Commentaries of the St. Petersburgh Academy of Sciences 6 (1732/3), 1738, p. 103-107 . Translated and annotated by Ian Bruce.

1

OBSERVATIONS CONCERNING A CERTAIN THEOREM OF FERMAT AND OTHER CONSIDERATIONS REGARDING PRIME NUMBERS

L. Euler (E26)

It is well known that this quantity $a^n + 1$ always has divisors, as often as n shall be an odd number, or divisible by an odd number besides unity. In so much as $a^{2m+1}+1$ can be divided by $a+1$ and $a^{p(2m+1)}+1$, also $a^{p(2m+1)}+1$ can be divided by a^p+1, whatever number may be substituted in place of a. Truly on the other hand, if n were a number of such a kind, which may be divided by no odd number except unity, because that happens [in this case] when n is a power of two, no divisor is able to be assigned to the number a^n+1. On account of which, if which prime numbers are of this form a^n+1, all these may be taken by necessity to have this form $a^{2^m}+1$. Nor yet can it be concluded from this that $a^{2^m}+1$ will exhibit a prime number always, whatever a may be ; for in the first place it is evident, if a shall be odd, that form will have the divisor 2. Then also, even if a may denote some even number, innumerable cases are given still, in which a composite number will be produced. Thus at any rate this formula a^2+1 can be divided by 5, as often as there is $a = 5b \pm 3$, and 30^2+1 can be divided by 17 [$a = 17b \pm 4$ with $b = 2$, etc.] and 50^2+1 by 41. In a similar manner 10^4+1 has the divisor 73, 6^8+1 has the divisor 17 and $6^{128}+1$ is divisible by 257. But no case is detected in which some divisor of this form $2^{2^m}+1$ may have a place, as far as from a tables of prime numbers which indeed do not extend beyond 100000. Perhaps from this and other reasons Fermat was led to enunciate he had no doubt $2^{2^m}+1$ to be a prime number always and this he proposed to Wallis and other English mathematicians as an excellent theorem requiring to be shown. Indeed he admits not to have a demonstration of this itself, yet he asserts in no way less it to be the most true. But of that theorem its usefulness is because by its aid, and this he proclaims chiefly, for any given prime number, a greater may be shown easily, that which would be most difficult without a general theorem of this kind. These are read in the *Commercio Epistolico* of Wallis in the penultimate letter in the second book of his Works [in a letter from Fermat to Wallis via Kenelman Digby, *Opera*, Vol. II, p.857, set out in part below]. The following are also present in the works of Fermat [following p. 115, *Varia opera Matematica*, 1679] :

"But since it may be agreed by me , a number in [the form of] a square from two multiplied by itself [the idea of expressing such notions by indices had not yet been established] and increased by one shall be a prime number always and now the truth of that theorem had been shown by Analysts a long time ago, clearly 3, 5, 17, 257, 65537 etc. to infinity, become primes, without labour etc."

Commentaries of the St. Petersburgh Academy of Sciences 6 (1732/3), 1738, p. 103-107 . Translated and annotated by Ian Bruce.

The truth of this theorem may be elicited, as I have said now, if for *m* there may be put 1, 2, 3 and 4; indeed these numbers emerge 5, 17, 257 and 65537, which all are found among the prime numbers in the table. But I do not know by what fate it may have come about, that following at once $2^{2^5}+1$ evidently ceases to be a prime number ; for I have observed from these tedious days that this number by acting another way can be divided by 641, and so it will be apparent for that at once to be tested. Indeed there is $2^{2^5}+1=2^{32}+1=4294967297$. From which it can be understood the theorem fails in this and also in other cases which follow, and now on this account the problem concerning the finding of a greater prime number is not solved.

