6 + 3x^3y^3z^3$$
$$:: Z: \quad xyz\,(x^6 + y^6 + z^6 - x^3y^3 - y^3z^3 - z^3x^3),$$

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 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 $3 \times (9 + 9 + 6)$, that is 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

* 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, namely, $ab'c'' = bc'a'' = ca'b''$, 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 3rd 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

$$\begin{array}{ccc} & PP = Q & \\ IP = JQ & JP = KQ & KP = IQ \\ I'P = J'Q & J'P = K'Q & K'P = I'Q \\ I''P = J''Q & J''P = K''Q & K''P = I''Q. \end{array}$$

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.

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, representing 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.

* When the cubic is $x^3+y^3+z^3$, X, Y, Z become $x^9+6x^6y^3+3x^3y^6-y^9$, ..., $xyz(x^6+x^3y^3+y^6)$ $X=0$ then gives $\frac{x^3}{y^3}=t-t^2$ if $t^3-3t+1=0$, that is, $t=2\cos\frac{2\pi}{9}$, $2\cos\frac{4\pi}{9}$, $2\cos\frac{8\pi}{9}$; calling the three values of $\frac{x^3}{y^3}$ thus obtained τ_1, τ_2, τ_4, one of the two real in- and- exscribed triangles will have at its vertices $\frac{x}{y}, \frac{y}{z}, \frac{z}{x}=\tau_1^{\frac{1}{3}}, \tau_2^{\frac{1}{3}}, \tau_4^{\frac{1}{3}}=\tau_2^{\frac{1}{3}}, \tau_4^{\frac{1}{3}}, \tau_1^{\frac{1}{3}}=\tau_4^{\frac{1}{3}}, \tau_1^{\frac{1}{3}}, \tau_2^{\frac{1}{3}}$ 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.

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

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

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 $\chi_k x$ 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 $2 \cdot 4^{i-1}+1$; the number of points on the cubic (exclusive of inflexions) satisfying this condition is $3(2 \cdot 4^{i-1}+1)-27 = 24(4^{i-2}-1)$. 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; that is, 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 out 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 $x^3 + x^2 - \frac{k-1}{2}x - \frac{3k-1+\epsilon mk}{27}$, where $\epsilon^2 = \pm 1$ and $m - \epsilon$ 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

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

Hence, when $\theta=1$, that is 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

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

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 $\mathfrak{Y}$ the number of solutions of the congruence $1+3\beta\equiv 0 \pmod{k}$, that is 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 $\mathfrak{Y}$ 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 $(n^2-1)+\epsilon\left\{\left(\frac{m-\epsilon}{3}\right)^3-\frac{m-\epsilon}{3}\right\}$, and consequently is divisible or not by 81 according as n is not, or is, divisible by 3. Hence $\mathfrak{Y}=1$ 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.

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 $U+\frac{3\theta}{2}=\frac{3k-1+\epsilon mk}{18}$ contains a complete solution of the interesting question, "How many times, if the cubic residues to a given

* 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.

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

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, $\alpha, n-\beta$ and $\beta, n-\alpha$, differing by units. But when 2 is a cubic residue, there will be three extra sequences not contained among the $2U$ just spoken of, namely,

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

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

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

$$\begin{array}{cccc} p, & q, & p^2, & q^2, \\ 9p, & 9q, & 9p^2, & 9q^2, \\ 2p, & 4q, & 4p^2, & 2q^2, \\ pq, & p_1p_2^2, & q_1q_2^2, & p^2q^2, \end{array}$$

(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.

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.

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

* 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.

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 $\bar{1}$, 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

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

and

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

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. [327]), the above equation is insoluble in integers†.

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 which 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

* 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, $(\mu^3-3\mu+1)\xi^3\equiv0$ 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 $\mu^3-3\mu+1\equiv0$ mod. A_1. Thus, in the case of $A=9$, $3A=B^3$, and our inference would become $\mu^3-3\mu+1\equiv0$ mod. 1, which, of course, is satisfied, and, accordingly, 9 ought to be resoluble into two cubes, as it obviously is, namely, 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.

It may be worth noting that, in general, if $(x, y)^n=Az^n$, and $A=A_1B^n$, 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 a 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, $\xi=-2\eta_1$, $\eta=\xi_1-\eta_1$.

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 footnote to p. [341], 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 $\eta=-\xi_1+3\eta_1$, $(\xi, \eta, \zeta)<4.3^{\frac{1}{3}}(x, y, z)^{\frac{1}{3}}$ and therefore $(u, v, w)<4.3^{\frac{4}{3}}(x, y, z)^{\frac{1}{3}}$. Hence $x'.y'.z'<(u, v, w)<4.3^{\frac{4}{3}}(x, y, z)^{\frac{1}{3}}$.

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 $\zeta<\left(\frac{1}{3}\right)^{\frac{3}{3}}(x, y)^{\frac{1}{3}}$ $(\xi_1, \eta_1)<(x, y)^{\frac{1}{3}}$, $(\xi_1, \eta_1, \zeta)<(x, y, z)^{\frac{1}{3}}$, $(\xi, \eta, \zeta)<(x, y, z)^{\frac{1}{3}}$, $x'.y'.z'<(u, v, w)<3(x, y, z)^{\frac{1}{3}}$.

In any case therefore $x'.y'.z'<4.3^{\frac{4}{3}}(x, y, z)^{\frac{1}{3}}<18(x, y, z)^{\frac{1}{3}}$. But the difference between any two cubes except 8 and 1 being greater than 8, the 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 $\eta^3-3\eta\xi^2+\xi^3+3\zeta^3=0$, namely, $\xi, \eta, \zeta=\bar{1}, 1, 1$ or $2, 1, 1$ or $1, 2, \bar{1}$ respectively.

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

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

CHAPTER I.

Excursus B.—On the Chain Rule of Cubic Rational Derivation.

I think it desirable, while the colours, so to say, are still wet on the palette, and my mind is still dwelling upon the subject which has been casually introduced in the note to the proem contained in the last number of the *Journal* (and there made use of to determine the number of in-and-exscribed k-laterals to a cubic), without waiting to put forth the titles which in natural order of sequence, perhaps, should immediately follow Title 1 of Section 2, to proceed at once to develop the theory of derivation which, irrespective of the casual use of it alluded to, will be found to be of essential importance when I reach that part of my proposed task which deals with soluble cubic-form equations, nor less so when, in Chapter II., I have to treat of insoluble cases of certain classes of cubic-form equations with four or more terms.

Title 1.—*On the Natural or Discontinuously Numbered Scale of Rational Derivatives to a Point on a Cubic Curve.*

Let us take any point on a cubic curve along with its successive tangentials *ad infinitum*. We may, by drawing straight lines through any two of these points, either contiguous or apart, to meet the curve, obtain an additional set of points, and thus form an enlarged system which may again be subjected to a like process of collineation or tangentialization, and such method of augmentation and amplification may be continued indefinitely. Every point thus obtained will obviously be a rational derivative of the original point (that is, its co-ordinates will be rational integral functions of those of that point), and, at first sight, it would seem as if we might in this way obtain a network, or spread*, of rational derivatives; but I shall proceed to show that such is not the case, but that only a line or chain of points will be thus obtained, usually infinite in extent, although for certain positions of the initial point coming to a stop, and in other cases winding round and round upon itself so as still to include only a finite number of distinct points. It will be shown subsequently that, in order to complete the theory of the chain for the purposes of this memoir, it will be necessary to take into account the rational derivatives not merely from a single arbitrary point, but from such points, *combined with a point of inflexion*, and that this additional element will not alter the surprising fact of the absence of reticulation or spread, but merely bring about the insertion into the chain of

* Spread, as a noun (scarcely to be found in the dictionaries), I employ in the sense in which it occurs in the phrase *spread of foliage*. On this continent the word *spread* is also used to denote a thick coverlet or padded woollen quilt, laid over the bedclothes in winter to keep out the cold; also on both continents as a familiar name for a college banquet.

points corresponding to missing numbers in it as first described, and to the duplication of the chain so completed, owing to every point in it having an opposite point also situated on the curve and collinear with it in respect to the given inflexion. This duplication will be of little importance in general to the arithmetical theory with which we shall be occupied, inasmuch as opposite points will correspond to the same arithmetical values, with merely a change of name between two out of the three variables which denote the co-ordinates of any point. First, let us consider the chain law of derivation when a point on the cubic curve alone is given. I shall call the original point 1, and its first and second tangentials 2 and 4 respectively, and in general use (m, n) to denote the point on a given cubic collinear with two points m, n also situated upon it*. Obviously, then, we shall have $(1, 1) = 2$ $(2, 2) = 4$, using $(1, 1)$ $(2, 2)$ to denote, in either case, two consecutive points upon the cubic. It is also obvious that if $(m, n) = p$ then $(m, p) = n$ and $(n, p) = m$, so that $(1, 2) = 1$ $(2, 4) = 2$.

Let us call $(1, 4) = 5$ $(2, 5) = 7$ $(1, 7) = 8$ $(2, 8) = 10$ $(1, 10) = 11$ $(2, 11) = 13$ and so on. It will be seen that no number which is a multiple of 3 is brought into existence by this process. Supposing a, b to be any two integers, neither of them divisible by 3, let us agree to signify by $a \ddagger b$ that of the two values $a + b$, $a - b$ which is not divisible by 3. The theorem to be established is that the point (m, n) collinear to m and n will have for its value $m \ddagger n$; as, for instance, (4, 4), or the third tangential to 1, will have for its value 8, that is, will be identical with (1, 7), that is to say, with $\{1, [2, (1, 4)]\}$, where 2 and 4 are the first and second tangentials to 1, which amounts to a rule for obtaining the third tangential, when a point on a cubic and its first and second tangentials are given, by collineation alone. The *theory of residuation*, in its simplest form (see Salmon's *Higher Plane Curves*, 3rd ed., p. 134)† teaches us that the rule of the older chemistry known by the name of double decomposition, namely that $\{(a, b), (c, d)\} = \{(a, c), (b, d)\}$ is applicable to the same symbols regarded as points on a cubic curve. This rule of double decomposition is all that is required to prove the theorem in question.

Thus, for example, in order to prove that $(1, 7) = (4, 4)$, I write $(1, 7) = \{(1, 2), (2, 5)\} = \{(2, 2), (1, 5)\} = (4, 4)$. Q. E. D.

So, to prove in general that $(r, s) = r \ddagger s$ I proceed as follows:

* Sometimes, however, it will be found more convenient to use $P_1, P_2 \ldots P_n$; $P_1', P_2', \ldots P_n'$ in lieu of 1, 2, ... n; 1′, 2′, ... n'.

† The theory of residuation was originally brought by me before the Mathematical Society of London, and subsequently, in the form of questions, in the *Educational Times*. Dr Salmon makes no allusion to the fact of my applying the theory to curves of all orders: in the case of the quartic, the residual becomes a system of three points; of a quintic, a system of six points, and so on. I understood Professor H. S. Smith to say that he made use of my theory for the quartic in his memoir which gained half the prize for the subject set by the Academy of Sciences of Berlin, but which I have never seen.

(1) Suppose $r = 3i + 1$; $s = 3j + 1$, where $j - i$ is positive. Then

$$(r, s) = \{(3i - 1, 2), (3j + 2, 1)\} = \{(3i - 1, 1), (3j + 2, 2)\}$$
$$= (3i - 2, 3j + 4) = (r - 3, s + 3).$$

Hence $(r, s) = (r - 3i, s + 3i) = (1, s + r - 1) = s + r$.

(2) Suppose $r = 3i - 1$; $s = 3j - 1$. Then $(r, s) = \{(3i - 2, 1), (3j + 1, 2)\}$
$= \{(3i - 2, 2), (3j + 1, 1)\} = (3i - 4, 3j + 2) = (r - 3, s + 3)$,

as before. Hence $(r, s) = \{r - 3(i - 1), s + 3(i - 1)\} = (2, s + r - 2) = s + r$.

(3) Suppose $r = 3i - 1$; $s = 3j + 1$. Then $(r, s) = \{(3i - 2, 1), (3j - 1, 2)\}$
$= \{(3i - 2, 2), (3j - 1, 1)\} = (3i - 4, 3j - 2) = (r - 3, s - 3)$.

Hence $(r, s) = (r - 3i + 3, s - 3i + 3) = (2, s - r + 2) = s - r$.

(4) Suppose $r = 3i + 1$; $s = 3j - 1$. Then $(r, s) = \{(3i - 1, 2), (3j - 2, 1)\}$
$= \{(3i - 1, 1), (3j - 2, 2)\} = (3i - 2, 3j - 4) = (r - 3, s - 3)$.

Hence $(r, s) = (r - 3i, s - 3i) = (1, s - r + 1) = s - r$.

Collecting the four cases, it will be seen that I have proved, for all values of the points r, s in the chain, that $(r, s) = r \ddagger s$. Q.E.D.

The points 2^i correspond to tangentials of the ith order to the point 1. It is obvious from the above theorem that no process of continued collineation or tangentialization performed upon these points can lead to any points extraneous to the series of points 1, 2, 4, 5, 7, 8 ... which form a simple chain extending in general to infinity. Moreover, as it follows from the theory of residuation that any single point reached through the intervention of curves drawn through any number of points on a cubic can be reached by simple linear constructions, it follows that by no conceivable geometrical process can any rational point be reached not included in the numbered chain, and the inference becomes in the highest degree probable, and, as a matter of fact, is undoubtedly true (although the reasoning upon which it is here made to rest is not absolutely conclusive), that no rational deducts from a *general* point on a *general* cubic exist save those that belong to the numbered chain, the points upon which constitute what may properly be termed a self-contained *group*, infinite or finite (as the case may be) in regard to the number of terms which it contains. I shall presently determine the order of each successive derivative, meaning thereby the order in the co-ordinates of the initial point of any one of the three functions which express the co-ordinates of the derived one*.

* There is a further question, but which, as not material to the object of this memoir, I shall not discuss here, namely, the *degree* in the coefficients of each such derivative. For the tangential, the degree-order (being that of the minor determinants of the matrix made up of the differential derivatives of the function and its Hessian) we know to be 4, 4. If x, y, z, be the original co-ordinates, and X, Y, Z, those of the tangential, we know that $F(X, Y, Z)$ being zero when $F(x, y, z)$ (the given cubic) is zero, must be divisible by $F(x, y, z)$. The quotient will be of the degree-order 13, 12 – 1, 3, that is, 12, 9, and is in fact the skew covariant of F.

The case in which the chain forms a closed polygon, which can only happen when for some number i the ith tangential coincides with the initial point, has already been discussed in the note to the proem.

If the chain is an open but finite one, it is necessary that a tangential of some order shall fall upon a point of inflexion, in which case the succeeding tangentials remain fixed at that point, but otherwise continual new tangentials could be drawn. These are obviously necessary conditions of the chain being finite, whether it be an open chain or winding round upon itself; it remains to show that they are sufficient as well as necessary, but that will best appear after the theory of derivation from a general point combined with a point of inflexion has been discussed.

