74.

ON THE GOLDBACH-EULER THEOREM REGARDING PRIME NUMBERS.

[*Nature*, LV. (1896–7), pp. 196, 197; 269.]

IN the published correspondence of Euler there is a note from him to Goldbach, or, the other way, from Goldbach to Euler, in which a very wonderful theorem is stated which has never been proved by Euler or any one else, which I hope I may be able to do by an entirely original method that I have applied with perfect success to the problem of partitions and to the more general problem of denumeration, that is, to determine the number of solutions in positive integers of any number of linear equations with any number of variables. In applying this method I saw that the possibility of its success depended on the theorem named being true in a stricter sense than that used by its authors, of whom Euler verified but without proving the theorem by innumerable examples. As given by him, the theorem is this: *every even number* may be broken up in one or more ways into two primes.

My stricter theorem consists in adding the words "where, if $2n$ is the given number, one of the primes will be greater than $\frac{n}{2}$, and the other less than $\frac{3n}{2}$." This theorem I have verified by innumerable examples. Such primes as these may be called mid-primes, and the other integers between 1 and $2n-1$ extreme primes in regard to the range 1, 2, 3 ..., $2n-1$.

I have found that with the exception of the number 10, Euler's theorem is true for the resolution of $2n$ into two *extreme* primes; but this I do not propose to consider at present, my theorem being that every even number $2n$ may be resolved into the sum of two mid-primes of the range

$$(1, 2, 3 \ldots, 2n-1).$$

As, for example

$$\begin{aligned}
4 &= 2+2 & 6 &= 3+3 & 8 &= 3+5 & 10 &= 3+7\\
12 &= 5+7 & 14 &= 7+7 & 16 &= 5+11\\
18 &= 5+13 = & & 7+11 & 20 &= 7+13\\
40 &= 11+29 = & & 17+23 & 50 &= 13+37 = 19+31\\
100 &= 29+71 = & & 41+59\\
200 &= 61+139 = & & 73+127 = \&c.\\
500 &= 127+373 = & & 193+307 = \&c.\\
1000 &= 257+743 = \&c.
\end{aligned}$$

And so on.

My method of investigation is as follows. I prove that the number of ways of solving the equation $x+y=2n$, where x and y are two mid-primes to the range $2n-1$, that is twice the number* of ways of breaking up $2n$ into two mid-primes + zero or unity, according as n is a composite or a prime number, is exactly equal to the coefficient of x^{2n} in the series

$$\left(\frac{1}{1-x^p}+\frac{1}{1-x^q}+\ldots+\frac{1}{1-x^l}\right)^2$$

where $p, q, \ldots, l$ are the mid-primes in question. This coefficient, we know *à priori*, is always a positive integer, and therefore if we can show that the coefficient in question is not zero, my theorem is proved, and as a consequence the narrower one of Goldbach and Euler. By means of my general method of expressing any rational algebraical fraction, say ϕx, as a residue, by taking the distinct roots of the denominator, say ρ, and writing the variable equal to $\rho\epsilon^t$, and taking the residue with changed sign of $\Sigma\rho^{-n}\epsilon^{-nt}\phi(\rho\epsilon^t)$, we can find the coefficient of x^n or (if we please to say so) of x^{2n} in the above square, and obtain a superior and an inferior limit to the same in terms of $p, q, \ldots, l$; and if, as I *expect* (or rather, I should say, *hope*) may be the case, these two limits do not include zero between them, the theorems (mine, and therefore *ex abundantia* Euler's) will be apodictically established.

The two limits in question will be algebraic functions of $p, q, \ldots, l$, whereas the *absolute* value of the coefficient included within these limits would require a knowledge of the residues of each of these numbers in respect to every other as a modulus, and of $2n$ in respect of each of them. In a word, the limits will be algebraical, but the quantity limited is an algebraical function of the mid-primes $p, q, r, \ldots, l$.

Postscript. The shortest way of stating my refinement on the Goldbach-Euler theorem is as follows:—"It is always possible to find two primes

* This number may be shown to be of the order $\frac{n}{(\log n)^2}$, and a very fair approximate value of it is $\frac{\mu^2}{n}$ where μ is the number of mid-primes corresponding to the frangible number $2n$.

differing by less than any given number whose sum is equal to twice that number."

Another more instructive and slightly more stringent statement of the new theorem is as follows. Any number n being given, it is possible to find two primes whose sum is $2n$, and whose difference is less than n, $n-1$, $n-2$, $n-3$, according as n divided by 4 leaves the remainders 1, 0, -1, -2 respectively.

Major MacMahon, to whom and to the Council of the Mathematical Society of London I owe my renewed interest in this subject, informs me that in a very old paper in the *Philosophical Magazine* I stated that I was in possession of "a subtle method, which I had communicated to Prof. Cayley," of finding the number of solutions in positive integers of any number of linear equations in any number of variables. This method (never printed) must have been in essence identical with that which within the last month I have discovered and shall, I hope, shortly publish.

I have verified the new law for all the even numbers from 2 to 1000, but will not encumber the pages of *Nature* with the details. The approximate formula hazarded for the number of resolutions of $2n$ into two primes, namely $\frac{\mu^2}{n}$, where μ is the number of mid-primes, does not always come near to the true value. I have reasons for thinking that when n is sufficiently great, $\frac{\mu^2}{2n}$ may possibly be an inferior limit. The generating function

$$\left[\Sigma \frac{1}{1-x^p}\right]^2$$

is subject to a singular correction when the partible number $2n$ is the double of a prime. In this case, since the development to be squared is

$$\mu + x^n + x^{2n} + \ldots + x^p + x^{2p} + \ldots + \&c.,$$

the coefficient of x^{2n} will contain 2μ, arising from the combination of 0 with $2n$, which is foreign to the question, and accordingly the result given by the generating function would be too great by 2μ.

This may be provided against by always rejecting the centre of the mid-range from the number of mid-primes. The formula will then in all cases give twice the number of ways of breaking up $2n$ into two unequal primes. Another method would be to take as the generating function not the square of the sum, but the product of the fractions $\frac{1}{1-x^p}$ (without casting out n when it is a prime), but this method would be inordinately more difficult to work with in computing series involving the roots of unity than the one

chosen, which is in itself a felicitous invention*. Whether the method turns out successful or not, it at the very least gives an analytical expression for the number of ways of conjoining the mid-primes to make up $2n$ without trial, which in itself is a somewhat surprising result. Having lost my preliminary calculations, it may be some little time before I shall be able to say whether the method does or does not contain a proof of the new theorem; but that this can be ascertained, there is no manner of doubt. This is the first serious attempt to deal with Euler's theorem, or to bring the question into line with the general theory of partitions.

It is proper to regard the range 1 to $2n-1$ as consisting of two complementary flank regions, two lateral mid-prime regions, and a region reduced to a single term in the middle, as for example,

1, 2, 3 : 4, 5 : 6 : 7, 8 : 9, 10, 11.

Or, again, 1, 2, 3 : 4, 5, 6 : 7 : 8, 9, 10 : 11, 12, 13.

And the question of $2n$ being resoluble into 2 primes breaks up into three, namely, whether $2n$ can be composed with two flank primes, two lateral mid-primes, or with the number in the central region repeated.

* For the generating function we may take any power greater than 2, instead of the square, and the coefficient of x^{2n} will then be the number of couples making up $2n$ multiplied by $(r^2-r)\,\mu^{r-1}$, which can be calculated by the same method as for the square, but is more difficult and must give rise to numerous theorems of great interest, arising from the multiform representation of the same quantity.