Now I will consider also the formula 2^n-1, which may have divisors, as often as n is not a prime number, and not only 2^n-1, but also a^n-1. But if n may be considered to be a prime number, it may be able to consider that 2^n-1 always show such also; yet no one has dared to assert this, as far as I know, since it may be refuted so easily. For $2^{11}-1$, *i.e.* 2047, has the divisors 23 and 89, and $2^{23}-1$ can be divided by 47. Moreover I see the celebrated Wolf has turned his attention to this neither in his *Elem. Matheseos* nor has it changed in the other edition, where he investigates perfect numbers and he enumerates 2047 among the primes, moreover also 511 or 2^9-1 is had for such, since yet it shall be divisible by 2^3-1, i. e. 7. Moreover $2^{n-1}\left(2^n-1\right)$ gives a perfect number, as often as 2^n-1 is prime [Euclid; Book 9, Prop. 36]; therefore also *n* must be a prime number. Therefore I have considered it worth the effort to note these cases, in which 2^n-1 is not a prime number, whenever *n* shall be such. But I have found this always happens, if there shall be $n=4m-1$, and *8m* - 1 were a prime number ; for then 2^n-1 always will be able to be divided by *8m* -1. Hence the following cases are to be excluded : 11, 23, 83, 131, 179, 191, 239 etc., which numbers substituted for *n* return 2^n-1 a composite number. Nor yet all the remaining prime numbers put in place of *n* are satisfactory, but several in addition are excepted ; thus I have observed $2^{37}-1$ to be able to be divided by 223, $2^{43}-1$ by 431, $2^{29}-1$ by 1103, $2^{73}-1$ by 439; yet not all to be excluded is in a power. But yet I dare to assert besides these cases noted all the prime numbers less than 50 and perhaps less than 100 bring about $2^{n-1}\left(2^n-1\right)$ to be a perfect number with the following numbers put in place for *n* : 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47, from which 11 perfect numbers have come upon. I have deduced these observations from a certain theorem not devoid of elegance, of which indeed also I do not have a demonstration, yet truly I am most certain concerning the truth of this. This is the theorem: a^n-b^n *can be divided by* $n+1$ *always, if* $n+1$ *were a prime number and a and b shall not be divided by that ;* but I think the demonstration of this to be more difficult from that, because it is not true, unless $n+1$ shall be a prime number. From this it follows at once that 2^n-1 can always be divided by $n+1$, if $n+1$ were a prime number, or , since all the primes shall be odd except 2 and this on account of the conditions of the theorem, because there is $a=2$, will not be able to be used, $2^{2^m}-1$

always will be able to be divided by $2m+1$, if $2m+1$ shall be a prime number. Whereby also either 2^m+1 of 2^m-1 will be able to be divided by $2m+1$. But I have grasped $2m+1$ able to be divided, if there were $m=4p+1$ or $4p+2$; but $2^{2^m}-1$ will have a divisor $2m+1$, if $m=4p$ or $4p-1$. I have fallen upon many other not less elegant theorems in this pursuit, which with that one I think to be required to be valued more, because either in short they are unable to be demonstrated or they may follow from propositions of this kind, which are unable to be demonstrated ; therefore it has been considered to add the more outstanding here.

THEOREM 1

If n were a prime number, [*for some number a*] *every power of the exponent* $n-1$ *divided by n leaves either zero or* 1. [This is Fermat's Little Theorem, which Euler later writes (in E54 below) in the form : *For a signified prime number p, the formula* $a^{p-1}-1$ *can be divided by p always, unless a may be divided by p.*]

THEOREM 2

With n remaining a prime number every power [*of a*], *of which the exponent is* $n^{m-1}(n-1)$, *divided by* n^m *, leaves either 0 or 1.*

THEOREM 3

Let m, n, p, q etc. be unequal prime numbers and let A be the smallest common divisor of these diminished by unity, consider of these $m-1$, $n-1$, $p-1$, $q-1$ *etc.; with these in place I say that every power of the exponent A as* a^A *divided by* $mnpq$ *etc. leaves either* 0 *or* 1, *unless a shall be divided by any of these numbers m, n, p, q etc.*

THEOREM 4

With $2n+1$ *denoting a prime number* 3^n+1 *will be divided by* $2n+1$, *if there shall be either* $n=6p+2$ *or* $n=6p+3$; *but* 3^n-1 *will be divided by* $2n+1$, *if there shall be either* $n=6p$ *or* $n=6p-1$.