I shall begin with finding the co-ordinates X, Y, Z of a point on the cubic curve collinear with any two given points x, y, z; ξ, η, ζ. Let

$$X = \lambda x + \mu\xi,\ Y = \lambda y + \mu\eta,\ Z = \lambda z + \mu\zeta;$$

then

$$F(X, Y, Z) = \lambda^3 F(x, y, z) + \lambda^2\mu\left(\xi\frac{d}{dx} + \eta\frac{d}{dy} + \zeta\frac{d}{dz}\right)F(x, y, z)$$

$$+ \mu^3 F(\xi, \eta, \zeta) + \lambda\mu^2\left(x\frac{d}{d\xi} + y\frac{d}{d\eta} + z\frac{d}{d\zeta}\right)F(\xi, \eta, \zeta).$$

Hence X, Y, Z will be the collineal to (x, y, z), (ξ, η, ζ) if

$$\lambda : \bar{\mu} :: \left(x\frac{d}{d\xi} + y\frac{d}{d\eta} + z\frac{d}{d\zeta}\right)F(\xi, \eta, \zeta) : \left(\xi\frac{d}{dx} + \eta\frac{d}{dy} + \zeta\frac{d}{dz}\right)F(x, y, z).$$

If now we write $F(x, y, z)$ under its canonical form $x^3 + y^3 + z^3 + Kxyz$, it will be found, on substituting for λ and $\bar{\mu}$ the quantities to which they are proportional, that

$$X = (y^2\eta\xi - y\eta^2 x + z^2\zeta\xi - z\zeta^2 x) + K(yz\xi^2 - \eta\zeta x^2)$$
$$Y = (z^2\zeta\eta - z\zeta^2 y + x^2\xi\eta - x\xi^2 y) + K(zx\eta^2 - \zeta\xi y^2)$$
$$Z = (x^2\xi\zeta - x\xi^2 z + y^2\eta\zeta - y\eta^2 z) + K(xy\zeta^2 - \xi\eta z^2).$$

But these expressions admit of a surprising simplification, namely, we may neglect the terms not containing K, for it will be found that the quantities affected with the coefficient K are to each other in the same ratios as the other three corresponding groups in the values of X, Y, Z. Thus, for example

$$(yz\xi^2 - \eta\zeta x^2)(z^2\zeta\eta - z\zeta^2 y + x^2\xi\eta - x\xi^2 y)$$
$$-(zx\eta^2 - \zeta\xi y^2)(y^2\eta\xi - y\eta^2 x + z^2\zeta\xi - z\zeta^2 x)$$
$$= (\xi y - x\eta)\{\xi\eta\zeta(x^3 + y^3 + z^3) - xyz(\xi^3 + \eta^3 + \zeta^3)\}$$

hence $$X : Y : Z :: yz\xi^2 - \eta\zeta x^2 : zx\eta^2 - \zeta\xi y^2 : xy\zeta^2 - \xi\eta z^2.$$

We might, instead of these simple expressions, take for X, Y, Z the other three groups and (using $x_1y_1z_1$; $x_2y_2z_2$ instead of x, y, z; ξ, η, ζ and (pq) to

denote the determinant $p_1q_2 - p_2q_1$) say that X, Y, Z are the minor determinants of

$$\begin{matrix} x_1 \,.\, x_2 & y_1 \,.\, y_2 & z_1 \,.\, z_2 \\ (yz) & (zx) & (xy), \end{matrix}$$

and these are actually the expressions found by Cauchy, and given by him in his *Exercices de Mathématiques*, Paris, 1826, p. 256, ll. 18—21, pp. 257—60. I take this reference from a loose page of an article by M. Lucas, but have not access either to that article or to Cauchy's.

It is remarkable that Cauchy should have given quadrinomial expressions for the collineal to two given points on a cubic curve, or their connective, as I shall hereafter term it, when, as shown above, binomial ones fulfil the same purpose. The correctness of these remarkable formulæ admits of easy verification, as follows:

For greater simplicity denote x^3, y^3, z^3, xyz by u, v, w, μ; and $\xi^3, \eta^3, \zeta^3, \xi\eta\zeta$ by u', v', w', μ' respectively. Then

$$\begin{aligned} \Sigma\,(yz\xi^2 - \eta\zeta x^2)^3 &= \Sigma\,(vwu'^2 - v'w'u^2) - 3\mu\mu'\,\{(u'+v'+w')\,\mu - (u+v+w)\,\mu'\} \\ &= \Sigma\,(vwu'^2 - v'w'u^2). \end{aligned}$$

Also
$$\begin{aligned} &K\,(yz\xi^2 - \eta\zeta x^2)\,(zx\eta^2 - \zeta\xi y^2)\,(xy\zeta^2 - \xi\eta z^2) \\ &= -Kxyz\,(\xi^3\eta^3z^3 + \eta^3\zeta^3x^3 + \zeta^3\xi^3y^3) + K\xi\eta\zeta\,(x^3y^3\zeta^3 + y^3z^3\xi^3 + z^3x^3\eta^3) \\ &= (u+v+w)\,(uv'w' + vw'u' + wu'v') - (u'+v'+w')\,(u'vw + v'wu + w'uv) \\ &= \Sigma\,(u^2v'w' - u'^2vw). \end{aligned}$$

Hence, giving X, Y, Z the values indicated by the formula, we find

$$X^3 + Y^3 + Z^3 + KXYZ = 0,$$

which equation depends, as seen, and as we know *a priori* must be the case, on the pure algebraical fact that $X^3 + Y^3 + Z^3 + KXYZ$ is a syzygetic function of $x^3 + y^3 + z^3 + Kxyz$ and $\xi^3 + \eta^3 + \zeta^3 + K\xi\eta\zeta$, taking no account of the function $\xi\eta\zeta\,(x^3 + y^3 + z^3) - xyz\,(\xi^3 + \eta^3 + \zeta^3)$, as that is itself a syzygetic function of the two others. If we call the syzygetic multipliers of those two Φ and F respectively, it will at once be seen from what precedes that

$$\Phi = 3\xi^2\eta^2\zeta^2xyz - \xi^3\eta^3z^3 - \eta^3\zeta^3x^3 - \zeta^3\xi^3y^3$$

$$F = 3x^3y^3z^3\xi\eta\zeta - x^3y^3\zeta^3 - y^3z^3\xi^3 - z^3x^3\eta^3\ *.$$

I now proceed to apply the foregoing results to the problem of determining the order in the co-ordinates of any derivative numbered j (where $j = 3i \pm 1$),

* Thus
$$F = -(yz\xi + zx\eta + xy\zeta)\,(yz\xi + \rho zx\eta + \rho^2xy\zeta)\,(yz\xi + \rho^2zx\eta + \rho xy\zeta)$$
$$\Phi = -(\eta\zeta x + \zeta\xi y + \xi\eta z)\,(\eta\zeta x + \rho\zeta\xi y + \rho^2\xi\eta z)\,(\eta\zeta x + \rho^2\zeta\xi y + \rho\xi\eta z),$$
and it is worthy of notice that we have incidentally solved with quantic values for F, Φ, U, V, W the simultaneous algebraico-diophantine equations
$$U^3 + V^3 + W^3 = (a^3 + b^3 + c^3)\,\Phi - (a^3 + \beta^3 + \gamma^3)\,F$$
$$UVW = abc\Phi - \alpha\beta\gamma F.$$

which may be called its index, and shall prove that *the order of any derivative is the square of its index**. It will also be shown that each of the derivatives above referred to will be of the form xU, yV, zW, where U, V, W are quantics in x^3, y^3, z^3 as variables, since these quantities satisfy the equation

$$(xU)^3 + (yV)^3 + (zW)^3 + Kxyz\,UVW = 0,$$

where

$$Kxyz = -x^3 - y^3 - z^3.$$

From this it follows that, calling x^3, y^3, z^3; a, b, c respectively, the scheme of derivatives contains the various solutions of the algebraico-diophantine equation

$$aU^3 + bV^3 + cW^3 - (a+b+c)\,UVW = 0,$$

and that, supposing the law of the squares to be demonstrated, U, V, W will be of the order $\frac{1}{3}\{(3i \pm 1)^2 - 1\}$, that is, $3i^2 \pm 2i$ in a, b, c, where i is any integer. We thus see that the above equation admits of solutions in which U, V, W are of the orders 1, 5, 8, 16, 21, 33, 40 ... respectively. It will hereafter be shown, in like manner, that the missing derivatives, whose indices are multiples of 3 (belonging to the arbitrary point and point of inflexion combined), will satisfy the equation

$$U^3 + V^3 + abc\,W^3 - (a+b+c)\,UVW = 0,$$

where U, V, W will be necessarily of the orders $3i^2 \pm 2i$, $3i^2 \pm 2i$, $(i \pm 1)(3i \pm 1)$ respectively, i, as before, representing any integer. Thus we see that, if $a+b+c=0$, the equations

$$aU^3 + bV^3 + cW^3 = 0 \text{ and } U^3 + V^3 + abc\,W^3 = 0$$

will admit of an infinite number of solutions in integers, when a, b, c are integer. This fact, as regards the latter equation, has been already pointed out by M. Lucas in this *Journal*, and previously by the Abbé Pépin in his memoir in *Liouville's Journal*, 2nd series, Tome XV.

Let us begin with applying the formulæ to obtaining the co-ordinates of the tangential.

Let

$$x^3 + y^3 + z^3 + 3kxyz = 0$$

be the equation to the cubic. If we take x, y, z; $x+\delta x$, $y+\delta y$, $z+\delta z$ two consecutive points, their connective will be the tangential.

Applying the formulæ just obtained, we shall obtain for its co-ordinates expressions each of the form $P\delta x + Q\delta y + R\delta z$ with only one relation between $\delta x, \delta y, \delta z$. Hence, if we write $\delta z = \lambda\delta x + \mu\delta y$ the resulting ratios must be

* The proof here supplied is sufficiently exact to dispel any reasonable doubt as to the truth of the law; but an exact proof which does not assume but demonstrates the non-existence of latent common measures to the reduced values of the co-ordinates of the connective to any two derivatives will be furnished under Title 5—one of the most surprising feats of demonstration which it has ever fallen to the author's lot to accomplish.

independent of λ and μ. Consequently we may make $\delta z = 0$. The two connectives then become

$$x,\ y,\ z$$

$$x + \delta x,\ y + \delta y,\ z,$$

and the co-ordinates of the tangential will therefore be proportional to

$$yz(x+\delta x)^2 - z(y+\delta y)x^2 : zx(y+\delta y)^2 - z(x+\delta x)y^2 : z^2\{xy - (x+\delta x)(y+\delta y)\}$$

that is, to $\quad x(2y\delta x - x\delta y) : y(2x\delta y - y\delta x) : z(x\delta y + y\delta x)$

where $\quad \delta x : \delta y :: y^2 + kxz : x^2 + kyz.$

Hence the co-ordinates required are as

$$x\{2y^3 + x^3 + 3kxyz\} : y\{-2x^3 - y^3 - 3kxyz\} : z(x^3 - y^3),$$

that is, as $\quad x(y^3 - z^3) : y(z^3 - x^3) : z(x^3 - y^3),$

a result which appears to have been first found by Cauchy for the general form, but previously by Euler, and before him by Fermat, for the case $k = 0$.

If we write $a, b, c,$ instead of $x, y, z,$ and call the co-ordinates of the tangential $x, y, z,$ we might find their values by virtue of the condition that the connective of a, b, c and x, y, z is a, b, c over again. This furnishes the equations

$$bcx^2 - a^2yz = am$$

$$cay^2 - b^2zx = bm$$

$$abz^2 - c^2xy = cm,$$

which may be satisfied by writing

$$x = a(b^3 - c^3)\rho\ ;\quad y = b(c^3 - a^3)\rho\ ;\quad z = c(a^3 - b^3)\rho\ ;$$

$$(a^6 + b^6 + c^6 - a^3b^3 - b^3c^3 - a^3c^3)\rho^2 = m\ ;$$

but whether or not the above is necessarily the only possible solution is not quite clear *a priori*, and *a posteriori* it looks as if the solutions might be manifold.

The co-ordinates of the point whose index is 4, that is, of the second tangential, will be those of the first tangential to the point

$$x(y^3 - z^3) : y(z^3 - x^3) : z(x^3 - y^3),$$

namely,

$$x(y^3 - z^3)\{y^3(x^3 - z^3)^3 + z^3(x^3 - y^3)^3\} : y(z^3 - x^3)\{z^3(y^3 - x^3)^3 + x^3(y^3 - z^3)^3\}$$
$$: z(x^3 - y^3)\{x^3(z^3 - y^3)^3 + y^3(z^3 - x^3)^3\},$$

and are of the order 16.

To find the co-ordinates of the point whose index is 5, we may take the connective of the one last found, and of $x, y, z,$ that is, of 4 and 1. Let us

call them xU, yV, zW, and, for greater simplicity, denote x^3, y^3, z^3, by u, v, w. Then, omitting the common factor xyz,

$$U = (v-w)^2\{v(u-w)^3 + w(u-v)^3\}^2$$
$$-(w-u)(u-v)\{w(v-u)^3 + u(v-w)^3\}\{u(w-v)^3 + v(w-u)^3\},$$

with similar quantities (*mutatis mutandis*) set against V and W.

These quantities will have the common measure

$$u^2 + v^2 + w^2 - uv - uw - vw.$$

To prove this let either one of its factors, as $u + \rho v + \rho^2 w, = 0$.

Then $$v - u = \rho^2(w-v) \text{ and } u - w = \rho(w-v),$$

and the representative of U above written becomes

$$\{(v-w)^2 - (w-u)(u-v)\}(w-v)^8 = (v^2 + w^2 + u^2 - vw - uw - uv)(w-v)^8 = 0.$$

Hence the representative of U vanishes with, and therefore contains

$$u^2 + v^2 + w^2 - uv - uw - vw$$

as a factor, and the same must evidently be true for the representatives of V and W; hence, U, V, W, will be of the order $10-2$ or 8, in u, v, w, and the co-ordinates xU, yV, zW, of the order $3.8+1$, that is, of the order 25 in xyz.

The preceding demonstration depends essentially on the fact that my simplified formulæ for the co-ordinates of the connective of two points on a cubic fail, that is to say, become illusory, for a particular relation between the two points, as is easily seen; for let x, y, z; $x, \rho y, \rho^2 z$ be two points on a cubic, then the formulæ for X, Y, Z, the connective's co-ordinates, become

$$(\rho y \,.\, \rho^2 z - yz)x^2;\ (\rho^2 z \,.\, x - xz\rho^2)y^2;\ (x \,.\, \rho y - xy\rho^4)z^2,$$

that is, all vanish, whereas it may be remarked that the general expressions given at page [354],

$$X = (y^2\eta\xi - y\eta^2 x + z^2\zeta\xi - z\zeta^2 x) + K(yz\xi^2 - \eta\zeta x^2)$$
$$Y = (z^2\zeta\eta - z\zeta^2 y + x^2\xi\eta - x\xi^2 y) + K(zx\eta^2 - \zeta\xi y^2)$$
$$Z = (x^2\xi\zeta - x\xi^2 z + y^2\eta\zeta - y\eta^2 z) + K(xy\zeta^2 - \xi\eta z^2),$$

become the minors of

$$\begin{matrix} x^2 & \rho y^2 & \rho^2 z^2 \\ (\rho^2-\rho)yz & (1-\rho^2)zx & (\rho-1)xy; \end{matrix}$$

that is, $(\rho^2-\rho)x(y^3-z^3)$, $(\rho-1)y(z^3-x^3)$, $(1-\rho^2)z(x^3-y^3)$,

which are the same as

$$x(y^3-z^3),\quad \rho^2 y(z^3-x^3),\quad \rho z(x^3-y^3),$$

and remain perfectly valid.

This law of the failing case enables me to prove very easily the *Law of Squares*, as follows:

Suppose it proved that for all indices inferior to $6i$ the order of the derivative is equal to the square of its index; then, to prove that the same law is true up to $6(i+1)$, it is only necessary to consider the cases of $6i+1$, $6i+5$, for, as regards the indices $6i+2$ and $6i+4$, the derivatives may be regarded as the tangentials of the derivatives to indices $3i+1$ and $3i+2$, and will consequently be of the orders $4(3i+1)^2$ and $4(3i+2)^2$, that is, $(6i+2)^2$ and $(6i+4)^2$ respectively.

Let us further suppose that for derivatives whose indices are inferior to $6i$ the co-ordinates are of the form xU, yV, zW; U, V, W being quantics in x^3, y^3, z^3; then, obviously, from the mode of forming the tangential, this will be true for derivatives whose indices are $6i+2$, $6i+4$: for the tangential to xU, yV, zW is

$$xU(y^3V^3 - z^3W^3), \quad yV(z^3W^3 - x^3U^3), \quad zW(x^3U^3 - y^3V^3).$$

Let us consider the point (1) whose co-ordinates x, y, z satisfy the equation

$$x^3 + \rho y^3 + \rho^2 z^3 = 0.$$

For such a point $\quad y^3 - z^3 : z^3 - x^3 : x^3 - y^3 :: 1 : \rho : \rho^2,$

and the point (2) becomes $x, \rho y, \rho^2 z$. Consequently the point (4) becomes $x(y^3 - z^3), \rho y(z^3 - x^3), \rho^2 z(x^3 - y^3)$, the same as $x, \rho^2 y, \rho z$; hence the point (5), the connective of (1, 4), becomes $x(y^3 - z^3), \rho y(z^3 - x^3), \rho^2 z(x^3 - y^3)$, the same as $x, \rho^2 y, \rho z$, so that, denoting the derivatives by their indices,

$$5 = 4 \qquad 7 = 1,\ 8 = 1,\ 1 = 2 \qquad 10 = 2,\ 8 = 2,\ 1 = 1$$

$$11 = 4,\ 7 = 4,\ 2 = 2 \qquad 13 = 2,\ 11 = 2,\ 2 = 4, \text{ etc.}$$

We have, thus, for all values of the point i

$$9i \pm 1,\ 2,\ \pm 4 = 1,\ 2,\ 4,$$

when 1 is the point for which $x^3 + \rho y^3 + \rho^2 z^3 = 0$.

