60.

ON THE DIVISORS OF THE SUM OF A GEOMETRICAL SERIES WHOSE FIRST TERM IS UNITY AND COMMON RATIO ANY POSITIVE OR NEGATIVE INTEGER.

[*Nature*, XXXVII. (1888), pp. 417, 418.]

"Nein! Wir sind Dichter*."
—*Kronecker in Berlin.*

A REDUCED Fermatian†, $\frac{r^p-1}{r-1}$, is obviously only another name for the sum of a geometrical series whose first term is unity and common ratio an integer, r.

If p is a prime number, it is easily seen that the above reduced Fermatian will not be divisible by p, unless $r-1$ is so, in which case (unless p is 2) it will be divisible by p, but not by p^2.

This is the theorem which I meant to express [p. 591, above] in the footnote to the second column of this journal for December 15, 1887, p. 153, but by an oversight, committed in the act of committing the idea to paper, the expression there given to it is erroneous.

Following up this simple and almost self-evident theorem, I have been led to a theory of the divisors of a reduced Fermatian, and consequently of the Fermatian itself, which very far transcends in completeness the condition

* Such were the pregnant words recently uttered by the youngest of the splendid triumvirate of Berlin, when challenged to declare if he still held the opinion advanced in his early inaugural thesis (to the effect that mathematics consists exclusively in the setting out of self-evident truths, —in fact, amounts to no more than showing that two and two make four), and maintained unflinchingly by him in the face of the elegant raillery of the late M. Duhamel at a dinner in Paris, where his interrogator—the writer of these lines—was present. This doctoral thesis ought to be capable of being found in the archives of the University (I believe) of Breslau.

† The word Fermatian, formed in analogy with the words Hessian, Jacobian, Pfaffian, Bezoutiant, Cayleyan, is derived from the name of Fermat, to whom it owes its existence among recognized algebraical forms.

in which the subject was left by Euler (see Legendre's *Theory of Numbers*, 3rd edition, vol. I. chap. 2, § 5, pp. 223—27, of Maser's literal translation, Leipzig, 1886)*, and must, I think, in many particulars be here stated for the first time. This theory was called for to overcome certain difficulties which beset my phantom-chase in the chimerical region haunted by those doubtful or suppositious entities called odd perfect numbers. Whoever shall succeed in demonstrating their absolute non-existence will have solved a *problem of the ages* comparable in difficulty to that which previously to the labours of Hermite and Lindemann (whom I am wont to call the Vanquisher of PI, a prouder title in my eyes than if he had been the conqueror at Solferino or Sadowa) environed the subject of the quadrature of the circle. Lambert had proved that the Ludolphian† number could not be a fraction nor the square root of a fraction. Lindemann within the last few years, standing on the shoulders of Hermite, has succeeded in showing that it cannot be the root of any algebraical equation with rational coefficients (see Weierstrass' abridgment of Lindemann's method, *Sitzungsberichte der A. D. W. Berlin*, Dec. 3, 1885).

It had already been shown by M. Servais (*Mathesis*, Liège, October 1887), that no one-fold integer or two-fold odd integer could be a perfect number, of which the proof is extremely simple. The proof for three-fold and four-fold numbers will be seen in articles of mine in the course of publication in the *Comptes Rendus* [above, pp. 604—619], and I have been able also to extend the proof to five-fold numbers. I have also proved that no odd number not divisible by 3 containing less than eight elements can be a perfect number, and see my way to extending the proof to the case of nine elements.

How little had previously been done in this direction is obvious from the fact that, in the paper by M. Servais referred to, the non-existence of three-fold perfect numbers is still considered as problematical; for it contains a "Theorem" that if such form of perfect number exists it must be divisible by fifteen: the ascertained fact, as we must know, being that this hypothetical

* I find, not without surprise, that some of the theorems here produced, including the one contained in the corrected footnote, have been previously stated by myself in a portion of a paper "On certain Ternary Cubic Form Equations," entitled "Excursus A—On the divisors of Cyclotomic Functions" [Vol. III. of this Reprint, p. 317] the contents and almost the existence of which I had forgotten: but the mode of presentation of the theory is different, and I think clearer and more compact here than in the preceding paper; the concluding theorem (which is the important one for the theory of perfect numbers) and the propositions immediately leading up to it in this, are undoubtedly not contained in the previous paper.