THEOREM 5

3^n+2^n *can be divided by* $2n+1$, *if there shall be either* $n=12p+3$, $12p+5$, $12p+6$ *or* $12p+8$. And 3^n-2^n *can be divided by* $2n+1$, if there shall be either $n=12p$, $12p+2$, $12p+9$ *or* $12p+11$.

THEOREM 6

Under the same conditions, by which 3^n+2^n *may be divided,* 6^n+1 *also will be divided by* $2n+1$; *and* 6^n-1 *under the same conditions, by which* 3^n-2^n *can be so divided.*

LETTER XLV.

Pierre Fermat to John Wallis via Kenelm Digby.

***Noble** Sir,*
I Received lately from *Mons. Fermat,* the enclosed written paper, with a desire from him to conveigh it to my *Lord Brouncker* and your self: I hope you have received mine of the 8 and 25 of May. A main errand of this present Letter is humbly to take my leave of you for some months ; for I am ere long going a journey that will take up all this summer at the least. When I return to *Paris,* I will give you an account of it by presenting my humble respects unto you. In the mean time I cease further troubling you, and remain

Paris 19 *June* 1658.

Noble Sir,
Your most humble and most obedient servant, that highly honoureth you,
KENELM DIGBY.

EPISTOLA XLVI.

From Fermat to Wallis
including the preceding note via Kenelmum Digby.

Indeed I delight in and I acknowledge the solutions of numerical questions proposed by me that the most illustrious of men the Viscount Brouncker and John Wallis finally have given in a willing and proper manner. The most illustrious men have been unwilling to concede even an odd moment or to render assistance to the proposed questions ; but I wish rather that these questions also be recognised at once as worthy of the labours of the English [mathematicians], and after the solutions of these should be arrived at, to have accomplished from that a more illustrious triumph from which a great labour would become apparent. But the opposite of this has been seen. Certainly that glory must be given to the most illustrious and ingenious men of nations. Truly so that henceforth we may act honourably on both sides, the English may admit to have satisfied the questions proposed by the French: But in turn the English may propose questions themselves to be worthy to these they have solved, so that they may not disdain considering and examining following the nature of whole numbers more carefully, and indeed to propagate that science, which they have influenced by the strength of their ingenuity and subtleness. As because from that we may submit [the theory of] *Diophantus* itself and its most celebrated translator *Bachet,* to the authority of the matter we propose. *Diophantus* supposed in most of books 4 & 5 every whole number to be either a square, or composed from two or three or four squares. For *Bachet* himself admits in the commentary to question 3l of book 4 that it is not yet evident to follow by a prefect demonstration. That *Rene Descartes* himself not knowing his own ability declares in a certain letter that soon we must accept a certain addendum, and indeed a way by which at this stage the difficulty and abstruseness may be denied. Therefore I do not see why we should have doubts about the worth of that proposition. Yet I do advise the most illustrious men that a perfect demonstration of this has been found by me. Also I may add several propositions

not only the most famous, but also true from the most rigorous demonstrations. For the sake of examples.

Each prime number which is exceeds a multiple of four by one is composed from two squares. Of this kind are 5, 13**,** 17, 29, 37, 41, &c. Each prime number which exceeds a multiple of three by one is composed from four or three other squares, of such a kind are 7, 13, 19, 31, 37, 43, &c. Each prime number which exceeds a multiple of eight either by one or three, is composed from a square and twice another square, of such a kind are 3, 11, 17,19, 41, 43, &c.

But also and preceding that of *Bachet,* we have proposed generally at one time the proposition by *Saint Croise*, and we are not ignorant of its demonstration.

Each whole number is a triangle, so that it is composed from two or from three triangles.

It is a square or composed from two, three or four squares.

It is a pentagon, or composed from two, three, four or five pentagons.