Hence, if p, p' be any two points for which $p - p' = 3$, then p, p' will be respectively identical with some two out of the three points 1, 2, 4. And it will at once be seen that the simplified formulæ for the connective of any two of these three points become illusory.

Now the point $6i + 1$ is the connective of $3i - 1$ and $3i + 2$, and the point $6i + 5$ is the connective of $3i + 1$ and $3i + 4$.

Hence, in each of these cases, the simplified formulæ become illusory, that is, the expressions for each of the co-ordinates vanish when

$$x^6 + y^6 + z^6 - x^3y^3 - x^3z^3 - y^3z^3$$

vanishes, and must therefore contain it as a common measure. Moreover, the simplified formulæ for the connective co-ordinates for the points xU, yV, zW;

xU', yV', zW' will contain x^2yz, y^2zx, z^2xy, and will therefore have the common measure xyz. Hence the values of the co-ordinates when freed from these common measures will be of the order in x, y, z, $2(3i-1)^2+2(3i+2)^2-9$ for the point $6i+1$, and $2(3i+1)^2+2(3i+4)^2-9$ for the point $6i+5$, that is $(6i+1)^2$ and $(6i+5)^2$ respectively, and will obviously continue to be quantics in x^3, y^3, z^3 multiplied by x, y, z respectively. Hence the theorem being true for index inferior to 6 is true universally.

It will be observed that any co-ordinate X of the point k must contain the X co-ordinate of the point k' where k' is any factor of k; for if $k=\delta k'$ the point k may be obtained by forming the point δ to the point k', and it has been shown that the δ derivative to any point has co-ordinates which contain respectively those of the initial point. Consequently the X co-ordinate to any point k may be resolved into factors containing a primitive part of the order τk (the totient of k) in the variables, and a non-primitive part containing the primitive part of each power of a prime contained in k, and with the exception of the single factor x all the others will be quantics in x^3, y^3, z^3; and, of course, the same remark applies to the other two co-ordinates Y and Z. We might obtain the point $m \ddagger n$ as the connective of m, n. In that case the simplified formulæ would give expressions of the order $2(m^2+n^2)$ in x, y, z; and as the actual order of the co-ordinates in those variables is $(m \ddagger n)^2$, it follows that when $m-n \equiv 0$, mod. 3, there will be a common measure (a symmetrical function of x, y, z) of the order $(m-n)^2$, and when $m+n \equiv 0$, mod. 3, of the order $(m+n)^2$ running through those expressions, and it might be desirable to ascertain its form; but without waiting to solve this problem*, which is irrelevant to the matter in hand, I shall proceed at once to consider the derivatives corresponding to indices which are multiples of the number 3, to obtain which it is only necessary, as will be seen immediately, to combine one given point of inflexion with one arbitrary point of the curve. But, before doing so, it may be well to notice, that while the preceding investigation serves to show that the abridged formulæ for the connective co-ordinates possess the common measure

$$xyz(x^6+y^6+z^6-x^3y^3-x^3z^3-y^3z^3),$$

it does not demonstrate categorically that there is no other; or that some power of the second factor above written other than the first might not be a common measure. Consequently, what we have strictly proved, as will be evident on reviewing the argument, is that the order to a derivative of the index $3i \pm 1$ cannot *exceed* the square of that index; but before I come to an end of the discussion I trust to be able to establish with *Dirichletian* rigour that the order is actually equal to the square of the index†.

* It is completely solved in the corollary to Title 5.

† This anticipation (for it was only such when these words were written) will be found fully realised under Title 5.

Title 2.—*On the Completed or Continuously Numbered Scale of Rational Derivatives to an Arbitrary Point on a Cubic, of which one Point of Inflexion is given.*

Let I be the given point of inflexion, and let any point (or system of points) and another point (or system of points respectively) collinear with the former in respect to I be called opposites. It is obvious that $(I, I) = I$, or that the inflexion is its own opposite. It will be convenient to denote the opposite to any point by the same index, but accented.

We have, then, obviously,

$$(p', p) = I;\ (p')' = p \text{ and } (p', q)' = I,\ (p', q) = (I, I),\ (p', q) = (I, p'),\ (I, q) = (p, q').$$

Let $(I', 2) = 3$; $(I', 5) = 6$; and in general $(I', 3i-1) = 3i$. This is matter of definition. Let, now, the infinite system 1, 2, 3, 4, 5, 6, 7 ... and its opposite be regarded as a single group. I say, (1), that this will be a closed group, in the sense that a straight line drawn through any two points (contiguous or apart) of this double chain will cut the cubic in a third point included in the group, (2), that the new points will be rational in respect to the co-ordinates of the initial point and the given point of inflexion, and, (3), that the order in the variables for every point, without regard to its relation to the modulus 3, will be, as before, the square of its index.

I proceed to show that the connective of any two points in the double chain may be expressed as a single point therein. Several cases present themselves according to the form of each of the two connected points in respect to the modulus 3, except when the indices are congruent in respect to that modulus.

When the residues (r, r'), in respect to that modulus, are dissimilar, the result will in general be different according as one of them (as r) belongs to the higher or lower index.

In what follows it is to be understood that $i \gtrless j$.

Theorem 1. To prove that

$$3i+1,\ (3j+1)' = 3j-3i$$

and

$$3i+2,\ (3j+2)' = (3j-3i)'.$$

[This will imply that

$$(3i+1)',\ 3j+1 = (3j-3i)'$$

and

$$(3i+2)',\ 3j+2 = 3j-3i.]$$

We have

$$3i+1,\ (3j+1)' = (3i-1, 2),\ [(3j-1)', 2'] = (2, 2'),\ [3i-1, (3j-1)'] = (3i-1)',\ 3j-1 = [(3i-2)', 1'],\ (3j-2, 1) = (1, 1'),\ [(3i-2)', 3j-2] = 3i-2,\ (3j-2)'.$$

Hence, $3i+1,\ (3j+1)'=1,\ (3j-3i+1)'=(1,\ 2),\ [(3j-3i-1)',\ 2']$
$=(2,\ 2'),\ [1,\ (3j-3i-1)']=1',\ (3j-3i-1)=3j-3i$
and $3i-1,\ (3j-1)'=I,\ [3i-2,\ (3j-2)']=(3j-3i)'.$

Theorem 2. To prove that

$$3i+1,\ (3j-1)'=(3i+3j)'$$
and
$$3i-1,\ (3j+1)'=3i+3j.$$

[This will imply that

$$(3i+1)',\ 3j-1=3i+3j$$
and
$$(3i-1)',\ 3j+1=(3i+3j)'.]$$

We have $3i+1,\ (3j-1)'=3i-1,\ 2;\ (3j+1)',\ 2'=(3i-1)',\ 3j+1$
$=[(3i-2)',\ 1'],\ (3j+2,\ 1)=3i-2,\ (3j+2)'.$
Therefore, $3i+1,\ (3j-1)'=1,\ (3j+3i-1)'=(3i+3j)'$
and $3i-1,\ (3j+1)'=I,\ [(3i-1)',\ 3j+1]=3i+3j.$

Collecting the results of these two theorems, we see that

$$\left.\begin{aligned} &3i\pm1,\ (3j+1)'=3j\mp3i=(3i\mp1)',\ 3j-1\\ \text{and}\quad &3i\pm1,\ (3j-1)'=(3j\pm3i)'=(3i\mp1)',\ 3j+1\end{aligned}\right\},\qquad (A)$$

so that, using $p \doteq q$ (where neither p nor q contains 3), to denote that one of the two numbers $p+q,\ p\sim q$, which is divisible by 3, $(p,\ q')$ is always either $p \doteq q$ or $(p \doteq q)'$. Also

$$3i+1,\ (3j)'=(3i-1,\ 2),\ [1,\ (3j-1)']=(1,\ 2),\ [3i-1,\ (3j-1)']$$
$$=(3j-3i)',\ 1=(1',\ 3j-3i+1),\ (2,\ 1)=[(1',\ 1),\ (3j-3i+1,\ 2)]$$
$$=(3j-3i-1)';$$
again $3i,\ (3j+1)'=(3i-1,\ 1'),\ [(3j-1)',\ 2']=1',\ (3j-3i)'$
$=(1',\ 2'),\ [1,\ (3j-3i-1)']=(1,\ 1'),\ [(3j-3i-1)',\ 2']=3j+1-3i;$
and lastly $3i,\ (3i+1)'=(3i-1,\ 1'),\ [(3i-1)',\ 2']=I,\ 1'=1.$

Hence, collecting the results, $3\iota,\ (3i+1)'=(3i+1)\sim3\iota$, whatever the relation of magnitude may be between i and ι.

Similarly,

$$3i-1,\ (3j)'=(3i+1,\ 2),\ [1,\ (3j-1)']=(1,\ 2),\ [3i+1,\ (3j-1)']$$
$$=1,\ (3i+3j)'=(3i+3j-1)';$$
$$(3i)',\ 3j-1=[(3i-1)',\ 1],\ (3j+1,\ 2)=1,\ (3i+3j)'=(3i+3j-1)';$$
and $(3i)',\ 3i-1=[(3i-1)',\ 1],\ (3i+1,\ 2)=1,\ (6i)'=(6i-1)'.$

Hence, collecting the results, $3i-1,\ (3\iota)'=(3i+3\iota-1)'$, and we have

$$\left.\begin{aligned} &3\iota,\ (3i+1)'=(3i+1)\sim3\iota;\quad (3\iota)',\ 3i+1=[(3i+1)\sim3\iota]'\\ &3\iota,\ (3i-1)'=3i-1+3\iota;\quad (3\iota)',\ 3i-1=(3i-1+3\iota)'.\end{aligned}\right\}\qquad (B)$$

Also,

$$\left.\begin{array}{l} 3\iota,\ 3i-1=(3\iota-1,\ 1'),\ (3i-2,\ 1)=(3\iota-1,\ 3i-2)'=[(3i-1)\sim 3\iota]' \\ 3\iota,\ 3i+1=(3\iota-1,\ 1'),\ (3i+2,\ 1)=(3\iota-1,\ 3i+2)'=(3\iota+3i+1)'. \end{array}\right\} \quad (B')$$

It remains only to determine the connectives of $3i$, 3ι and of $3i$, $(3j)'$ or $(3i)'$, $3j$, which is easily done, for

$$3i,\ 3\iota=(3i-1,\ 1'),\ (3\iota-1,\ 1')=(1',\ 1'),\ (3i-1,\ 3\iota-1)=2',\ 3i+3\iota-2.$$

Hence (by A) $3i$, $3j=(3i+3j)'$ and consequently $(3i)'$, $(3\iota)'=3i+3\iota$.

Again

$3i$, $(3j)'=(3i-1,\ 1')$, $[(3j-1)',\ 1]=(1,\ 1')$, $[3i-1,\ (3j-1)']=$(by theorem A) I, $(3j-3i)'=3j-3i$. Hence also $3j$, $(3i)'=(3j-3i)'$.

These three results may be designated theorem C; and theorems A, B, B', C collectively prove that the original scale 1, 2, 4, 5, 7, 8 ..., which formed a closed system (so to say "group"), remains still closed when we complete it by insertion of multiples of 3, provided that we join on to the completed system 1, 2, 3, 4, 5, 6, 7 ... the opposite system 1', 2', 3', 4', 5', 6', 7' ....

In every case it will be observed the connective of two indices (disregarding the accent) is either their sum or their difference.

The double scale may be formed by alternate addition of 1 and 1' in the manner following:

$$1,\ 1=2 \qquad 1',\ 2=3 \qquad 1,\ 3=4' \qquad 1',\ 4'=5' \qquad 1,\ 5'=6' \qquad 1',\ 6'=7$$

$$1,\ 7=8 \qquad 1',\ 8=9 \qquad 1,\ 9=10' \qquad 1',\ 10'=11' \qquad 1,\ 11'=12' \ldots$$

which gives the numbers 1, 2, 3, 4', 5', 6', 7, 8, 9, 10', 11', 12', etc.; and, in like manner, by interchanging 1, 1', we may obtain 1', 2', 3', 4, 5, 6, 7', 8', 9', 10, 11, 12, etc.

The new points 3, 6, 9 ...; 3', 6', 9' ... belong to the natural scales 1, 2, 5 ...; 1', 2', 5' ... collectively and not respectively; and the accented and unaccented multiples of 3 might have had their significations interchanged without any impropriety. It is now necessary to extend the law of the order in the variables to these inserted points, and to prove that for them, as for the points in the natural scale, the order of any point, in the variables of the initial point, is the square of its index.

If the cubic be thrown into the canonical form $x^3+y^3+z^3+kxyz$, the point $x=1$, $y=-1$, $z=0$ may be taken to represent I, and if x, y, z be the initial point 1, the co-ordinates of 1' (the connective of 1 and I) become by the general formula yz, zx, z^2, or, more simply, y, x, z.

To find 3, then, we have to take the connective of y, x, z and $x(y^3 - z^3)$, $y(z^3 - x^3)$, $z(x^3 - y^3)$; its co-ordinates, accordingly, by the general formula, are

$$yz(z^3 - x^3)(x^3 - y^3)y^2 - x^3z(y^3 - z^3)^2$$
$$xz(x^3 - y^3)(y^3 - z^3)x^2 - y^3z(z^3 - x^3)^2$$
$$xy(y^3 - z^3)(z^3 - x^3)z^2 - yxz^2(x^3 - y^3)^2;$$

or, neglecting the common factor z, the co-ordinates of 3 are

$$y^3(x^3 - y^3)(x^3 - z^3) + x^3(y^3 - z^3)^2$$
$$x^3(y^3 - x^3)(y^3 - z^3) + y^3(z^3 - x^3)^2$$

and $$xyz(z^3 - x^3)(z^3 - y^3) + xyz(x^3 - y^3)^2;$$

or $$y^3x^6 + z^3y^6 + x^3z^6 - 3x^3y^3z^3$$
$$x^3y^6 + z^3x^6 + y^3z^6 - 3x^3y^3z^3$$

and $$xyz(z^6 + y^6 + x^6 - x^3y^3 - z^3x^3 - y^3z^3).$$

In the particular case where $x^3 + y^3 + z^3 = 0$, these expressions (writing for greater brevity L, M, N for x^3, y^3, z^3) become

$$ML^2 - (L + M)M^2 + L(L + M)^2 + 3LM(L + M)$$
$$LM^2 - (L + M)L^2 + M(L + M)^2 + 3LM(L + M)$$
$$xyz[(L + M)^2 + L^2 + M^2 - LM + (L + M)^2]$$

or $$L^3 + 6L^2M + 3LM^2 - M^3$$
$$M^3 + 6M^2L + 3ML^2 - L^3$$
$$3xyz(L^2 + LM + M^2);$$

which remain equally good, as co-ordinates of the point 3 to the initial point x, y, z, when the cubic is $x^3 + y^3 + Cz^3$, as is easily seen by writing $C^{\frac{1}{3}}z = \zeta$.

The point 3, it follows from what precedes, is of the order 9 in the variables x, y, z, and the same will be true for 3′, which is obtained from 3 by the interchange of x and y; but in order that these points may be arithmetically as well as algebraically rational, it is of course necessary that the given cubic may admit of being expressed under the form

$$Ax^3 + Ay^3 + Cz^3 + Kxyz,$$

where A, C and K are integers.