I need hardly add that the term *cyclotomic* function is employed to designate the core or primitive factor of a Fermatian, because the resolution into factors of such function, whose index is a given number, is virtually the same problem as to divide a circle into that number of equal parts.

† So the Germans wisely name π, after Ludolph van Ceulen, best known to us by his second name, as the calculator of π up to thirty-six places of decimals.

theorem is the first step in the *reductio ad absurdum* proof of the non-existence of perfect numbers of this sort (see *Nature*, December 15, 1887, p. 153, written before I knew of M. Servais' paper, and recent numbers of the *Comptes Rendus*).

But after this digression it is time to return to the subject of the numerical divisors of a reduced Fermatian.

We know that it can be separated algebraically into as many irreducible functions as there are divisors in the index (unity not counting as a divisor, but a number being counted as a divisor of itself), so that if the components of the index be a^α, b^β, c^γ, ... the number of such functions augmented by unity is

$$(\alpha+1)(\beta+1)(\gamma+1)....$$

All but one of these algebraical divisors, with the exception of a single one, will also be a divisor of some other reduced Fermatian with a lower index: that one, the core so to say (or, as it is more commonly called, the irreducible primitive factor), I call a cyclotomic function of the base, or, taken absolutely, a cyclotome whose index is the index of the Fermatian in which it is contained.

It is obvious that the whole infinite number of such cyclotomes form a single infinite complex. Now it is of high importance in the inquiry into the existability of perfect numbers to ascertain under what circumstances the divisors of the same reduced Fermatian, that is, cyclotomes of different indices to the same base, can have any, and what, numerical factor in common. For this purpose I distinguish such divisors into superior or external and inferior or internal divisors, the former being greater, and the latter less, than the index.

As regards the superior divisors, the rule is that any one such cannot be other than a unilinear function of the index (I call $kx+1$ a unilinear function of x, and k the unilinear coefficient) and that a prime number which is a unilinear function of the index will be a divisor of the cyclotome when the base in regard to the index as modulus is congruous to a power of an integer whose exponent is equal to the unilinear coefficient.

As regards the inferior divisors, the case stands thus. If the index is a prime, or the power of a prime, such index will be itself a divisor. If the index is not a prime, or power of a prime, then the only possible internal divisor is the largest element contained in the index, and such element will not be a divisor unless it is a unilinear function of the product of the highest powers of all the other elements contained in the index.

It must be understood that such internal divisor in either case only appears in the first power; its square cannot be a divisor of the cyclotome.

It is easy to prove the important theorem that no two cyclotomes to the same base can have any the same *external* divisor*.

We thus arrive at a result of great importance for the investigation into the existence or otherwise of perfect odd numbers, which (it being borne in mind that in this theorem the divisors of a number include the number itself, but *not* unity) may be expressed as follows:

The sum of a geometrical series whose first term is unity and common ratio any positive or negative integer other than $+1$ or -1 must contain at least as many distinct prime divisors as the number of its terms contains divisors of all kinds; except when the common ratio is -2 or 2, and the number of terms is

* The proof of this valuable theorem is extremely simple. It rests on the following principles:

(1) That any number which is a common measure to two cyclotomes to the same base must divide the Fermatian to that base whose index is their greatest common measure. This theorem needs only to be stated for the proof to become apparent.

(2) That any cyclotome is contained in the quotient of a Fermatian of the same index by another Fermatian whose index is an aliquot part of the former one. The truth of this will become apparent on considering the form of the linear factors of a cyclotome.