It is a hexagon or composed from two, three, four, five or from six hexagons.

And thus by propositions continued indefinitely.

All these and boundless others which can be seen for whole numbers, have been found and generally demonstrated by us, and we can propose to the most illustrious men and proposing perhaps a little of this to be done. But Gallic ingenuity will discern certain other propositions the demonstration of which we cannot deny but to be unknown to us , although the truth of these may be agreed upon by us. Indeed we may bear in mind *Archimedes* without disdain, with the true but still undemonstrated propositions of *Conon*, finally to put at hand the truth of these to be confirmed by the most subtle demonstrations. Therefore why may I not expect similar aid from the most outstanding men, as it were the Gallic *Conon* from the English *Archimedes* ?

1. All the powers of the number 2, the exponents of which are the terms of a geometric progression of the same number 2, increased by one are prime numbers.
The geometrical progression with its exponents 2 may be set out :

1	2	3	4	5	6	7	8
2	4	8	16	32	64	128	256

The first term 2 increased by unity makes 3, which is a prime number. The fourth term 4 increased by one makes 5, which equally is a prime number. The fourth term 16 increased by one makes 17 , a prime number. The eighth term 256 increased by one makes 257, a prime number. Generally on taking all the powers of 2, the exponents of which are a progression of numbers, the same will come about. For if then you may take the sixteenth term which is 65536, that increased by one will make 65537, a prime number. With this agreed upon it is possible to give and to assign without any effort a prime number greater than any given number. The demonstration of that proposition is sought, of beauty to be sure but also most true, with the aid of which, as we have now said, another most difficult problem can be solved at once. For any given number to find a prime number greater than that given number. With the benefit of this key perhaps the most illustrious men will uncover all the mystery concerning prime numbers, that is : for

any number given to find in the shortest and easiest way whether it shall be prime or composite.
2. Thus from which. The double of any prime number one less than a multiple of eight, is composed from three squares. Let there be some prime number less by one than a multiple of eight, (such as are 7, 23, 31, 47, &c.) of which the double are as 14, 46, 62, 94, is composed from three squares. We may assert that true proposition, but in the manner of Conon not yet either with the assertion nor demonstration from Archimedes.
3. If two prime numbers ending either in 3 or in 7 may be multiplied together with a multiple of four exceeding a multiple of three. The product is composed from a square and five times another square. Such numbers are 3, 7, 23, 43, 47, 67, &c. [Thus, 13 is not such a number.] Take two from these for example 7 and 23 because from under these 161 may be composed from a square and five times another square; for the square 81 and five times 16 is be equal to 161. That truly we may assert generally, yet we may await the demonstration. But from these individual squares and squares of multiples of five, which it is required to be demonstrated.

But lest we may appear to be excessively lacking in demonstrations, we can assert and demonstrate the following proposition.

No triangular number besides one is equal to the square of a square number.

All the triangular numbers as they are known are 1,3,6,10,15,21,28,36,45, &c. None generally made from the progression to infinity except one alone will be a square from a square.
etc. etc. [The remainder of the letter is concerned with geometrical problems.]

THE DEMONSTRATION OF CERTAIN THEOREMS REGARDING PRIME NUMBERS

Commentaries of the St. Petersburg Academy of Sciences 8 (1736), 1741, p.141-146.
Now accorded the Enestrom index E54.

1. In the past most arithmetical theorems by Fermat have been set forth in publications but without demonstration, in which if they were true, not only would there be present an extraordinary number of properties, but truly also that science of numbers, which generally may be seen to exceed the bounds of analysis, would be strongly promoted. But any such as you please from many of significance which the Geometer proposed, he has himself asserted of the theorem that either it can be demonstrated or perhaps the truth of that is certain, yet nowhere, as far as it can be established by me, has he set out demonstrations. Instead rather, the great part of Fermat's numerical theorems is seen to follow by induction, clearly by this single way properties of this kind requiring to be elicited may be seen to become apparent. But truly I may indicate by several examples that as little as possible should be attributed to inductions in this business; by which it may suffice with a single example chosen reported from Fermat. I speak of course about that theorem, the falsehood of which I have shown now several years ago, in which Fermat asserted that all numbers of this form $2^{2^{n+1}}$ taken together are prime numbers. Moreover towards establishing the truth of this proposition it is considered that in general