Again, since $6 = 3'$, 3′, 6 is the 2 of 3′, and similarly 6′ is the 2 of 3; since $9 = 3'$, 6′ and 6′ is the 2 of 3, 9 is the 3 of 3. So again, since $12 = 3'$, 9′ and 9′ is the 3 of 3′, 12 is the (1, 3) of 3′, that is, the 4′ of 3′ or 4 of 3; and similarly 12′ is the 4 of 3′. So again,

$15 = (3', 12') = (1, 4)$ of $3' = 5$ of 3′, and $15' = 5$ of 3
$18 = (3', 15') = (1, 5')$ of $3' = 6'$ of $3' = 6$ of 3, and $18' = 6$ of 3′
$21 = (3', 18') = (1, 6)$ of $3' = 7'$ of $3' = 7$ of 3, and $21' = 7$ of 3′
$24 = (3', 21') = (1, 7)$ of $3' = 8$ of 3′, and $24' = 8$ of 3;
$27 = (3', 24') = (1, 8')$ of $3' = 9'$ of $3' = 9$ of 3 ....

Hence, in general,

$$9i+3=(3i+1) \text{ of } 3;\ 9i+6=(3i+2)' \text{ of } 3;\ \text{and } 9i=3i \text{ of } 3.$$

Consequently

$$3^q(3i+1)=(3i+1) \text{ of } 3 \text{ of } 3 \text{ of } 3 \ldots (q \text{ times repeated}),$$

and

$$3^q(3i+2)=(3i+2)' \text{ of } 3 \text{ of } 3 \text{ of } 3 \ldots (q \text{ times repeated}).$$

From this it follows, obviously, that $3^q(3i \pm 1)$ and $[3^q(3i \pm 1)]'$ are each of the order $[3^q(3i \pm 1)]^2$ in the variables, and thus the law of the squares extends to all points alike in the completed scale.

Title 3.—*On Compound Derivation.*

The object of what follows is to show that any derivative of a derivative has for its index (due regard being paid to the accents) the product of the numerical values of the indices of the operator and operand derivatives, that is to say, the $i^?$ of $j^? = ij^?$; the mark of interrogation denoting either a blank or an accent, as the case may be. Thus, while connection involves addition or subtraction, composition involves a process of multiplication.

(1) Let us consider the i of j when neither i nor j contains 3. Then

$$3k+1 \text{ of } j=(2 \text{ of } j),\ (3k-1 \text{ of } j) \text{ and } 3k+2 \text{ of } j=(1 \text{ of } j),\ (3k+1 \text{ of } j).$$

Suppose the theorem proved up to $3k-1$. Then

$$3k+1 \text{ of } j = 2j,\ 3kj-j=(3k+1)j$$

$$3k+2 \text{ of } j = j,\ 3kj+j=(3k+2)j.$$

Hence it is true up to $3(k+1)-1$, and, being true when $k=1$ (since 1 of $j=j$ and 2 of $j=j, j=2j$), it is true universally.

In like manner, since 1 of $j'=j'$ and 2 of $j'=j'$, $j'=I$, $(j, j)=(2j)'$, it may be shown that i of $j'=(ij)'$. Moreover

$$1' \text{ of } j=j', \text{ and therefore } 2' \text{ of } j=(1' \text{ of } j),\ (1' \text{ of } j)=j', j'=2j'$$

and

$$(3k+1)' \text{ of } j=(2' \text{ of } j),\ [(3k-1)' \text{ of } j]$$

$$(3k+2)' \text{ of } j=(1' \text{ of } j),\ [(3k+1)' \text{ of } j];$$

so that, if the equation i' of $j=(ij)'$ holds good up to $i=3k-1$,

$$(3k+1)' \text{ of } j=[(3k+1)j]', \text{ and } (3k+2)' \text{ of } j=[(3k+2)j]';$$

so that the equation i' of $j=(ij)'$ will hold good up to $3(k+1)-1$, and, being true for $k=1$, is true universally.

In like manner, since 1′ of $j'=j$, it will follow that i' of $j'=ij$.

It remains to obtain the corresponding equations when i, j are one or both of them multiples of 3.

Since 3 of $3^q = (3^q, 3^q)$, $(3^q)' = (2 \cdot 3^q)'$, $(3^q)' = 3^{q+1}$,

9 of $3^q = 3$ of 3 of $3^q = 3$ of $3^{q+1} = 3^{q+2}$,

27 of $3^q = 3$ of 9 of $3^q = 3$ of $3^{q+2} = 3^{q+3}$, and so on.

Hence 3^p of $3^q = 3^{p+q}$.

Again, 3 of $3j+1 = (3j+1, 3j+1)$, $(3j+1)'$

$= 6j+2$, $(3j+1)' = 9j+3$ by A.

Hence 3^2 of $3j+1 = 3$ of $9j+3 = (18j+6)'$, $(9j+3)' = 27j+9$ by C,

3^3 of $3j+1 = 3$ of $27j+9 = (54j+18)'$, $(27j+9)' = 81j+27$ by C,

and so on. Hence 3^p of $3j+1 = 3^p(3j+1)$.

Again, 3 of $3j+2 = (3j+2, 3j+2)$, $(3j+2)'$

$= 6j+4$, $(3j+2)' = (9j+6)'$ by A.

Hence 3^2 of $3j+2 = 3$ of $(9j+6)' = 18j+12$, $9j+6 = (27j+18)'$ by C,

and so on. Hence 3^p of $3j+2 = [3^p(3j+2)]'$.

Again, $3j+1$ of $3^p = (2$ of $3^p)$, $(3j-1$ of $3^p) = (3^p, 3^p)$, $(3j-1$ of $3^p)$

$= (2 \cdot 3^p)'$, $(3j-1$ of $3^p)$

and $3j-1$ of $3^p = (1$ of $3^p)$, $(3j-2$ of $3^p)$.

Suppose it true that $3j-2$ of $3^p = (3j-2)\,3^p$ for a certain value of j.

Then $3j-1$ of $3^p = 3^p$, $(3j-2)\,3^p = [(3j-1)\,3^p]'$

and $3j+1$ of $3^p = (2 \cdot 3^p)'$, $[(3j-1)\,3^p]' = (3j+1)\,3^p$.

But 1 of $3^p = 1 \cdot 3^p$; hence, for all values of j,

$3j+1$ of $3^p = (3j+1)\,3^p = 3^p$ of $3j+1$

$3j-1$ of $3^p = [(3j-1)\,3^p]' = 3^p$ of $3j-1$.

Hence, by the well-known method of successive transformation, we obtain the following results:

When neither m nor n contains 3, when both contain 3, and when one of them contains 3 and the other is of the form $3j+1$, we have

m of $n = n$ of $m = m'$ of $n' = n'$ of $m' = mn$

m of $n' = n'$ of $m = m'$ of $n = n$ of $m' = (mn)'$.

In the remaining case (namely when of m and n, one contains 3 and the other is of the form $3j-1$), we have

m of $n = n$ of $m = m'$ of $n' = n'$ of $m' = (mn)'$

m of $n' = n'$ of $m = m'$ of $n = n$ of $m' = mn$.

This completes the algorithm of rational derivation.

Title 4.—On Pertactile or Periodic Points on a Cubic Curve.

A pertactile point, or point of pluperfect tactility, on a general cubic is a point at which the cubic admits of a higher order of contact with another curve than is in general possible. Thus the points of inflexion are pertactile points, because a tangent at one of them will meet the curve in three consecutive points. The same is the case with Plücker's twenty-seven points, because at each of them a conic of closest contact will pass through six consecutive points, the sixth point in which any conic passed through five consecutive points cuts the curve coinciding, in this case, with the point of contact. So, in general, a curve of the ith order can only be made to pass through $3i-1$ consecutive points situated at P; but if the ith derivative of P is a point of inflexion, then the $3i$th point common to all curves of the ith order passing through $3i-1$ consecutive points at P will coincide with P, so that such curves will pass through $3i$ consecutive points, and P may accordingly be termed a point of pluperfect tactility, or more briefly, a pertactile point.

To prove that this is the case, it is necessary, in the first place, to prove that, at a general point P in the cubic, the $3i$th point in which all curves of the ith order passing through $3i-1$ consecutive points at P intersect the cubic, is the $(3i-1)$th derivative of P, which may be done inductively as follows:

Suppose P_{3i-1} is the residual of $3i-1$ consecutive points at P. To find the residual of $3i+2$ consecutive points there, we may combine $3i-1$ giving the residual P_{3i-1}, two more of them giving the residual P_2, and one giving Q, R, any two points collinear with P. We then combine (P_{3i-1}, P_2), (Q, R) and obtain P_{3i+1}, P_1 which gives P_{3i+2} as the required residual. Hence the theorem, being true for P_2 (the residual of two consecutive points at P) and true for $P_{3(i+1)-1}$ if true for P_{3i-1}, is true universally.

If, now, the residual of $3i-1$ points at P is to fall at P we must have $P_1 = P_{3i-1}$.

(1) Suppose $i = 3k-1$, then P_1, $P_{i-1} = P_{i-1}$, P_{3i-1}, that is $P_i = P_{2i}$.

Hence P_i is a point of inflexion I, or, as we may express it, P is an ith sub-derivative of such point, or $P = \underset{i}{I_1}$.

(2) Suppose $i = 3k+1$, then P_1, $P_2 = P_2$, P_{3i-1}, that is $P_1 = P_{3i+1}$.

Hence P_1, $P_{i+1} = P_{i+1}$, P_{3i+1}, that is $P_i = P_{2i}$, and, as before, $P = \underset{i}{I_1}$.

(3) Suppose $i = 3k$.

Then 1, $(i-1)' = (i-1)'$, $3i-1$, that is $i' = 2i = i''$, i'. Consequently i'', and therefore also i, is a point of inflexion.

Hence, as in the other two cases, P is an ith sub-derivative of a point of inflexion*, which may either be the point used to form the scale, or any of the eight other inflexions†.

It may be well to notice here that whilst P_i, when i does not contain 3, is, as already shown, of the form xU, yV, zW, it follows from the law of compound derivation, since P_3 is of the form R, S, $xyz\Theta$ (where R, S, Θ, like U, V, W, are quantics in x^3, y^3, z^3) that P_i, when i is a multiple of 3 or any power of 3, will be of the form M, N, $xyz\Omega$ (where M, N, Ω are still quantics in x^3, y^3, z^3).

Calling X, Y, Z any ith derivative to $x^3+y^3+z^3+kxyz=0$, we must have $X^3+Y^3+Z^3+kXYZ=0$; and, in order for such derivative to be a point of inflexion, it is necessary and sufficient that $X=0$ or $Y=0$ or $Z=0$; combining these equations respectively with the given cubic, we shall obtain, in all, 3 times $3i^2$ or $9i^2$ points, sub-derivatives of the ith grade to one or other of the inflexions; but out of these, whether i be or be not divisible by 3, nine will correspond to $x=0$, $y=0$, or $z=0$ combined with the curve, that is, will be the points of inflexion themselves. Moreover, unless i be a prime number, it follows from the law of compound derivation, combined with the fact that x, y, z enter distributively or collectively into the derived co-ordinates X, Y, Z, that, if i' be any factor of i, and X', Y', Z' the co-ordinates of the i'th derivative, Z will contain Z' and X, Y or Y, X, will contain X', Y' respectively. There will thus be a *primitive* part to X, Y, Z which results from driving out all the factors corresponding to any factor of i (unity included), and, if we suppose $i=a^\alpha.b^\beta.c^\gamma\ldots$, the order of this primitive part in the variables x, y, z, it is easy to see, will be

$$a^{2(\alpha-1)}.b^{2(\beta-1)}.c^{2(\gamma-1)}\ldots\{(a^2-1)(b^2-1)(c^2-1)\ldots\},$$

which may be called the quadri-totient to i, and is the product of two factors, one the totient of i and the other what that totient becomes when $+1$ is substituted throughout for -1 in its expression, and which, if a name were needed for it, might be called the contra-totient.

The number of proper, or primitive, ith sub-derivatives of any point of inflexion will thus be the quadri-totient of i (just as the number of primitive ith roots of unity is the totient), and the total number of pertactile points of the ith grade, 9 times the quadri-totient of i.

It is easy to see that the points corresponding to the non-primitive factors of X, Y, Z satisfy, but in an *improper* manner, the conditions of the question. For, if i' is any sub-multiple of i $\left(\text{say } i'=\frac{i}{\delta}\right)$ and P' is an i'th sub-derivative

* A sub-derivative of an inflexion may conveniently be termed a sub-inflexion.

† The above formulæ show that i, $i'=3i=3i'$; hence $3i$ and $3i'$ coincide with the original point of inflexion, whereas i, i', $2i$, $2i'$ need not coincide with the original point of inflexion.

of a point of inflexion, through P' may be drawn δ curves each of the order i' (constituting an improper curve of the order i), each passing through $3i'$ consecutive points, and consequently their *ensemble* passes through $\delta . 3i'$ or $3i$ consecutive points. We have now obtained the generalization of the theorem of which the enumeration of the points of inflexion and Plücker's points constitute the two first steps, and it is very easy to calculate the number of pertactile points N of any given grade i. Thus for

$$i = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\ldots$$
$$\frac{N}{9} = 1, 3, 8, 12, 24, 24, 48, 48, 72, 72, 120, 96\ldots$$

The calculation is facilitated by the remark that if i, j are prime to each other, the number of (ij)th sub-derivatives to any one point of inflexion is the product of the number of ith by the number of jth sub-derivatives; the quadritotient obeying the same law as the totient in this particular.

If i is the grade of the pertactile point P, so that $P_1 = P_{3i-1}$, then P_i is an inflexion, and P_{3i} is I, the original inflexion. Moreover

$$P_1 = P_1,\ P_2 = P_{3i-1},\ P_2 = P_{3i+1}$$
$$P_2 = P_1,\ P_1 = P_1,\ P_{3i-1} = P_{3i-2} \text{ and also} = P_2,\ P_4 = P_{3i-2},\ P_4 = P_{3i+2}$$
$$P_4 = P_2,\ P_2 = P_2,\ P_{3i-2} = P_{3i-4} \text{ and also} = P_2,\ P_{3i+2} = P_{3i+4}, \text{ and so on.}$$

And again, $P'_3 = P_3$, $I = P_3$, $P_{3i} = P'_{3i+3}$, and therefore $P_3 = P_{3i+3}$;

and $P_{3i-3} = P'_{3i+3}$, $P_6 = P'_3$, $P_6 = P'_3$ whence $P_3 = P'_{3i-1}$;

$$P_6 = P'_3,\ P'_3 = P'_{3i+3},\ P'_{3i+3} = P_{6i+6} \text{ and also} = P_{3i-3},\ P_{3i-3} = P'_{6i-6}.$$

Thus in general, $P_{3r+1} = P_{3i\pm(3r+1)}$; $P_{3r-1} = P_{3r\pm(3r-1)}$

and $$P_{3r} = P_{3i+3r} = P'_{3i-3r}.$$

Thus the natural scale $P_1P_2P_4P_5\ldots$

and the completed scale $\begin{cases} P_1P_2P_3P_4P_5P_6\ldots \\ P'_1P'_2P'_3P'_4P'_5P'_6\ldots \end{cases}$

are each of them periodic, the period of the indices being $3i$. We may, accordingly, describe pertactile by the simpler name of periodic points. Every complete set of periodic points forms a closed system. By a complete set is to be understood the $9i^2$ sub-derivatives of the 9 points of inflexion, and by a closed system is to be understood one such that every connective and tangential of the points which it contains is itself a point of the system. According to what law such closed system may be resolved into partial closed systems must form the subject of further inquiry. When $i = 2$, the complete closed system of 36 points we know is resoluble into nine closed systems, each containing one point of inflexion and its three collinear anti-tangentials, and also, in four different ways, into three closed systems, each containing a collinear set of inflexions and their three sets of anti-tangentials.

We are now in a position to solve the problem of in-and-exscribed k-laterals.

Suppose $k=3$, then $2^3+1=3i$ where $i=3$, and the point P_1 will coincide with the point P_3, provided P_3 is a point of inflexion. So that the apices of the in-and-exscribed triangles are the 81 points which satisfy the equation $P_3=P'_6$, of which 9 will correspond to the points of inflexion and 72 remaining over will give 24 finite triangles. If we denote by p, p', p'' three consecutive points in a straight line at any point of inflexion, pp', $p'p''$, $p''p$ form an infinitesimal triangle degenerating into a straight line, and this furnishes an improper solution of the question.