Suppose now that any prime number, k, is a common measure to two cyclotomes whose indices are PQ, PR respectively, where Q is prime to R, and whose common base is Θ. Then k must measure $\Theta^P - 1$ and also $\frac{\Theta^{PQ}-1}{\Theta^P-1}$; it will therefore measure Q, and similarly it will measure R; therefore $k=1$ [unless $Q=1$ or $R=1$; for suppose $Q=1$, then $\frac{\Theta^{PQ}-1}{\Theta^P-1}$ is unity, and no longer contains the *core* of $\Theta^{PQ}-1$]. Hence k being contained in R can only be an internal factor to one of the cyclotomes (namely, the one whose index is the greater of the two). (See footnote at end.)

The other theorem preceding this one in the text, and already given in the "Excursus," may be proved as follows:

Let k, any non-unilinear function of P, the index of a cyclotome χ, be a divisor thereto. Then, by Euler's law, there exists some number, μ, such that k divides $x^{\frac{P}{\mu}}-1$, but the cyclotome is contained algebraically in $\frac{x^P-1}{x^{\frac{P}{\mu}}-1}$; hence k must be contained in μ, and therefore in P. Also, k will be a divisor of $x^{\frac{P}{k}}-1$ and of $\frac{x^P-1}{x^{\frac{P}{k}}-1}$, which contain $x^{\frac{P}{\mu}}-1$ and χ respectively; consequently, if k is odd, k^2 will not be a divisor of $\frac{x^P-1}{x^{\frac{P}{k}}-1}$, and *a fortiori* not of χ. (A proof may easily be given applicable to the case of $k=2$.)

Again, let $P=Qk^i$, where Q does not contain k. Then, by Fermat's theorem, $x^{k^i} \equiv x$ [mod. k] and therefore k divides x^Q-1; but it is prime to Q. Hence, by what has been shown, k must be an external divisor of this function, and consequently a unilinear function of Q. Thus, it is seen that a cyclotome can have only one internal divisor, for this divisor, as has been shown, must be an element of the index, and a unilinear function of the product of the highest powers of all the other elements which are contained in the index.

For an extension of this law to "cyclotomes of the second order and conjugate species," see the "Excursus," where I find the words *extrinsic* and *intrinsic* are used instead of *external* and *internal*.

even in the first case, and 6 *or a multiple of* 6 *in the other, in which cases the number of prime divisors may be one less than in the general case*.*

In the theory of odd perfect numbers, the fact that, in every geometrical series which has to be considered, the common ratio (which is an element of the supposed perfect number) is necessarily odd prevents the exceptional case from ever arising.

The establishment of these laws concerning the divisors and mutual relations of cyclotomes, so far as they are new, has taken its origin in the felt necessity of proving a purely negative and seemingly barren theorem, namely the non-existence of certain classes of those probably altogether imaginary entities called odd perfect numbers: the moral is obvious, that every genuine effort to arrive at a secure basis even of a negative proposition, whether the object of the pursuit is attained or not, and however unimportant such truth, if it were established, may appear in itself, is not to be regarded as a mere gymnastic effort of the intellect, but is almost certain to bring about the discovery of solid and positive knowledge that might otherwise have remained hidden†.

* A reduced Fermatian obviously may be resolved into as many cyclotomes, less one, as its index contains divisors (unity and the number itself as usual counting among the divisors). But, barring the internal divisors, all these cyclotomes to a given base have been proved to be prime to one another, and, consequently, there must be at least as many distinct prime divisors as there are cyclotomes, except in the very special case where the base and index are such that one at least of the cyclotomes becomes equal to its internal divisor or to unity. It may easily be shown that this case only happens when the base is -2 and the index any even number, or when the base is $+2$ and the index divisible by 6; and that in either of these cases there is only a single unit lost in the inferior limit to the number of the elements in the reduced Fermatian.

† Since receiving the revise, I have noticed that it is easy to prove that the algebraical resultant of two cyclotomes to the same base is unity, except when their indices are respectively of the forms $Q(kQ+1)^h$ and $Q(kQ+1)^i$, where $(kQ+1)$ is a prime number, and Q any number (unity *not* excluded), in which case the resultant is $kQ+1$. This theorem supplies the *raison raisonnée* of the proposition proved otherwise in the first part of the long footnote.