

V.—*On the Theory of Numbers.* By H. F. TALBOT, Esq.

(Read 21st April 1862.)

The object of this paper will be, to give a connected view of some theorems of importance, which are often found in books rather obscurely demonstrated, and in some cases are inaccurately given, or are liable to exceptions which are not mentioned.

§ 1. *On Fermat's Theorem, and Wilson's Theorem.*

The most convenient starting-point for this investigation seems to be the well-known theorem, "If p is a prime number, and $(x+1)^p$ is expanded by the binomial theorem, all the coefficients, except the first and last, are divisible by p .

For it is obvious, in the first place, that all the coefficients are integers. If we multiply $x+1$ into itself, any number of successive times, the coefficients arise from the multiplication and addition of integers, and are therefore themselves integers.

Next, the binomial theorem gives the coefficients in the form

$$p, \frac{p(p-1)}{2}, \frac{p(p-1)(p-2)}{2 \cdot 3}, \text{ \&c.}$$

Let us consider any one of these, for instance the last; then, since $\frac{p(p-1)(p-2)}{2 \cdot 3}$ is an integer, the numbers 2 and 3, found in the denominator must divide some of the factors in the numerator. But they cannot divide p , it being a prime by hypothesis; consequently, they divide $(p-1)(p-2)$, therefore $\frac{(p-1)(p-2)}{2 \cdot 3}$ is an integer. But this integer is the quotient of the coefficient divided by p . Therefore, p divides this coefficient, and so for all the others.

This is the place to introduce a convenient notation, invented, I believe, by GAUSS.

If a and b are two numbers which, when divided by the number n , leave the same remainder, GAUSS says that they are *congruous* to each other, according to the *modulus* n ; which he expresses thus, $a \equiv b \pmod{n}$. The sign \equiv is imitated from $=$ the sign of equality, and implies, not that the numbers are really equal, but that they are *equivalent* (under certain circumstances only). For, if $a \equiv b \pmod{n}$ this would not, in general be the case with a different *modulus*.

I propose in the present paper sometimes to use the word *equivalent* instead of *congruous*.

If any number a is divisible by n , it is equivalent to zero, with modulus n , which is written $a \equiv 0 \pmod{n}$.

To return to the last theorem.

If p is a prime,

$$(x+1)^p = (x^p + 1) + \left(p \cdot x^{p-1} + \frac{p(p-1)}{2} x^{p-2} + \&c. \right)$$

Therefore we have the congruence or equivalence,

$$(x+1)^p \equiv x^p + 1 \pmod{p}.$$

For all the other terms vanish, their coefficients being all divisible by p , whence,

$$p \equiv 0 \pmod{p} \quad \frac{p(p-1)}{2} \equiv 0 \quad \frac{p(p-1)(p-2)}{2 \cdot 3} \equiv 0,$$

and so on.

Take this equivalence

$$(x+1)^p \equiv x^p + 1$$

and suppose $x = 1$

$$\therefore 2^p \equiv 1 + 1 \equiv 2$$

Next suppose $x = 2$

$$\therefore 3^p \equiv 2^p + 1$$

But we found $2^p \equiv 2$

$$\therefore 3^p \equiv 3$$

Next suppose $x = 3$

$$\therefore 4^p \equiv 3^p + 1$$

But we found $3^p \equiv 3$

$$\therefore 4^p \equiv 4$$

And so on till we reach

$$a^p \equiv a.$$

a being any number. Transposing, we have $a^p - a \equiv 0 \pmod{p}$. In other words, the prime number p divides $a^p - a$, or $a(a^{p-1} - 1)$. It therefore divides one of the two factors a , or $a^{p-1} - 1$, whence we obtain FERMAT'S celebrated theorem,—“ If p is a prime number, which does not divide a , it necessarily divides $a^{p-1} - 1$.”

Next let us consider a beautiful theorem first given by LAGRANGE. If p is any prime number, and an equation be formed of $p-1$ dimensions, whose roots are the series of natural numbers, 1, 2, 3, $(p-1)$, all the coefficients of this equation (except the first and last) are divisible by p .

Example.—Let the roots be 1, 2, 3, 4, 5, 6, the equation will be

$$x^6 - 21x^5 + 175x^4 - 735x^3 + 1624x^2 - 1764x + 720 = 0$$

and each coefficient except the first and last is divisible by 7. Assuming LAGRANGE'S theorem as proved, we can deduce a remarkable consequence from it. Let Z be the last coefficient, it is the product of all the roots, or $Z = 1, 2, 3, \dots (p-1)$. Z is always positive, because the equation has an even number of dimensions.