Calling M, N, $xyz\Omega$ the co-ordinates of P_3 when $P_1=x$, y, z, the 72 points are given by combining the equation $MN\Omega=0$ with the equation to the curve.

If $k=4$, we make $2^4-1=3i$ where $i=5$, and if $P_1=P_{3i-1}$, we have also $P_1=P_{3i+1}$; and the apices of the quadrilateral are found by making P_i, that is P_5, a point of inflexion.

The general form of P_5 being xU, yV, zW, the proper sub-derivatives P_5 result from $UVW=0$ combined with the equation to the cubic, and there result $\frac{9(25-1)}{4}$, that is 54 in-and-exscribed quadrilaterals.

Each point of inflexion may still be regarded as yielding an improper solution of the question, since pp', $p'p''$, $p''p'$, $p'p$ may be viewed as a degenerate infinitesimal quadrilateral.

So when $k=5$, making $2^5+1=3i$, $i=11$; and there will result $\frac{9(11^2-1)}{5}=216$ in-and-exscribed pentagons.

Likewise, since $\frac{2^7+1}{3}=43$, there result $9\,\frac{43^2-1}{7}$, that is $9\,.\,264$ or 2376 in-and-exscribed heptagons.

Let us now consider a case of k a composite number, and to fix the ideas, suppose $k=15$. Make $\frac{2^{15}+1}{3}=i$, then $i=10923$. $\frac{2^{15}+1}{3}$, *by virtue of its form*, contains the factors $\frac{2^3+1}{3}$ and $\frac{2^5+1}{3}$, that is 3 and 11, and is in fact equal to $3\,.\,11\,.\,331$. P_i will therefore be of the form $xU_3U_{11}\mathbf{U}$, $yV_3V_{11}\mathbf{V}$ $zW_3W_{11}\mathbf{W}$ (xU_3, yV_3, zW_3 corresponding to P_3, and xU_{11}, yV_{11}, zW_{11} to P_{11}).

Accordingly $\mathbf{U}$, $\mathbf{V}$, $\mathbf{W}$ will each be of the degree $(3\,.\,11\,.\,331)^2-3^2-11^2+1$, and the equation $\mathbf{UVW}=0$, combined with the equation to the curve, will give the apices of the in-and-exscribed quindecagons, not including the improper solutions due to the points of inflexion, nor those due to the apices of the in-and-exscribed triangles or pentagons, which, in a certain but improper

sense, each belong to the case of quindecagons. The number of apices of the proper quindecagons will therefore be $9[(3.11.331)^2 - 3^2 - 11^2 + 1]$, comprising sub-inflexions of several grades, as follows: $9(331^2 - 1)$ of the 331th grade, $9(3^2 - 1)(11^2 - 1)$ of the 33rd grade, $9(3^2 - 1)(331^2 - 1)$ of the 993rd grade, $9(11^2 - 1)(331^2 - 1)$ of the 3641th grade, and $9(3^2 - 1)(11^2 - 1)(331^2 - 1)$ of the 10923rd grade*. The above number of apices may be written $9[11^2.3^2(331^2 - 1) + (3^2 - 1)(11^2 - 1)]$, so that the number of quindecagons is $9[11^2.3^2.22.332 + 8^2]$.

It may be noticed that the primitive algebraical factor of $2^{15} + 1$, namely 331, is a prime number. But the primitive part of $2^k - 1$ (k being even) or $2^k + 1$ (k being odd), that is $2^k - 1$ or $2^k + 1$ stripped of its obligatory factors dependent algebraically on the prime factors of k, may be a composite number.

Thus, let us suppose $k = 9$, the problem being that of finding the nature and number of the in-and-exscribed nonagons. Here $i = \frac{2^9 + 1}{3} = 171$, $2^9 + 1$ having, besides the obligatory factor $2^3 + 1$ due to its algebraical form, the *two* factors 3 and 19.

Taking each divisor of 171, namely 3, 9, 19, 57, 171, we see that the 3rd, 9th, 19th, 57th, and 171th sub-derivatives of the nine points of inflexion will each of them be an apex of an in-and-exscribed nonagon. Of these, the 3rd sub-derivatives, and they only, give improper solutions of the problem, they being the apices of the in-and-exscribed triangles. Hence the aggregate of proper apices and the corresponding nonagons separate into four distinct groups, corresponding to the primitive sub-derivatives of the 9th, 19th, 57th, and 171th grades respectively, of the inflexions. The number of the nonagons belonging to the several groups will be the quadritotients of 9, 19, 57, 171, that is $9^2 - 9$, $19^2 - 1$, $(19^2 - 1)(3^2 - 1)$, $(9^2 - 9)(19^2 - 1)$ respectively, that is $171^2 - 9$, exactly the same as if 57 had been a prime number N, in which case the $(3N)^2$ sub-derivatives of an inflexion of the grade $3N$ would be subject to the deduction of $9 - 1$ for in-and-exscribed triangles, and 1 for the point itself.

To make more clear the distinct solutions of which the problem of in-and-exscription of a k-lateral in general admits, consider the case of $k = 8$. Here

$$i = \frac{2^8 - 1}{3} = \frac{2^4 - 1}{3}(2^4 + 1) = 85.$$

The first factor (the one algebraically contained in i) is 5 and the primitive algebraical factor is 17. The total number of octagonal apices

* It is obvious that any derivative of an inflexion is itself an inflexion. For instance, if J is an inflexion, J_2 is the same as J, and J_3 (namely, J', J_2) is either J, J_2, that is J, or (I, J), J_2, that is, (I, J), J, that is, I (I being some other point of inflexion). Hence if P_δ is an inflexion, P_δ is also an inflexion.

will be $9(85^2-5^2)$, the number 5^2 corresponding to the points of inflexion and the in-and-exscribed quadrilaterals. These 255^2-15^2 apices will consist of points of the form $I_{\frac{1}{17}}$ and $I_{\frac{1}{85}}$, the number of the former being $9(17^2-1)$ and of the latter $9(17^2-1)(15^2-1)$.

It is easily seen that, in general, the number of apices of in-and-exscribed k-laterals is nine times the *functional totient* of $\left(\frac{2^k-\overline{1}^k}{3}\right)^2$, or, what is the same thing the number of apices is the functional totient of $(2^k-\overline{1}^k)^2$, as previously stated in Note to Proem in the last number of the *Journal**; the number of k-laterals is, of course, the number of apices divided by k. For instance, we thus have for the number of apices of quindecagons, nonagons, and octagons, respectively,

$$(2^{15}+1)^2-(2^3+1)^2-(2^5+1)^2+(2^1+1)^2,$$
$$(2^9+1)^2-(2^3+1)^2,\ (2^8-1)^2-(2^4-1)^2,$$

as found above.

Since i is odd, every divisor of i will necessarily be so too. Conversely, it is easy to prove that every odd sub-derivative of a point of inflexion is an apex of an in-and-exscribed polygon, and to determine the number of its sides. For let i, any odd number, be given, and let k be the least number which will satisfy the condition that $2^k-\overline{1}^k$ shall be a multiple of $3i$, then the sub-inflexions of the ith grade will be the apices of an in-and-exscribed k-lateral. I give, in the annexed table, the values of k corresponding to a given value of i, which, of course, are unique; whereas to a given value of k, in general, several values of i will correspond.

i	3	5	7	9	11	13	15	17	19	21	23	25	27
k	3	4	6	9	5	12	12	8	9	6	22	20	27

to which may be subjoined the reciprocal table

$k=3$ $\quad i=3$
$k=4$ $\quad i=5$
$k=5$ $\quad i=11$
$k=6$ $\quad i=7, 21$
$k=7$ $\quad i=43$
$k=8$ $\quad i=17, 85$
$k=9$ $\quad i=9, 19, 57, 171$
$k=10$ $\quad i=31, 341$
$k=11$ $\quad i=683$
$k=12$ $\quad i=13, 15, 35, 39, 65, 91, 195, 273, 455, 1365.$

[* See p. 345 above.]

To illustrate the way in which this table is formed, take the case of $k=12$; then $\frac{2^{12}-1}{3}=3.5.7\times 13$ where 3 belongs to $k=3$, 5 to $k=4$, 7 to $k=6$; the values of i are found by taking the divisors of 1365, except those which are found set against $k=3$, $k=4$, $k=6$, that is 3, 5, 7, 21.

The successive tangentials of any even-graded inflexional sub-derivative as $2^q i$, where i is odd, will evidently consist of a chain of q points attached to the ring formed by the apices of an in-and-exscribed polygon of k sides, where k is the least number which makes $2^k \pm 1$ divisible by $3i$.

In all cases (since k is to have the minimum value which makes $\frac{2^k \pm 1}{3}$ contain i) $2k$ must be $\tau(3i)$ or a submultiple of it, so that, if $i=3^q j$, k is either $3^q \tau j$ or a submultiple of it; when $i=3^q$, since the cyclotomic functions of the first species $\chi_3\, 2$, $\chi_{3^2}\, 2, \ldots \chi_{3^q}\, 2$ can only contain the first power of the intrinsic divisor 3, it follows that $k=3^q=i$, as is seen in the table to be the case for $i=3$, 9, 27; or, in other words, a 3^qth sub-derivative of a point of inflexion is an apex of an in-and-exscribed polygon of 3^q sides.

It may be as well to mention again here, by way of a remind, that the number of in-and-exscribed k-laterals whose apices are ith sub-derivatives of the inflexions, is always the kth part of nine times the quadritotient of i; when $i=3^q$ this number will be $\frac{1}{3^{q-2}}\{3^{2q}-3^{2q-2}\}$, that is $3^{q+2}-3^q$, being thus 24, 72, 216, etc., for triangles, nonagons, eikosiheptagons, etc.

Title 5.—*An Exact Proof of the Scalar Law of Squares**.

I will now give an exact proof of the law that the order in the variables of P_n is n^2 in regard to the co-ordinates of P, and furthermore that the co-ordinates when $i=3m\pm 1$ are of the form xU, yV, zW, and when $i=3m$ are of the form M, N, $xyz\Omega$; x, y, z being the co-ordinates of the primitive P_1 and U, V, W, M, N, Ω quantics in x^3, y^3, z^3. Of course the order of a point means the order of its system of co-ordinates *expressed in its lowest terms*, that is to say when the values of the three co-ordinates have no common measure, and consequently the co-ordinates of any *two* of them are relatively prime in an algebraical sense, as follows from the equation

$$X^3+Y^3+Z^3+kXYZ=0.$$

The law to be established comprises, it will be seen, two elements,—one numerical, the *rule of squares;* the other formal, containing two rules, one regarding the *distribution* of x, y, z between the co-ordinates, the other the quanticity of the parts not multiplied by x, y, z or xyz in respect to x^3, y^3, z^3.

Let us suppose that the law is true up to n inclusive. I shall show that it is true up to $2n$ inclusive.

[* See below, p. 385.]

(1) For the case of $2i$ where $i \gtreqless n$.

Let X, Y, Z be the system of co-ordinates to P_i in its lowest terms; then, by the law of compound derivation, P_{2i} is

$$X(Y^3 - Z^3),\ Y(Z^3 - X^3),\ Z(X^3 - Y^3).$$

If these regarded as functions of X, Y, Z had any common measure X, Y or X, $Z^3 - X^3$ would have a common measure. Hence X, Y, Z would all have a common measure. Nor can they have any common factor F, a function of x, y, z. For in that case, when $F = 0$, we should have

$$Y^3 - Z^3 = 0,\ Z^3 - X^3 = 0 \text{ or } X^3 = Y^3 = Z^3,$$

and the arbitrary parameter k would be $-3.1^{\frac{1}{3}}$, so that the cubic would become a triplet of straight lines, a supposition which falls outside the pale of the question.

Hence P_{2i} will be of four times the order of P_i, and therefore, by hypothesis, of the order $4i^2$, that is, $(2i)^2$. Also, obviously, the form xU, yV, zW or M, N, $xyz\Omega$ (as the case may be) which exists for i is maintained for $2i$, which is or is not divisible by 3 according as i is or is not so divisible.

(2) Let the index be any odd number less than $2n$.

I shall first establish a Lemma concerning the co-ordinates given by my formulæ for the connectives of P, Q and P', Q, where P' is the opposite to P in respect to a given point of inflexion (say $x = 1$, $y = -1$), and

$$x^3 + y^3 + z^3 + kxyz = 0$$

is the equation to the cubic.

The connectives of (u, v, w) and (u', v', w') of (v, u, w) (u', v', w')

are represented respectively by

$$\left.\begin{matrix} vwu'^2 - v'w'u^2 \\ wuv'^2 - w'u'v^2 \\ uvw'^2 - u'v'w^2 \end{matrix}\right\} \text{ and } \left\{\begin{matrix} uwu'^2 - v'w'v^2 \\ wvv'^2 - w'u'u^2 \\ vuw'^2 - u'v'w^2, \end{matrix}\right.$$

the 3rd co-ordinate being the same in both systems, which, of course, remain to be reduced to their simplest terms, being at present each of the order $2i^2 + 2j^2$.

I say that the same quantity F cannot divide each of the two sets of quantities when u, v, w; u', v', w' are derivatives, one of an even, the other of an odd grade of the same point on the cubic.

For, if so, let $F = 0$; then each quantity in the two systems becomes zero.

Call $\frac{u}{w}, \frac{v}{w}; \frac{u'}{w'}, \frac{v'}{w'}$, r, s; r', s' respectively.

Then $(1).....sr'^2 - s'r^2 = 0 \qquad rr'^2 - s's^2 = 0.....(3)$

$(2).....rs'^2 - r's^2 = 0 \qquad r'r^2 - ss'^2 = 0.....(4)$

$(5).....rs = r's'.$

Writing $r^3 = R$, $s^3 = S$, $r'^3 = R'$, $s'^3 = S'$; 5, (3, 4), (1, 2) respectively give $RS = R'S'$, $RR' = SS'$, $R'S = RS'$. The second and third of these combined give $R^2 = S^2$, $R'^2 = S'^2$ and the first and second combined give $R'^2 = S^2$. Hence, $R^2 = R'^2 = S^2 = S'^2$, and consequently the original equations (1), (2), (3) give $S = S'$, $R = R'$, $R = S'$ or $r^3 = s^3 = r'^3 = s'^3$.

Let $r = \alpha s$, $r' = \beta s'$, $s = \gamma s'$. Then $\alpha^3 = \beta^3 = \gamma^3 = 1$, and all the equations (1), (2), (3), (4), (5) will easily be found to be satisfied when (and only when) $\alpha = \beta\gamma$.

The equations $r^3 = s^3$, $r'^3 = s'^3$, that is, $u^3 = v^3$, $u'^3 = v'^3$, imply that the points P, Q are two either distinct or identical anti-tangentials to the same point of inflexion $x = 1$, $y = -1$. I say that this is impossible when P, Q are derivatives of the degrees i, j of the same point U on the curve, if $i + j$ is an odd number. It must be noticed that P and Q (two Plückerian points belonging to the same point of inflexion I) are identical with P' and Q' respectively.

Any even-degreed derivative of P or Q is I, and any odd-degreed derivative is the same point P or Q over again.

Let now $i\mu - j\nu = 1$. Then $U = U_{i\mu - j\nu}$ will be (without regard to the modulus 3) the connective of $U_{i\mu}$ and $U_{j\nu}$, because we may substitute at will U_i' for U_i and U_j' for U_j. But $U_{i\mu}$ and $U_{j\nu}$, if μ, ν be both odd, will be U_i and U_j over again, or if μ, ν be one odd and the other even, will be I and one of the two Plückerian points.

Hence U is the connective of I and a Plückerian point, or else of two Plückerians which are identical, or of two Plückerians (both appurtenant to I) which are distinct.

In the 1st and 3rd cases, then, U is a Plückerian, in the 2nd case a point of inflexion. But every derivative of a point of inflexion is a point of inflexion, and every even-degreed derivative of a Plückerian is also a point of inflexion; but by hypothesis (since one of the two numbers i, j is even) an even-degreed derivative of U is a Plückerian, which is self-contradictory. Hence, it follows that the expressions given by *my* formulæ for the connectives of P_i, P_j and P_i', P_j when $i + j$ is odd, say P, Q, R; P', Q', R', cannot have a common factor; so that if M is a common measure of P, Q, R and M' of P', Q', R', M is relatively prime to M'.