induction be sufficient [Note that induction at this time does not correspond quite to the principle of induction]. For because, except that all these numbers less than 100000 actually shall be primes, also I have shown easily that no prime number greater than 600 can be judged by this formula $2^{2^{n+1}}+1$, however great the number substituted for *n* may be also. [The formula fails when $n=5$ as $2^{32}+1=4294967297=641\times 6700417$.] Since yet nevertheless it may be agreed that the truth of this proposition not be consented to, it is understood easily to what extent induction may prevail in speculations of this kind.

2. For this reason all numerical properties of this kind, which depend on induction only, I decided long ago to be taken as uncertain, until these either may be fortified by a clearly proved demonstration, or generally they may be refuted. Also no more of these propositions, which for that one I discussed concerned with Fermat's memorable theorem about perfect numbers that I made the subject of an off-handed treatment, may I consider to be trusted to be proved by induction, by that single way by which they may be determined, only until I have come upon an understanding of these arising with time. Now truly, afterwards I have found the most rigorous demonstrations of these theorems by a singular method, concerning the truth of these there is no further doubt. On account of which in this dissertation I have decided to set out my demonstrations, where I may explain both the truth of that theorem required to be shown as well as that method, by which these demonstrations have been found, which perhaps also in other investigations of numbers will be able to be brought into use.

3. But the proposition, which here I have undertaken to demonstrate, is the following:

With a signified prime number p, the formula $a^{p-1}-1$ *can be divided by p always, unless a is able to be divided by p.*

For from this proposition demonstrated the truth of the remaining theorems follows at once. Indeed the case of the formula proposed, in which there is $a=2$, now I have given the demonstration at another time [E26 above] ; but still then the demonstration was unable to be extended to a general formula. On account of which in the first place it may be convenient to bring forwards the proof of that case, from which a transition to more general may be returned there more easily. Therefore the following proposition will be required to be demonstrated:

With any odd prime number p specified, whichever formula $2^{p-1}-1$ *always will be able to be divided by p.*

DEMONSTRATION

In place of 2 there may be put 1 + 1 and there will be

$$(1+1)^{p-1}=1+\frac{p-1}{1}+\frac{(p-1)(p-2)}{1\cdot 2}+\frac{(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3}+\frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4}+\text{etc.},$$

the number of terms of which series is $=p$ and hence is odd. Besides any term, whatever kind of fraction it may have, will give a whole number ; and from which the numerator,

as it may be agreed well enough, can be divided by its own denominator. Therefore with the first term of the series 1 removed there will be

$$(1+1)^{p-1}-1=2^{p-1}-1=\frac{p-1}{1}+\frac{(p-1)(p-2)}{1\cdot 2}+\frac{(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3}+\frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4}+\text{etc.},$$

the number of terms of which is $= p-1$ and therefore even. Therefore each two terms may be gathered into one sum, from which the number of terms is made twice as small ; there will be

$$2^{p-1}-1=\frac{p(p-1)}{1\cdot 2}+\frac{p(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3\cdot 4}+\frac{p(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6}+\text{etc.},$$

the final term of which on account of the odd number p will be

$$\frac{p(p-1)(p-2)\cdots 2}{1\cdot 2\cdot 3\cdots(p-1)}=p\,.$$

But it appears the individual terms to be divisible by p ; for since p shall be a prime number and greater than any factor of the denominator, nowhere by division will it be able to be removed. On account of which if p were an odd prime, $2^{p-1}-1$ always will be able to be divided by that. Q. E. D.