Therefore the equation may be written thus:—

$$(x^p - 1 + Z) + Ax^{p-2} + Bx^{p-3} + \&c. = 0;$$

But by LAGRANGE'S theorem,

$$A \equiv 0 \pmod{p}, B \equiv 0, \&c.$$

And therefore all the terms of the congruence may be omitted except the two first.

$$\therefore x^{p-1} + Z \equiv 0, \text{ whence } -x^{p-1} \equiv Z.$$

In other words, if Z is divided by p , it leaves the same remainder as x^{p-1} does, when divided by p , but with a contrary sign; x being *any one* of the $p-1$ numbers, which are less than p .

The simplest case is when $x=1$. In this case the theorem gives—

$$-1 \equiv Z \text{ or } Z+1 \equiv 0 \pmod{p};$$

which result, expressed in other words, is:—“If p be any prime number, the product of all the numbers less than p , or 1, 2, 3, ($p-1$), augmented by unity is divisible by p .”

This is the celebrated theorem, known as “WILSON’S Theorem,” of which neither its inventor nor WARING, who first published it, could find any demonstration. It was first demonstrated by LAGRANGE (Berlin Memoirs, 1771).

We have not employed FERMAT’S theorem in demonstrating it, therefore it is well to show that the latter can be deduced from it. Thus, we have found $x^{p-1} \equiv -Z \pmod{p}$.

But we have found $Z \equiv -1$. And therefore $x^{p-1} \equiv 1$ (x being any number less than p), which is FERMAT’S theorem.

§ 2. On Associate Numbers.

By WILSON’S theorem, the product of all the numbers 1, 2, 3, ($p-1$), is congruent to $-1 \pmod{p}$. Another demonstration of this is given in GAUSS’S “Arithmetical Researches” (French translation, p. 57). It is there said that EULER discovered that this product, omitting the first and last numbers 1 and $p-1$, could be divided into pairs of *associate* numbers, the product of each of which is $\equiv 1 \pmod{p}$, while the product of the remaining two numbers, 1 and $p-1$ is obviously $\equiv -1 \pmod{p}$. So that the product of the whole series 1, 2, 3, $\overline{p-1}$, is $\equiv -1 \pmod{p}$, as we found before.

In the passage quoted, the following example is given:—The numbers less than 13 can be multiplied in pairs, thus:— $3 \times 9 = 27 = 1$ (if we omit the multiples of 13), which we write $3 \times 9 \equiv 1 \pmod{13}$.

Also, $2 \times 7 \equiv 1$, $4 \times 10 \equiv 1$, $5 \times 8 \equiv 1$, and $6 \times 11 \equiv 1$. But, on the other hand, $1 \times 12 \equiv -1$. Therefore the whole product $1, 2, 3, 12 \equiv -1$.

In this theorem of EULER’S, the product of each pair $\equiv 1$, with the exception of one pair, which is $\equiv -1$.

I have found that there exists another and very different system of *associate numbers*, in which the product of each pair is $\equiv -1$; and therefore, the product of the whole is $\equiv -1$ whenever the number of pairs is odd; but if it is even, in that case the product of one pair always deviates from the rule governing the rest, and is $\equiv +1$. So that in all cases the product of the whole is $\equiv -1$.

We will take the same example as before, the number 13. The *associate numbers* are 1, 12 . . . 2, 6 . . . 3, 4 . . . 7, 11 and 9, 10, the product of each pair being $\equiv -1 \pmod{13}$. Thus, for example, $7 \times 11 = 77$. Rejecting 78, a multiple of 13, there remains -1 . But the remaining pair of numbers, 5 and 8, produce the product 40, which, rejecting 39, a multiple of 13, is equivalent to 1. Therefore $5 \times 8 \equiv 1 \pmod{13}$. It will be observed that the numbers have different associates in EULER's system and in this system, 2 being associated with 6, and not with 7, &c.; except that 1 is still associated with 12, and 5 with 8.

I will add some other examples of this new system of *associate numbers*.