Let ϕ, ψ, ω be always understood to mean $\phi(x^3, y^3, z^3)$, $\psi(x^3, y^3, z^3)$, $\omega(x^3, y^3, z^3)$; let (μ), (ν) be understood to mean the prime systems of coordinates u, v, w; u', v', w' which represent μ, ν (μ and ν being numbers,

accented or unaccented, representing derivatives to the indices μ and ν); let $[\mu, \nu]$ represent the unreduced system of the co-ordinates of the connective of μ, ν, namely, $v'w'u^2 - vwu'^2$, $w'u'v^2 - wuv'^2$, $u'v'w^2 - uvw'^2$; (μ, ν) the above system *reduced* by elimination of the greatest common measure of its terms.

If (μ), (ν) are each of the form $x\phi$, $y\psi$, $z\omega$, $[\mu, \nu]$ is of the form $x^2yz\phi_1$, $xy^2z\psi_1$, $xyz^2\omega_1$, but $[\mu', \nu]$, that is, the unreduced connective of $y\psi$, $x\phi$, $z\omega$; $x\phi'$, $y\psi'$, $z\omega'$, is of the form $z\phi_1$, $z\psi_1$, $xyz^2\omega_1$.

Again, if (μ) is of the form $x\phi$, $y\psi$, $z\omega$ and (ν) of the form ϕ_1, ψ_1, $xyz\omega_1$, $[\mu', \nu]$, the unreduced connective of the systems $y\psi$, $x\phi$, $z\omega$ and ϕ_1, ψ_1, $xyz\omega_1$, is easily seen to be of the form $zx\Phi$, $zy\Psi$, $z^2\Omega$.

Furthermore, the order in the variables of (p') is obviously the same as that of (p).

Now it has been shown under Title 2 that

$6i-1=(3i-1)'$, $3i$ $\quad$ $6i-5=(3i-3)'$, $(3i-2)'$ $\quad$ $6i-3=(3i-2)'$, $3i-1$.

If, then, $(3i)$ and $(3i-3)$* are of the form ϕ, ψ, $xyz\omega$, and $(3i-2)$, $(3i-1)$ each of the form $x\phi$, $y\psi$, $z\omega$, it follows that $[6i-1]$ and $[6i-5]$ will be of the form $zx\phi$, $zy\psi$, $z^2\omega$, and $[6i-3]$ of the form $z\phi$, $z\psi$, $xyz^2\omega$.

The above inference suffices to show that, if, for all values of $3\mu \pm 1$ and 3μ up to n inclusive, it be true that $(3\mu \pm 1)$ is of the form $x\phi$, $y\psi$, $z\omega$ and of the order $(3\mu \pm 1)^2$, and (3μ) is of the form ϕ, ψ, $xyz\omega$ and of the order $(3\mu)^2$; then the same will be true up to $2n$ inclusive.

That this is true for even values not exceeding $2n$ appears from what has been already shown. Confining, then, our attention to odd numbers less than $2n$; these must be representable by $6i-5$, $6i-3$ or $6i-1$, and by hypothesis the form of each of the systems $(3i)$, $(3i-1)$, $(3i-2)$, $(3i-3)$ fulfils the conditions of the last paragraph but one; consequently the form of $[6i-5]$, $[6i-3]$, $[6i-1]$ will be $zx\phi$, $zy\psi$, $z^2\omega$; $z\phi$, $z\psi$, $xyz^2\omega$; $zx\phi$, $zy\psi$, $z^2\omega$, namely, in every case the factor z will be contained in each term of the system $[(\iota-1)', \iota^?]$, which represents an unreduced system of co-ordinates of the point $2\iota-1$, the mark of interrogation signifying a blank or an accent as the case may be.

But either the point 1 or the point 1′ will, in every case, correspond to the connective obtained by changing $(\iota-1)'$ into $\iota-1$†; moreover, the unreduced system of co-ordinates to that connective will have the third term, say π, in common with the unreduced system to $2\iota-1$ above mentioned.

This contrary system we know must have the common factor $\frac{\pi}{z}$ because 1

* $(3i-3)'$ will obviously be of the same form as $3i-3$.

† For, on consulting Title 2, it will be found that *in every case*, if the arithmetical value of the index of P_i, P_j is $i \neq j$, that of P_i', P_j is $(\iota \mp j)^?$.

and 1′ are denoted by x, y, z; y, x, z respectively. Hence the unreduced system for $2\iota - 1$ can have no other common factor except z, which they have been shown to have; since, were it otherwise, the *two* contrary systems would have some quantity contained in $\frac{\pi}{z}$ for a joint common measure, which has been proved to be impossible.

Hence, the form of $(2\iota - 1)$ is $x\phi$, $y\psi$, $z\omega$ or $\phi, \psi, xyz\omega$ according as $2\iota - 1$ is not or is divisible by 3, and its order is in all cases $2(\iota - 1)^2 + 2\iota^2 - 1$, that is, $(2\iota - 1)^2$.

Hence the form-law of distribution of the simple powers of the variables x, y, z and of the quanticity in x^3, y^3, z^3 of the multipliers of x, y, z or of 1, 1, xyz, as well as the numerical law that the order of any derivative is the square of its index, will be true up to $2n$ inclusive if true up to n inclusive; and being true for $n = 1$, is true universally.

As a corollary we may now do away with the restriction of $i + j$ being odd, and affirm that in all cases (the futile one of $i = j$ alone excepted), if the reduced system of co-ordinates to the connective of P_i, P_j be F, G, H, and to that of P_i', P_j be F', G', H', then the unreduced system expressing those connectives given by my formulæ of connection will be $H'F$, $H'G$, $H'H$; HF', HG', HH', respectively; for the two systems of unreduced co-ordinates (each of the order $2i^2 + 2j^2$) contain, one of them a common factor of the order $(2i^2 + 2j^2) - (i - j)^2$, that is, $(i + j)^2$, the other a common factor of the order $(2i^2 + 2j^2) - (i + j)^2$, that is, $(i - j)^2$, and these two factors being prime to each other, their product must be contained in the term common to the two systems, and being of the same order $(i + j)^2 + (i - j)^2$ as that common term, must be equal to it.

Hence, if π be the common unreduced term, and H, H' the two reduced terms, we must have $\pi = \frac{\pi}{H} \cdot \frac{\pi}{H'}$ or $\pi = HH'$, as was to be shown.

As a matter rather of curiosity than of real importance I will state the analogous law when the connective and cross-connective between two derivatives is expressed by Cauchy's formulæ instead of my own. These formulæ, it will be remembered, give for the co-ordinates of the connective of u, v, w; u_1, v_1, w_1 the minor determinants of the matrix

$$\begin{vmatrix} vw_1 - v_1w\,; & w_1u - wu_1\,; & uv_1 - u_1v \\ uu_1 & ; \quad vv_1 & ; \quad ww_1 \end{vmatrix}$$

If, now, the prime system of co-ordinates to the connectives of P_i, P_j; P_i', P_j be denoted as before by F, G, H; F', G', H', I find by calculation that the Cauchian formulæ will present these two systems under the unreduced forms

$$(F' + G')F, \quad (F' + G')G, \quad (F' + G')H$$
$$(F + G)F', \quad (F + G)G', \quad (F + G)H',$$

between which there is no common term; and consequently, had I not discovered my own simpler formulæ, the method of proof of the Law of Squares which I have employed would have been inapplicable, and it is not easy to see what other strict method of proof could have taken its place.

I have thus accomplished the very difficult task of proving a negative, in this instance the non-existence of *latent* common factors to the co-ordinates of the connective of any two given derivatives. I might have founded a much easier proof of the Law of Squares upon Mr Franklin's geometrical solution of the problem of finding the number of in-and-exscribed k-laterals to a cubic (if one could feel quite assured *à priori* of the strict logic of the process*) as follows: He has virtually found (*vide* last number of the *Journal*) that the number of apices of the in-and-exscribed k-laterals of *every kind* [and not excluding the points of inflexion] is $(2^k - \overline{1}^k)^2$. If, then, $2^k - \overline{1}^k = 3i$, it follows from what has been shown in the preceding pages, that the order of P_i in the co-ordinates of P is $\frac{1}{9}(3i)^2$, that is, i^2.

Let now i' be any number whatever, and τ the totient of $3i'$; then τ is even, and, by Fermat's Theorem, $2^\tau - \overline{1}^\tau = 3i'i''$.

Hence, if μ', μ'' are the orders of $P_{i'}, P_{i''}$ respectively, the law of compound derivation will suffice to lead to the conclusion that $\mu'\mu''$ will be the order of $P_{i'i''}$, and accordingly $\mu'\mu'' = i'^2 i''^2$; but $\frac{\mu'}{i'^2}, \frac{\mu''}{i''^2}$, it has been proved under a preceding Title, are neither of them greater than unity: hence each of them is equal to unity, and i'^2 is the order of $P_{i'}$, as was to be shown.

Addendum on the Degorder of the Derivatives to a Point on a Cubic in the Natural Scale.

Let n be any number not divisible by 3. The nth derivative, it has been proved, is of the order n^2 in the variables. It remains to determine its *degree in the coefficients.*

When $n = 2$ we know that the degorder is [4; 4], each new co-ordinate being one of the minors of the rectangular matrix

$$\begin{vmatrix} \frac{dU}{dx} & \frac{dU}{dy} & \frac{dU}{dz} \\ \frac{dH}{dx} & \frac{dH}{dy} & \frac{dH}{dz} \end{vmatrix},$$

where U is the cubic and H its Hessian.

* In that solution the apices are found as the intersections of the cubic with another curve. Certain of these intersections are seen from geometrical considerations to count twice, and others three times; but while we have no reason to suppose any further cause of reduction, the non-existence of such cause is not proved.—F. F.

Suppose ν to be the degree in the coefficients of the nth derivative. Then the degree of the $(2n)$th derivative regarded as the second of the nth will be $4\nu + 4$, and regarded as the nth of the second will be $n^2 . 4 + \nu$, and these two must be equal. Hence $3\nu = (n^2 - 1)\,4$ or $\nu = \frac{4}{3}(n^2 - 1)$.

Hence the degorder of any nth derivative in the natural scale is $\left[\frac{4n^2 - 4}{3};\ n^2\right]$. If we substitute the co-ordinates of this derivative in the given cubic U, the result must be of the form $U . R$ and will be of the degorder $[1 + 4n^2 - 4;\ 3n^2]$. Hence R is of the degorder $[4n^2 - 4;\ 3n^2 - 3]$. If the well-known covariant of the degorder $[12;\ 9]$ be called J, R is of the same degorder as $J^{\frac{n^2-1}{3}}$, and possibly may be found to be identical with it. To corroborate the validity of the determination of the degorder of the nth derivative, we may proceed as follows:

Imagine, at first, the cubic to be reduced to the canonical form $x^3 + y^3 + z^3 - 3kxyz$. The connective of P_1, P_2 in its reduced form is x, y, z; but in its unreduced form and prior to all simplification, will, by virtue of the theory (Titles 1 and 5), be of the form Mx, My, Mz where

$$M = x^3y^6 + y^3z^6 + z^3x^6 + x^6y^3 + y^6z^3 + z^6x^3 - 6x^3y^3z^3$$
$$+ kxyz\,(x^6 + y^6 + z^6 - y^3z^3 - z^3x^3 - x^3y^3)^*;$$

consequently M expressed (as I shall hereafter suppose) in terms of the original coefficients and variables, will be of the degorder $[9;\ 9]$: for Mx, My, Mz are of the degorder $[1 + 2 . 4;\ 2(1 + 4)]$, that is, $[9;\ 10]$†. Also the degorder of P_4 will be $[4 + 4 . 4;\ 16]$, that is, $[20;\ 16]$.

Suppose now we wish to find the degorder of P_5.

The unreduced connective of P_1, P_4 will be of the form MX, MY, MZ, where X, Y, Z are the reduced co-ordinates and M is exactly the same thing as before. The degorder of the unreduced co-ordinates will be $[1 + 2 . 20;\ 2(1 + 16)]$, that is, $[41;\ 34]$; and consequently, subtracting $[9;\ 9]$, the degorder of X, Y, Z will be $[32;\ 25]$, that is, $\left[4\frac{5^2 - 1}{3};\ 5^2\right]$.

So, again, to find P_7 we may regard it as the connective of P_2, P_5. The unreduced degorder of P_7 will thus be seen to be $[1 + 2(4 + 32);\ 2(4 + 25)]$, that is, $[73;\ 58]$, and subtracting, as before, $[9;\ 9]$, the degorder of the

* It is worthy of remark that, if we make $U = 0$, so that $3kxyz$ becomes equal to $x^3 + y^3 + z^3$, the expression in the text for M gives $3M$ equal to the norm of $x + 1^{\frac{1}{3}}y + 1^{\frac{2}{3}}z$, namely,

$$(x^3 + y^3 + z^3)^3 - 27x^3y^3z^3.$$

† In fact, M, as may easily be shown, is the covariant $\left[\Sigma\left(\frac{dU}{dy} \cdot \frac{dH}{dz} - \frac{dU}{dz} \cdot \frac{dH}{dy}\right)\frac{d}{dx}\right]^2 U$, in other words the symmetrical determinant of the 5th order formed by double-bordering the Hessian matrix with the differential derivatives of the Hessian and of the original cubic.

reduced co-ordinates of P_7 becomes [64; 49], that is, $\left[4\frac{7^2-1}{3}; 7^2\right]$, agreeable to what has been previously found; and so, in general, supposing the degrees of P_μ and $P_{\mu+3}$ in the coefficients to be $4\frac{\mu^2-1}{3}$ and $4\frac{(\mu+3)^2-1}{3}$, the unreduced degree of $P_{2\mu+3}$ will be $1+8\left\{\frac{\mu^2-1}{3}+\frac{(\mu+3)^2-1}{3}\right\}$, from which subtracting 9, the reduced degree becomes $8\left\{\frac{2\mu^2+6\mu+4}{3}\right\}$, which is the same thing as $4\left\{\frac{(2\mu+3)^2-1}{3}\right\}$, as ought to be the case. There is, therefore, no loophole for doubt left open as regards the degorder of any *natural* derivative to the index k (a number necessarily of the form $3i \pm 1$) being $[\frac{4}{3}(k^2-1); k^2]$, a notable result!

We are now in possession of a method for finding any natural derivative to the index n. If n is even, it may be derived immediately from the derivative to the index $\frac{n}{2}$. If n is odd, it must be of the form $2\mu+3$ where μ is not divisible by 3.

Taking P as the initial point, P_μ and $P_{\mu+3}$ may be considered as known. Calling their co-ordinates X, Y, Z; X_1, Y_1, Z_1 respectively, and substituting $\lambda X+\mu X_1, \lambda Y+\mu Y_1, \lambda Z+\mu Z_1$ in the equation to the cubic, we shall obtain an equation of the form $\lambda^2\mu B+\lambda\mu^2 C=0$. The unreduced co-ordinates of $P_{2\mu+3}$ will then be $CX-BX_1$, $CY-BY_1$, $CZ-BZ_1$, which will contain a common measure M of the degorder [9; 9], and $\frac{CX-BX_1}{M}$, $\frac{CY-BY_1}{M}$, $\frac{CZ-BZ_1}{M}$ will be the expression for the point $P_{2\mu+3}$ in its simplest terms.

More generally, if $n=2\mu+3i$, we may obtain, in like manner as above, the unreduced co-ordinates of the connective to P_μ, $P_{\mu+3i}$, and, by an easy calculation, it will be found that the new common measure will be of the degorder $[12i^2-3; 9i^2]$, and will be constant, that is, independent of μ for any given value of i, and identical with the common measure to the unreduced co-ordinates of P_{3i+2} regarded as the connective to P and P_{3i+1}.

It is well worthy of remark that if X, Y, Z be the co-ordinates of any derivative, and ξ, η, ζ contragredient to x, y, z, $X\xi+Y\eta+Z\zeta$ will be an invariantive concomitant to the given cubic. This gives rise to a new series of reflexions, the development of which must be deferred to a more convenient occasion*.