If the prime number be 5, the associates are 1, 4, whose product $\equiv -1$, and 2, 3 whose product $\equiv +1$. This prime is of the form $4n+1$, therefore the numbers less than it form $2n$ pairs, an even number; therefore the product of one pair deviates from the rest, as was observed before. Other examples of this, in primes of the form $4n+1$, are, $p=13$. This case has been given before. The associates are written one over the other in the following table, and the deviating pair stands by itself:—

1	2	3	7	9		5
12	6	4	11	10		8

In the case of $p=17$ we find,—

1	2	3	5	6	7	9		4
16	8	11	10	14	12	15		13

The sum of the deviant pair is always equal to the prime number. Thus, $4+13=17$. It is worth remark, that the same holds in EULER's system, where the deviant pair are always 1 and $p-1$, whose sum $=p$.

It will make the nature of these *associate numbers* plainer, if we subtract p from each of those which exceed $\frac{p-1}{2}$. The remainders will be negative numbers, less than $\frac{p-1}{2}$. Thus, if $p=17$, writing the associates one above the other, and their product in the lowest line,

	1	2	-2	3	6	5	7		4
	-1	8	-8	-6	-3	-7	-5		-4
	-1	16	16	-18	-18	-35	-35		-16
or	-1	-1	-1	-1	-1	-1	-1		+1

Rule to find the pair of numbers which deviate from the rest. Find the number x less than $\frac{p-1}{2}$, such that $1+x^2$ is divisible by p , which can always easily be done, and has only one solution. Then x and $-x$ are the pair required.

If now we turn to primes of the form $4n+3$, the numbers less than p form $2n+1$ pairs, an odd number, \therefore the product of each pair $\equiv -1$, and there are no deviations.

For example, if $p=7$, the associates are

1	2	4
6	3	5

If $p=11$, they are

1	2	3	4	6
10	5	7	8	9

We will now pass to the consideration of another system of *associate numbers*, which I do not find mentioned in the books.

Theorem.—If p is a prime number of the form $4n+1$, and the series of natural numbers 1, 2, 3, &c., be taken as far as $\frac{p-1}{2}$ (which will be of the form $2n$, and therefore an even number), then the *squares* of these $\frac{p-1}{2}$ numbers can be divided into *associate pairs*, in such a way that the sum of each pair shall be divisible by p .

Example.—Let $p=17$, $\therefore \frac{p-1}{2}=8$. The 8 squares may be divided into pairs, so that each pair is divisible by 17, as follows:—

$$1^2+4^2, 2^2+8^2, 3^2+5^2, 6^2+7^2.$$

It is plain that each number can have only one associate. For let a have the *associate* b $\therefore a^2+b^2 \equiv 0 \pmod{p}$. If c were another associate, we should have $a^2+c^2 \equiv 0 \pmod{p}$, and $\therefore b^2-c^2 \equiv 0 \pmod{p}$; that is, p must divide one of the factors of b^2-c^2 . But these are $b+c$ and $b-c$. And $b+c$ is less than p , because b and c are each less than, or equal to, $\frac{p-1}{2}$. Much more is $b-c$ less than p .

But p cannot divide numbers less than itself, therefore a has only the associate b . It remains, however, to show, that each number has an *associate*. This follows from the well-known theorem,—“That every prime of the form $4n+1$ is the sum of 2 squares, in one way only.”

Sometimes one of the squares is unity. For example, the prime 17 is the sum of $1+16=1^2+4^2$. When this happens, the other *associates* are easily deduced. Thus, multiplying the equation $1^2+4^2=17=p$ by 2^2 , we have $2^2+8^2=2^2 \cdot p$, which being divisible by p , is $\equiv 0 \pmod{p}$ $\therefore 2^2+8^2 \equiv 0$, and 2 has the associate 8. Similarly, $3^2+12^2 \equiv 0$, but 12 exceeding $\frac{p-1}{2}$ or 8, we substitute for it $p-12$, or 5, $\therefore 3^2+5^2 \equiv 0$, and 3 has the *associate* 5; and so on.

But when the prime p is the sum of 2 squares, neither of which is 1, we proceed a little differently. Thus, let $p=29$, which $=4+25=2^2+5^2$. Multiply the *least* of these numbers, a , by the number which will give a product *nearest* to the prime 29, and the difference will of course be less than a . Thus, if we

multiply the congruence $2^2 + 5^2 \equiv 0$ by 15^2 , we get $30^2 + 75^2 \equiv 0$, and rejecting the multiples of 29, we get $1 + (-12)^2 \equiv 0$, or $1 + 12^2 \equiv 0$ (because $75 = 3 \times 29 - 12$). And upon trial it will be found that $1 + 12^2$, or 145, is divisible by 29. Having thus found a pair of squares, such as $1 + a^2 \equiv 0$, we find all the others from it by simple multiplication, and rejecting the multiples of 29. If we had not found this pair $1 + a^2$ at first, we should at any rate have approximated to it.