* It is obviously a step towards the attainment of the desideratum of finding the general expression for any derivative in an explicit form, or, at all events, by explicit processes and without the necessity for division of the unreduced co-ordinates by a common measure. This latter, it should be observed however, by virtue of what is stated above, is always known *à priori*.

CHAPTER I.

Excursus C.—On the Trisection and Quartisection of the Roots of Unity to a Prime-Number Index.

What follows, so far as it relates to the trisection of the primitive roots of unity, may be regarded as auxiliary to Postscriptum 2, [p. 345, above], inasmuch as it establishes the equation in ω which, when $x = \frac{\omega - 1}{3}$, becomes the equation there assumed. The rest is episodical, except so far as it may be regarded as correlative to the subject matter of Titles 1 and 2 of Excursus A* [pp. 317 ff.].

It will be seen that the equations to a system of three and four periods, usually obtained by long and tedious processes, may, with the aid of one simple and well-known principle, be deduced by processes almost elementary in their character, and into which enter no algebraical calculations except of the very easiest kind.

A sketch of the method was laid by me before the Scientific Congress held at Rheims in the month of August last [p. 438, below].

The index p of the roots is, as usual, supposed to be a prime number; e is the number of the periods, f the number of roots whose sum forms a period, so that $ef = p - 1$; the periods themselves will be called η, namely, $\eta_1, \eta_2, \cdots \eta_e$.

Preliminaries.

1. I say, in the first place, that the sum of the ith powers of the periods will be congruous to $-f^{i-1}$ in respect to the modulus p.

For, were it not that in the development of the ith power of any one of the η's some of the combinations of the powers of the roots were unity, it is obvious that we should have $\Sigma\eta^i = -ef^i \div (p-1)$, that is, $-f^{i-1}$, and that we might regard every term in such development as equivalent to $-\frac{1}{p-1}$, without affecting this result. The existence of terms equal to unity will render it necessary to substitute for any such term 1 instead of $-\frac{1}{p-1}$, in order to obtain a correct result, and if there be N of them, the correction to be introduced will be $N\left(1 + \frac{1}{p-1}\right)$, that is, $\frac{N}{p-1} \cdot p$; but as it is obvious that the result must be an integer, it follows that N must be double by

* In any future redistribution of the contents of the entire memoir, it would be proper to incorporate the matter contained in Postscriptum 2, pp. [345—347], with this Excursus.

$(p-1)$, and consequently the value of $\Sigma\eta^i$ *to modulus* p will be $-f^{i-1}$, that is, $-\left(\frac{p-1}{e}\right)^{i-1}$, as was to be shown.

2. From the above it follows that *to modulus* p,

$$\Sigma(e\eta+1)^i \equiv (-1)^i + e(-1)^{i-1} + e\frac{e-1}{2}(-1)^{i-2} + \text{etc.}, \equiv (-1+1)^e \equiv 0,$$

or, in other words, $\Sigma(e\eta+1)^i$ is divisible by p.

But, if s_i and σ_i represent, respectively, the sum of the $i$ary combinations and $i$ary powers of the roots of an equation, we know that $(-)^i s_i =$ coefficient of x^i in $e^{-\sigma_1 x - \frac{\sigma_2}{2}x^2 - \frac{\sigma_3}{3}x^3 \ldots}$, so that s_i multiplied by numbers none exceeding i, is expressible as the sum of integer multiples of $\sigma_\lambda \sigma_\mu \sigma_\nu \ldots$ where

$$\lambda + \mu + \nu + \ldots = i.$$

3. Consequently, s_i multiplied by integers none greater than i, when the roots in question are the e values of $e\eta+1$ and $i>0$, will be divisible by p, and consequently, since e is less than p, all the coefficients of the equation to which those roots appertain will be divisible by p, the first, of course (which is unity), excepted.

Since $\Sigma(e\eta+1) = e\Sigma\eta + e = 0$, the equation whose roots are $\omega_1, \omega_2, \ldots \omega_e$ where $\omega = e\eta+1$ will be of the form $\omega^e + P\omega^{e-2} + Q\omega^{e-3} +$ etc., where P, Q, etc., each contain p; and I may remark, incidentally (although the fact is immaterial to the object in view), that, as may easily be seen, $\Sigma\omega^i$ will be divisible not only by p but also by e, and that consequently the coefficient of ω^{e-i}, in the above equation, will contain the greatest common divisor to e and i.

4. The coefficient P has one or the other of two determinate algebraical values according as f, that is, $\frac{p-1}{e}$, is even or odd.

In the former case, the congruence $x^e + 1 \equiv 0 \pmod{p}$ is soluble, and in the latter, insoluble. Accordingly, in the latter case, we shall have $\Sigma\eta^2 = -f$, and in the former $\Sigma\eta^2 = p-f$, and in each case $\Sigma\eta^2$ will be an odd number. Also, when f is odd (which involves the necessity of e being even)

$$\Sigma\omega^2 = \Sigma(e\eta+1)^2 = -e^2\frac{p-1}{e} - 2e + e = -ep,$$

and when f is even $\Sigma\omega^2$ will be this result augmented by e^2p, that is, $(e^2-e)p$.

Consequently, $P = \frac{e}{2}p$, or $= -\frac{e^2-e}{2}p$, according as f is odd or even.

Thus, when $e = 3$, f being necessarily even, $P = -3p$, and when $e = 4$, $P = -6p$, or $= 2p$, according as $\frac{p-1}{4}$ is even or odd*.

5. With regard to what immediately follows it will also be necessary to determine the *form* of Q in respect to certain moduli for the cases of e equal to 3 and e equal to 4. In the former case

$$\Sigma\omega^3 = \Sigma(e\eta + 1)^3 = \Sigma(e^3\eta^3 + 3e^2\eta^2 + 3e\eta + 1) \equiv 3 \bmod 9,$$

and consequently, since $Q = -\frac{1}{3}\Sigma\omega^3$, $-3Q \equiv 3 \bmod 9$ and $-Q \equiv 1 \bmod 3$.

In the latter case, that is, when $e = 4$, since $\Sigma\eta^2$ is always odd $\Sigma\omega^3$ [to mod 32] $\equiv 16 - 12 + 4$, that is, $\equiv 8$, and, consequently, $-3Q \equiv 8$ to that modulus.

These *preliminaries* being established, I will now proceed to state the principle referred to in the exordium.

Principle.

A rational integer function of any set of periods of the roots of unity whose coefficients are all whole numbers, which does not change its value for a circular substitution executed upon the periods, it is well-known, must be an integer number; but to this I add that if such function, without changing its arithmetical value, undergoes a change of sign when such a substitution is made, it must necessarily be an integer number multiplied by the difference of the two periods into which the entire sum of the roots may be divided, that is to say, will be a multiple of $\sqrt{p}$, when p is of the form $4K + 1$ and of $\sqrt{(-p)}$, when p is of the form $4K - 1$†.

As an example, the product of the differences of the roots of the equation in η will be an integer number when e, the number of the periods, is odd, and an integer number multiple of $\sqrt{p}$ or $\sqrt{(-p)}$ (according as $\frac{p-1}{2}$ is even or odd), when the number of periods is even. As another example, if $e = 2\epsilon$, the function

$$(\eta_0 - \eta_\epsilon)(\eta_1 - \eta_{\epsilon+1})(\eta_2 - \eta_{\epsilon+2}) \dots (\eta_{\epsilon-1} - \eta_{2\epsilon-1}),$$

which changes its sign but not its quantitative value, when 0, 1, 2, 3, ... $(2\epsilon - 1)$ are replaced by 1, 2, 3, ... -1, 0 will be an integer multiple of $\sqrt{p}$, or of $\sqrt{(-p)}$, according as ϵ is even or odd.

* When $e = 2$, $P = p$ or $-p$ according as f is odd or even, so that the equation in ω takes the known form $\omega^2 \pm p = 0$.

† To put the matter more clearly, call the alternating function F and the difference spoken of Δ. Then ΔF is invariable in sign as well as in magnitude for the circular substitutions in question. Hence $F = \frac{\text{An Integer}}{\sqrt{(\pm p)}}$ but F^2 is an Integer; therefore $F = \text{An Integer } \sqrt{(\pm p)}$. Q.E.D.

We are now in a position to obtain without difficulty the well-known equivalent to the equation corresponding to $e = 3$, given at p. [345], and the corresponding pair of equations for the case of $e = 4$.

A. *Case of* $e = 3$.

The equation in ω, from what has been shown in the preliminaries, must be of the form $\omega^3 - 3px + pq = 0$, and it only remains to determine q.

The discriminant of the above equation being $q^2p^2 - 4p^3$, it follows that the product of the differences of its roots will be $27(4p^3 - q^2p^2)$. But this product is 3^6 into $(\eta_0 - \eta_1)^2(\eta_0 - \eta_2)^2(\eta_1 - \eta_2)^2$, which latter, by the *principle*, is of the form M^2. We have, therefore,

$$4p^3 - q^2p^2 = 27M^2 = 27m^2p^2.$$

Hence,
$$4p = q^2 + 27m^2,$$

which serves to determine the value of q^2 absolutely.

To find the value of q, it follows from the preliminaries that $qp \equiv -1 \bmod 3$, and, consequently, since $p \equiv 1 \bmod 3$, $q \equiv -1 \bmod 3$, so that q is perfectly determined.

B. *Case of* $e = 4$.

$\omega^2 - 2\sqrt{p}\omega + R = 0$, $\omega^2 + 2\sqrt{p}\omega + R' = 0$, will be the form of the equations containing, respectively, the pairs of roots ω_0, ω_2 and ω_1, ω_3; for

$$\omega_0 + \omega_2 = (4\eta_0 + 1) + (4\eta_2 + 1) = 2\{2(\eta_0 + \eta_2) + 1\} = 2(2\delta_0 + 1),$$

and, similarly,

$$\omega_1 + \omega_3 = 2\{2(\eta_1 + \eta_3) + 1\} = 2(2\delta_1 + 1)$$

where δ_0 and δ_1 are the two periods which make up together the sum of all the roots, so that $2\delta_0 + 1$ and $2\delta_1 + 1$ are the roots of the equation $\Omega^2 - p = 0$, the sign of the last term being fixed from the fact of $\frac{p-1}{2}$ being by hypothesis even.

Furthermore, R, R' must be of the form $Ap + B\sqrt{p}$, $Ap - B\sqrt{p}$; for $(R - R')\sqrt{p}$, being integer, requires that R, R' shall be of the form $A_1 + B\sqrt{p}$, $A_1 - B\sqrt{p}$, and then RR' being an integer multiple of p involves the necessity of A_1^2, and therefore of A_1 containing p.

The product $(\eta_0 - \eta_2)(\eta_1 - \eta_3)$ consequently becomes

$$\{(A-1)p + B\sqrt{p}\}\{(A-1)p - B\sqrt{p}\},$$

which by the principle must be of the form m^2p, and consequently,

$$(A-1)^2p - B^2 = C^2 \text{ or } (A-1)^2p = B^2 + C^2.$$

The coefficient of ω^2 becomes $-4p+2Ap$ which, by the preliminaries, when $\frac{p-1}{4}$ is even must be equal to $-6p$, so that $A=-1$, and when $\frac{p-1}{4}$ is odd must be equal to $2p$, so that $A=3$.

In each case, therefore, $(A-1)^2=4$ and $4p=B^2+C^2$; consequently, if $p=g^2+h^2$, $4g^2=B^2$, and $4h^2=C$, and the complete equation in ω containing the roots ω_0, ω_1, ω_2, ω_3, becomes $(\omega^2-p)^2-4p(\omega+g)^2=0$ when $\frac{p-1}{4}$ is even and $(\omega^2+3p)^2-4p(\omega+g)^2=0$ when $\frac{p-1}{4}$ is odd. In either case g^2 is given, but the sign of g requires to be determined; alike, however, for one case as for the other, $-8pg$ being the 3rd coefficient after the first, we must have, as shown in the preliminaries, $24pg\equiv 8$ [mod 32], and consequently, since p is of the form $4K+1$, $24g\equiv 8$ [mod 32]. Hence, $3g\equiv 1$ [mod 4], that is, $g\equiv -1$ [mod 4], which gives the required complete determination of g.

The quartisecting equations thus naturally arrived at are expressed in the form in which, according to Bachmann (*Kreistheilung*, p. 230), they were first presented by Lebesgue; the method here given for finding the equations for the trisection and quartisection of the roots of unity will be found on examination to be incomparably simpler, shorter, and more direct than any in common use, and as removing a serious stumbling-block from the path of the student, and, occurring, so far as regards trisection, in the natural course of the development of my subject, I have thought entitled to a place in this memoir. Why I require the trisecting equation is, as will be remembered, to enable me to obtain the conditions of 2 and of 3 being cubic residues to a given index. The condition for 2 being such, strange to say, is nowhere to be found in Bachmann's *Kreistheilung*, although the cubic character of 3 is there duly and fully made out.

The conditions of the one and of the other being cubic residues were, I am informed by M. Lucas, given for the first time in a letter from Gauss to Mlle. Sophie Germain.

Excursus B.

Title 5 (bis).—On the Law of Squares.

There being errors and inaccuracies not a few in the matter printed under this title, owing to my absence abroad as it went through the press, I have thought it desirable to rewrite it, rectifying the errors, and supplying some steps which were wanting in the demonstrations*. I shall, in what follows,

* In the postscript [p. 378 above] which was thought out on board the transatlantic steamer, the *Bothnia*, and written out, as far as I can recollect, at a single sitting a day or two before

use throughout P_i to denote the ith derivative of P, and x_i, y_i, z_i to signify the reduced coordinates of P_i, so that P_1, x_1, y_1, z_1 will mean the same as P, x, y, z respectively. $x+y=0$, $z=0$ will be taken as the auxiliary point of inflexion, serving to complete the scale, and will be called I. In the natural scale it is easy to see that any derived co-ordinate, as z_i, must contain

---

posting it at Queenstown, I have not been able to detect any inaccuracy in the results, although some additional steps and explanations might advantageously have been supplied.

There is, perhaps, one slight exception to be made to this statement as regards the very important theorem, stated but not proved [p. 380], concerning the nature of the form $X\xi+Y\eta+Z\zeta$, where the coefficients of ξ, η, ζ are supposed to be the reduced co-ordinates of any derivative to x, y, z. If $U=0$ is the equation to the cubic in its general form, obviously X, Y, Z are indeterminate, as each may be augmented by an arbitrary multiple of U of suitable degree and order. Consequently, the theorem ought to have been stated in the following form. The co-ordinates X, Y, Z of any such derivative *may be* so expressed that $X\xi+Y\eta+Z\zeta$ shall be a mixed concomitant to U. The fundamental invariantive concomitants to a ternary cubic involving not more than one system of cogredients and a single linear system of contragredients are eleven in number and of the types underwritten:

4 . 0 . 0	4 . 4 . 1
6 . 0 . 0	5 . 4 . 1
1 . 3 . 0	7 . 4 . 1
3 . 3 . 0	9 . 7 . 1
8 . 6 . 0	11 . 7 . 1
12 . 9 . 0	

Hence the co-ordinates of every rational derivative in the natural scale to a point on a cubic curve may be expressed as the coefficients of the contragredient variables in a rational integer function of the above eleven quantities, linear in the latter five, and such that its degree and orders for the nth grade are $\frac{4(n^2-1)}{3}$; n^2, 1.

The particular forms of X, Y, Z which appertain to the concomitant $X\xi+Y\eta+Z\zeta$, and which may be called the *normal* forms, it may be added, are those which actually arise from the processes of *colligation* and *reduction* described in the excursus. By *colligation* I mean the determination of the *general* analytical connective of $x, y, z; x', y', z'$ by the same method as that applied at pages [354, 355] to the canonical quadrinomial form of the cubic. The co-ordinates of such connective are absolutely determinate, inasmuch as the equation which each set of co-ordinates must satisfy is of the order 3, whereas the co-ordinates in question are of the second order only in each set of variables (and of course of the first degree in the coefficients of the cubic). By *reduction* I mean that when in the co-ordinates of the general connective for $x, y, z; x', y', z'$ are substituted the *normal* forms of the co-ordinates for derivatives of the grades μ, $\mu+3i$, their common factor of the degorder $(12i^2-3, 9i^2)$ is to be cast out.