Another mode is the following:—Since $2^2 + 5^2 = 29 = p$ and 5 is not divisible by 2, add 29 to it $\therefore 2^2 + 34^2 \equiv p \equiv 0 \pmod{p}$, and dividing by 2^2 , $1^2 + 17^2 \equiv 0$ $\therefore 1 + (-12)^2 \equiv 0$, $\therefore 1 + 12^2 \equiv 0$, as before.

p being a prime of the form $4n + 1$, we have in all cases $p = m^2 + n^2$, and having ascertained the values of m, n , we can derive from them other numbers a, b, c, d , such that $a^2 + b^2 \equiv 0$, $c^2 + d^2 \equiv 0$, &c.; from which a curious theorem arises,—If the prime number p divides both $a^2 + b^2$, and $c^2 + d^2$, it also divides both $ac + bd$ and $bc - ad$.

Example.—29 divides $2^2 + 5^2$ and $3^2 + 7^2$. Therefore, it divides $5 \cdot 7 - 2 \cdot 3$ and $2 \cdot 7 + 5 \cdot 3$.

Demonstration.—Because $a^2 + b^2 \equiv 0$ and $c^2 + d^2 \equiv 0$, $\therefore a^2 c^2 + b^2 c^2 \equiv 0$ and $a^2 c^2 + a^2 d^2 \equiv 0$, \therefore by subtraction $b^2 c^2 - a^2 d^2 \equiv 0$, the factors of which being $bc + ad$ and $bc - ad$, p must divide one of them. [M.]

Permute the letters a, b , in this result, since it is immaterial which is which; therefore p divides one of the two factors, $ac + bd$, or $ac - bd$. [N.]

Comparing the results M and N, we see that if p divides $ac + bd$ in the second of them, it divides $bc - ad$ in the first.

It appears from what precedes, that a prime p of the form $4n + 1$ always divides some number of the form $1 + a^2$, where a is less than $\frac{p-1}{2}$. Annexed is a table of the values of a for the first prime numbers of that form, from 5 to 109.

5 divides $1 + 2^2$	61 divides $1 + 11^2$
13 ... $1 + 5^2$	73 ... $1 + 27^2$
17 ... $1 + 4^2$	89 ... $1 + 34^2$
29 ... $1 + 12^2$	97 ... $1 + 22^2$
37 ... $1 + 6^2$	101 ... $1 + 10^2$
41 ... $1 + 9^2$	109 ... $1 + 33^2$
53 ... $1 + 23^2$	

The law which governs these results is not manifest, therefore, although the prime p always divides a number of the form $1 + x^2$ (x less than $\frac{p-1}{2}$), yet x must be found by tentative methods.

We will here add a few more examples of a theorem previously mentioned:—

The prime $13 = 2^2 + 3^2$ and divides $1 + 5^2$ $\therefore 3 \cdot 5 - 1 \cdot 2 = 13$, and $2 \cdot 5 + 1 \cdot 3 = 13$.

The prime $41 = 4^2 + 5^2$ and divides $1 + 9^2$ $\therefore 4 \cdot 9 + 1 \cdot 5 = 41$, and $5 \cdot 9 - 1 \cdot 4 = 41$.

The prime $61 = 5^2 + 6^2$ and divides $1 + 11^2$ $\therefore 5 \cdot 11 + 1 \cdot 6 = 61$, and $6 \cdot 11 - 1 \cdot 5 = 61$.

Although a prime of the form $4n+1$, is always the sum of 2 squares, yet a rule is wanting to determine these squares. The following answers for one case:—

Let p be the prime. Try if $2p-1$, is a square, and if so, call it g^2 .

Then

$$p = \left(\frac{g-1}{2}\right)^2 + \left(\frac{g+1}{2}\right)^2$$

Example.—Let $p=1861 \therefore 2p-1=3721=61^2=g^2 \therefore p=30^2+31^2$.

§ 3. *Remarks on Barlow's Theory of Numbers.*

PETER BARLOW, of the Royal Military Academy, a mathematician of eminence, and author of a volume of tables most useful to all persons engaged in numerical computations, and believed to be exceedingly accurate, published in 1811 a work entitled “An Elementary Investigation of the Theory of Numbers.” This book, which gives much useful information on a subject at that time little known to the English reader, contains a few errors which ought to be pointed out, lest they should acquire credit, by having appeared in a work of authority.