This common factor, it may be noticed, is *always* a covariant of the cubic. When $i=1$, it is seen *a posteriori* that this is the case, for its value is expressible (see footnote, p. [379]) under the form of a known covariant, say Θ (which was obtained by means of using the canonical form of the cubic); that it must be true for all values of i may be deduced from the general algebraical theorem that if in a covariant to any given form, in place of the variables x, y, z be substituted $\frac{d\Omega}{d\xi}, \frac{d\Omega}{d\eta}, \frac{d\Omega}{d\zeta}$, where Ω is any invariantive concomitant to such form, and ξ, η, ζ are contragredient to x, y, z, the resulting expression will be itself an invariantive concomitant. To obtain now the reducing factor for the connective to P_μ, $P_{\mu+3i}$ (p. [380]) it is only necessary to substitute in Θ x_i, y_i, z_i (the normal co-ordinates of the ith derivative) in lieu of x, y, z where $x_i\xi+y_i\eta+z_i\zeta$ is known to be an invariantive concomitant to the cubic. Hence, by the algebraical theorem above stated, the corresponding reducing factor (not containing ξ, η, ζ) is necessarily a covariant to the cubic, as was to be shown.

the original one, as z. For when $z = 0$, P will be a point of inflexion and P_i identical with P, hence (x_i, y_i, z_i) will express the same point of inflexion, and consequently $z_i = 0$; hence z_i must contain z. When we leave the rational scale, so that i is a multiple of 3, z must contain xyz. For when $z = 0$, the ith derivative P will be one of the three points I, I', I'', expressed by $z = 0$, $x^3 + y^3 = 0$. If P is I, P_3 is obviously I; if P is I', P_2 is I', and P_3 will be the connective of P_2 and I''; consequently P_3 is I and $z = 0$, and the same will be the case if P is I''; hence z_3' contains z.

Again, if $y = 0$, P will be some inflexion J, and the connective to I, J being called K, P_3 will be the connective of J, K, that is I, as before; hence z_3 will contain y, and in like manner it will contain x. Also, since in each case P_3 is I, every derivative of P_3 will be I; hence, when $xyz = 0$, $z_{3\nu}$ becomes 0; consequently z_i (if i is a multiple of 3) contains xyz.

Again, if x_i, y_i, z_i are the reduced co-ordinates of P_i, I say that $x_i(y_i^3 - z_i^3)$; $y_i(z_i^3 - x_i^3)$; $z_i(x_i^3 - y_i^3)$ will be the *reduced* co-ordinates of x_{2i}, y_{2i}, z_{2i}.

For, if possible, let two of the above co-ordinates have a common factor F; then, since x_i, y_i, z_i have no common factor, $x_i^3 - y_i^3$, $y_i^3 - z_i^3$ have a common factor, and when $F = 0$, $x_i^3 = y_i^3 = z_i^3$; but $x_i^3 + y_i^3 + z_i^3 + Kx_iy_iz_i = 0$. Hence, unless $x_i^3 = y_i^3 = z_i^3 = 0$, we must have $3 + \sqrt[3]{1}K = 0$, but K is arbitrary. Hence, F must be contained in x_i, y_i, z_i contrary to hypothesis.

Although it is a consequence of a general law* that z_i cannot contain z^2, for present purposes it will be sufficient to establish that z_i cannot, for each of two consecutive values of i, contain z^2. Thus, suppose z_{2i-1} and z_{2i} each contained z^2, then, because z_{2i} contains z^2, z_i must do so too; since, otherwise, $x_i^3 - y_i^3$ must contain z. If that is possible, let $z = 0$; then $x_i^3 - y_i^3 = 0$; but P, and therefore P_i, becomes an inflexion, whereas $x_i^3 = y_i^3$ is the necessary and sufficient condition that P_i is a Plückerian point, which is self-contradictory. But since z_i contains z^2, z_{i-1} must also contain z^2, for z_{2i-1} will be contained (see p. [374]) in $\frac{1}{z}(x_iy_iz_{i-1}^2 - x_{i-1}y_{i-1}z_i^2)$, and therefore, if z_{i-1} does not contain z^2, z must be contained in x_i or y_i, which is impossible. In like manner, if z^2 is contained in z_{2i}, z_{2i+1}, it will be contained also in z_i and z_{i+1}. Hence it would be contained eventually in z, which is absurd.

Again, it may be shown that z will be the only common measure to z_{i-1} and z_i. For, if possible, let them have any other common measure F, and let F become zero. Then P_{i-1} and P_i both become points of inflexion belonging to the system previously designated as I, I', I'', and by a collineation process

* The law is that $x^i \cdot y^i \cdot z^i x_iy_iz_i$, cannot for any value of i contain a square algebraical factor, just as, and *en dernière analyse* for the same general kind of reason, the binomial exponential $(a^i + b^i)$ can contain no such factor.

performed on these points alone or combined with I, P may be obtained. Hence P belongs to the same system of inflexions, that is $z = 0$. Hence F would be contained in a power of z, contrary to hypothesis.

I will now show that if the two systems of unreduced co-ordinates obtained by the colligation of

$$\left.\begin{matrix} x_{i-1},\ y_{i-1},\ z_{i-1} \\ x_i\ ,\ y_i\ ,\ z_i \end{matrix}\right\} \text{ and of } \left\{\begin{matrix} y_{i-1},\ x_{i-1},\ z_{i-1} \\ x_i\ ,\ y_i\ ,\ z_i \end{matrix}\right.$$

be called F, G, H; F', G', H; respectively, the terms F, G, H; F', G', H can have no other measure common to all four than z, or, in other and more precise terms, z is the greatest common measure to the greatest common measures of F, G, H and of F', G', H. For brevity call the two sets of co-ordinates of P_{i-1} and P_i, u, v, w; u', v', w' respectively. Then the unreduced co-ordinates in question will be (p. [374])

$$\left.\begin{aligned} F &= vwu'^2 - v'w'u^2 \\ G &= wuv'^2 - w'u'v^2 \\ H &= uvw'^2 - u'v'w^2 \end{aligned}\right\} \text{ and } \left\{\begin{aligned} uwu'^2 - u'w'v^2 &= F' \\ wvv'^2 - w'v'u^2 &= G' \\ vuw'^2 - v'u'w^2 &= H \end{aligned}\right.$$

into each of which z necessarily enters as a factor, because w, w' have been proved each to contain z.

(u, v, it will be observed, cannot have a common factor, for then u, v, w would have a common factor contrary to hypothesis; and, in like manner, u', v' can have no common factor.)

I say, in the first place, that no indecomposable function of x, y, z, say M, not contained either in w or in w', can be common to F, G, F', G'. For, if so, let F vanish; then, calling $\frac{u}{w}$, $\frac{v}{w}$; $\frac{u'}{w'}$, $\frac{v'}{w'}$, r, s; r', s' respectively, we have

$$\begin{aligned} &(1)\quad sr'^2 - s'r^2 = 0, && (3)\quad rr'^2 - s's^2 = 0, \\ &(2)\quad rs'^2 - r's^2 = 0, && (4)\quad r'r^2 - ss'^2 = 0. \end{aligned}$$

Now, none of the terms r, s, r', s' can vanish: for example r cannot vanish, for, if so, from (1) it would follow that $s = 0$, or $r' = 0$, and from (3) that $s = 0$, or $s' = 0$, so that either $r = 0$ and $s = 0$, or $r' = 0$ and $s' = 0$, that is the general values of u and v or of u' and v' must have a common factor M, which is impossible. Hence, combining (1) and (2) or (3) and (4), we derive $rs = r's'$ (5), as might also be obtained immediately by equating to zero the term common to the two systems above.

From (5), from (3) and (4), and from (1) and (2) we obtain respectively

$$r^3s^3 = r'^3s'^3, \quad r^3r'^3 = s^3s'^3, \quad r'^3s^3 = r^3s'^3,$$

the second and third of which are equivalent to $r^6 = s^6$, $r'^6 = s'^6$, and the first and second combined give $r'^6 = s^6$. Hence $r^6 = r'^6 = s^6 = s'^6$, and consequently the original equations (1), (2), (3) give $r^3 = s^3 = r'^3 = s'^3$.

The equations $r^3 = s^3$, $r'^3 = s'^3$ imply that P_{i-1}, P_i are each of them distinct or identical antitangentials to one of the points of inflexion corresponding to $z = 0$, that is are each of them a Plückerian point on the cubic, and P or (P, I) will be a residual either to P_{i-1}, P_i or to (P_{i-1}, I), P_i where I is the auxiliary inflexion used to complete the scale. Hence P is either a Plückerian or an inflexion point, and in either case P_2 will necessarily be an inflexion. Hence one at least of the derivatives P_{i-1}, P_i is an inflexion, but each is a Plückerian, which is absurd.

Thus M (an irresoluble factor common to F, G, F', G') must be contained either in w or in w'. Suppose it is not z and is contained in w, then it cannot be contained in w', for w, w' have no common measure except z, and consequently when $M = 0$, $v'u^2 = 0$, $u'v^2 = 0$, $v'v^2 = 0$, and $u'u^2 = 0$, and either u and v or u' and v' each become zero, which is impossible seeing that neither the general values of u, v nor those of u', v' can have any common factor. In like manner, it follows that M cannot be contained in w'. Consequently, the two systems F, G, H; F', G', H can have no other common measure, except some power of z.

Finally, I say that the only common measure in question is z itself. (1) Suppose it were possible (which it is not) that one of the two terms w or w' (say w) contains z^2, then it has been proved that the other (w') cannot contain z^2. Hence, if $wvv'^2 - w'u'u^2$ contains z^2, u or u' must contain z, and in like manner, if w' and not w contained z, v or v' must contain z, none of which suppositions are admissible. (2) Suppose that neither w nor w' contains z^2. Then writing $w = \omega z$, $w' = \omega' z$, and writing for $\frac{u}{\omega}$, $\frac{v}{\omega}$; $\frac{u'}{\omega'}$, $\frac{v'}{\omega'}$, r, s; r', s' respectively, we shall obtain over again, as before, $r^3 = s^3$, $r'^3 = s'^3$, indicating as before that P_{i-1} and P_i are each of them Plückerian points when $z = 0$, that is, when P is a point of inflexion, which is doubly absurd. Hence it follows that the common measures of F, G, H and of F', G', H have the common measure z, and no other.

We are now in a position to prove the *law of squares*. Suppose it is true for P_{i-1} and P_i, I say it will be true for P_{2i-1}. For consider the connectives of

$$\left.\begin{matrix} x_{i-1}, & y_{i-1}, & z_{i-1} \\ x_i & , y_i & , z_i \end{matrix}\right\} \text{ and of } \left\{\begin{matrix} y_{i-1}, & x_{i-1}, & z_{i-1} \\ x_i & , y_i & , z_i \end{matrix}\right.$$

as expressed by the formulas above employed. Let $z^2\Omega$ be the third term common to the unreduced systems of co-ordinates.

Allowing (as is the fact) that Ω does not contain z, the reducing factor common to the unreduced co-ordinates of P (or it may be its opposite in

respect to I) must be $z\Omega$, and consequently to the other system corresponding to P_{2i-1} or its opposite, can only be z or z^2; but the latter is impossible, for then z_{2i-1} would not contain z.

Again, if Ω could be conceived equal to $z^q\Omega_1$, the reducing factor for P or its opposite would be $z^{1+q}\Omega_1$, and consequently that for P_{2i-1} or its opposite could not be z^2 and would be z as before. Hence the order of P_{2i-1} in the variables is necessarily $2(i-1)^2+2i^2-1$, that is, $4i^2-4i+1$ or $(2i-1)^2$.

Moreover, it has been shown that if x_i, y_i, z_i are the reduced co-ordinates for P_i, $x_i(y_i^3-z_i^3)$, $y_i(z_i^3-x_i^3)$, $z_i(x_i^3-y_i^3)$ are such for P_{2i}, and consequently, if the law is true for i, it is true for $2i$. Hence, being true for 1, it is true for 2, and therefore for 3, and therefore for 4 and 5 and 6, and therefore for $3+4$, that is, 7, and for 2.4, that is, 8, and for $4+5$, that is, 9, and for 2.5, that is, 10, and so on for every number, as was to be proved*. Thus, this negative proposition, as I have termed it (p. [356]), is completely established. There remains to prove the important proposition contained (but incorrectly proved) on p. [377], to wit, that the unreduced systems of co-ordinates arising from the colligation of

$$\left.\begin{matrix}(x_i, y_i, z_i)\\(x_j, y_j, z_j)\end{matrix}\right\} \text{ and of } \left\{\begin{matrix}(y_i, x_i, z_i)\\(x_j, y_j, z_j)\end{matrix}\right.$$

will be of the forms LN', MN', NN'; $L'N$, $M'N$, $N'N$, where L, M, N; L', M', N' are the reduced systems of the co-ordinates of the connectives of P_i, P_j, and P_i', P_j respectively.

To illustrate this proposition by an example, consider the connectives of P', P_3, that is, P_2 and of P, P_3, that is, P_4.

z_2 is $z(y^3-x^3)$ and z_4 is of the form $z(y^3-x^3)\Omega$, where Ω is of the order 12 in the variables.

Call X_4, Y_4, Z_4 the unreduced co-ordinates arising from the colligation of P, P_3. Suppose x^3-y^3 to become zero, then P becomes a Plückerian, and P_3 will be also such, namely, one of the nine appertaining to the inflexions given by $z=0$†. Hence $x_3^3-y_3^3$ becomes zero. Now X_4, Y_4 represent $yzx_3^2-y_3z_3x^2$,

* In other words, if the theorem is true up to i inclusive, any number between $i+1$ and $2i$ inclusive is either of the form $2j$ or $2j-1$, where j does not exceed i; and being true for j, it is true for $2j$, and being true for $j-1$ and j, it is true for $2j-1$. Hence, if true up to i it is true up to $2i$, but it is true for $i=1$ and therefore for all values of i. Q.E.D.

† The nine points of inflexion on a cubic curve form a closed group, but so also do any three of them which lie in a right line, and also any single one. In like manner, the nine inflexions with their antitangentials, any three of these lying in a right line with their antitangentials, and any one with its antitangentials, form closed groups containing 36, 12, and 4 points respectively. The ornamental-gardening problem of *alignement*, anglice *allineation*, which consists in so disposing a number of points on a plane as to obtain the maximum number or all the various possible numbers of right lines each containing three of the points, finds its systematic solution in the theory of groups of inflexional and sub-inflexional points of various grades.

$xzy_3^2 - x_3z_3y^2$ respectively, and since

$$yzx_3^2 \,.\, x_3z_3y^2 - y_3z_3x^2 \,.\, xzy_3^2 = zz_3\,(x_3^3y_3^3 - y_3^3x_3^3) = 0,$$

$X_4 : Y_4 :: yx_3^2 : xy_3^2$, and consequently $X_4^3 - Y_4^3 = 0$; but P_4 is a point of inflexion and not a Plückerian; hence X_4, Y_4 must each contain the factor $x^3 - y^3$, and Z_4 must be of the form $z^2(x^3 - y^3)^2\,\Omega$, for after division by $z(x^3 - y^3)$ it must still contain that factor. Also X_4, Y_4, Z_4 can have no other common measure except $z(x^3 - y^3)$, for after throwing out that factor the quotient is of the order 16, the order of z_4 given by the law of squares. Thus we see that the third unreduced coefficient common to (P, P_3) and (P', P_3) is equal to $z_2 \,.\, z_4$, as it ought to be according to the proposition in question.

In some very old numbers of the *Educational Times* will be found questions of the kind proposed by me (not reproduced in the Reprint), of which the solution depends on this order of considerations. In certain cases that had been studied, I ascertained the possible existence of a larger number of collineations than had previously been imagined by other writers on the subject, among whom Mr S. B. Woolhouse deserves special mention for the ingenuity of his constructions. As far as I am aware, the theory of allineation has never been treated by other writers than myself, except by empirical methods, and its dependence on the theory of the general cubic curve was not even suspected.