I. It is well known that mathematicians have never been able to find the demonstration of FERMAT'S theorem, which asserts that $a^n+b^n=c^n$, is an impossible equation, if n is an integer number greater than 2. Nevertheless, BARLOW, at p. 169 of his work, professes to give a demonstration of this theorem. Subsequent mathematicians, however, have tacitly ignored BARLOW'S demonstration, and the question has continued to be proposed from time to time by the French Institute and other learned societies, without receiving any solution. It is worth while, therefore, to inquire for what reason BARLOW'S demonstration has been put aside. Before treating of the general problem, to satisfy the equation $a^n+b^n=c^n$, he treats of the particular case $a^3+b^3=c^3$, and as he treats this exactly in the same way pp. 132–140, one explanation will suffice for all. It appears to me that the error of the demonstration lies in p. 139, where he obtains an equation $\frac{t^2}{r} - \frac{s^2}{tr} - \frac{9r^2}{st} = 6$, and says, *first*, that because r, s, t , are prime to each other, each of the above fractions is in its simplest form; and, *secondly*, that they each contain a factor in their denominator, that is not common with the other denominators; and therefore, these fractions cannot, anyhow combined, be equal to an integer, by Corollary 2 of Art. 13. But this theorem is not true. Take for example the equation $\frac{7}{2 \cdot 3} + \frac{8}{3 \cdot 5} + \frac{3}{2 \cdot 5} = S$. According to the theorem, S cannot be an integer, because the fractions are in their lowest terms, and each denominator contains a factor, *that is not common to the other denominators*.

But on trial, we find that $S=2$, an integer. Turning, therefore, to the Corollary mentioned, which is found at p. 20, we see that it rests upon a theorem in p. 19, viz.:—“The sum of two fractions in their lowest terms, of which the denominator of the one contains a factor not common with the other, cannot be an integer.” This may be admitted; but Cor. 2, which follows, appears to be

erroneous, viz. :—“ Cor. 2. *In the same manner it may be shown*, if there be several fractions, and one of them be in its lowest terms, and contain a factor in its denominator, *that is not common to all the other denominators*, the sum of these fractions cannot be an integer.” As BARLOW’S demonstration of FERMAT’S theorem reposes on this Corollary, that demonstration falls to the ground, and a true demonstration of the theorem still remains to be sought for.

II. There is a well known and very remarkable theorem, that “ Every prime number of the form $4n+1$ is the sum of two squares, and in one way only.”

The most simple proof of this appears to consist in the following series of propositions :—

(1.) The product of the sum of two squares by a similar quantity is likewise the sum of two squares, and in two ways,—

Because $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$;
and also, $= (ac - bd)^2 + (ad + bc)^2$

(2.) The sum of two squares can only be divided by a quantity of like form.

(3.) By WILSON’S theorem, a prime p always divides $1, 2, 3, \dots (p-1) + 1$, and this product may be written

1. $(p-1) \dots 2. (p-2) \dots 3. (p-3) \dots \&c.$
or, $(p-1) (2p-2^2) (3p-3^2) \dots \&c.$

or omitting the multiples of p , and observing that the number of factors is even, if p is of the form $4n+1$, the product may be written

$$1^2 \times 2^2 \times 3^2 \dots (2n)^2 = [1 \cdot 2 \cdot 3 \dots 2n]^2 = Q^2.$$

Therefore p divides $Q^2 + 1$ the sum of two squares. Therefore p is itself the sum of two squares.

BARLOW, at p. 205 of his work, gives the converse of this theorem, and says, that a number of the form $4n+1$ is necessarily a prime number, if it is the sum of two squares, in one way only. Suppose, however, that we take for example the number 45. This is the sum of two squares $36+9$, and in one way only. Nevertheless, the number 45 is not a prime, as it ought to be by this rule. This shows how much caution is necessary in writing on this branch of mathematics. The fact is, the theorem only holds good in case the two squares are *prime to each other*. Now, 36 and 9 are not so; and, consequently, the conclusion that their sum is a prime number is erroneous. With this limitation, however, I believe the theorem is correct. There is one apparent exception, however, which should be pointed out. The square of a prime number of the form $4n+1$ is of the same form, and is the sum of two squares in one way only. Thus, 5^2 , or $25=16+9$ and 13^2 , or $169=144+25$. The test, therefore, appears to fail in these instances. But in fact it holds good; for 25 is not only the sum of the squares $16+9$, but also of $25+0$, and this consideration applies to all similar cases.