OTHERWISE

If $2^{p-1}-1$ can be divided by a prime p, and in turn also the double of this 2^p-2. But there is

$$2^p=(1+1)^p=1+\frac{p}{1}+\frac{p(p-1)}{1\cdot 2}+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}+\cdots+\frac{p}{1}+1.$$

Which series of terms with the first and last cut off gives

$$\frac{p}{1}+\frac{p(p-1)}{1\cdot 2}+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}+\cdots+\frac{p(p-1)}{1\cdot 2}+p=2^p-2.$$

But it is evident any term of this series to be divisible by p, if indeed p were a prime number. On account of this always 2^{p-2} also p and therefore $2^{p-1}-1$ too can be divided by p, unless there shall be $p = 2$. Q. E. D.

4. Therefore since $2^{p-1}-1$ may be divided by an odd prime p, it is understood easily this formula $2^{m(p-1)}-1$ is able to be divided by p also, with m denoting some whole number. Whereby also all the following formulas $4^{(p-1)}-1$, $8^{(p-1)}-1$, $16^{(p-1)}-1$ etc. can be divided by a prime number p. Therefore the truth of this general theorem has been demonstrated for all cases, in which a is some power of two and p any prime number other than two.

5. Now with the help of this theorem we will show the following also:

THEOREM

With p denoting any prime number except 3 *, this formula* $3^{p-1}-1$ *will always be able to be divided by that.*

DEMONSTRATION

If $3^{p-1}-1$ can be divided by *p* with 3 excepted, then in turn 3^p-3 will be able to be divided by *p*, as often as *p* were some prime number.
Truly there is

$$3^p=(1+2)^p=1+\tfrac{p}{1}\cdot 2+\tfrac{p(p-1)}{1\cdot 2}\cdot 4+\tfrac{p(p-1)(p-2)}{1\cdot 2\cdot 3}\cdot 8+\cdots+\tfrac{p}{1}\cdot 2^{p-1}+2^p,$$

of which series the individual terms except the first and the last will be able to be divided by *p*, if indeed *p* were a prime number. Therefore this formula 3^p-2^p-1can be divided by *p*, which is equal to this :

$$3^p-3-2^p+2.$$

But 2^p-2 can always be divided by the prime number *p* ; therefore also 3^p-3.
Whereby $3^{p-1}-1$ can be divided by *p* always, as often as *p* were a prime number with 3 excepted.
Q. E. D.

6. In the same manner it is possible to progress further from this value of *a* to the following greater by one. But in order that I may prove the demonstration of the general theorem in a more neat and natural way, I present the following

THEOREM

With p denoting a prime number if a^p-a *can be divided by p, then the formula* $(a+1)^p-a-1$ *will be able to be divided by the same p also.*

DEMONSTRATION

$(a+1)^p$ may be resolved into a series in the usual manner ; there will be

$$(1+a)^p=1+\tfrac{p}{1}a+\tfrac{p(p-1)}{1\cdot 2}a^2+\tfrac{p(p-1)(p-2)}{1\cdot 2\cdot 3}a^3+\cdots+\tfrac{p}{1}a^{p-1}+a^p,$$

of which the individual terms of the series are able to be divided by *p* except the first and the last, if indeed *p* were a prime number. On account of which $(a+1)^p - a^p - 1$ allows division by *p* ; but this formula agrees with this $(a+1)^p - a - 1 - a^p + a$. But by hypothesis, $a^p - a$ can be divided by *p*, therefore also $(a+1)^p - a - 1$. Q. E. D.

7. Therefore since, because on putting $a^p - a$ able to be divided by the prime number *p*, this formula too $(a+1)^p - a - 1$ allows division by *p*, it follows also $(a+2)^p - a - 2$, likewise $(a+3)^p - a - 3$ and generally $(a+b)^p - a - b$ to be able to be divided by *p*. But on putting $a = 2$, because $2^p - 2$, as we have now shown, can be divided by *p*, it is evident the formula $(b+2)^p - b - 2$ must be allowed to be divided by *p*, whatever whole number may be substituted in place of *b*. Therefore *p* passes through the formula $a^p - a$ and consequently also this $a^{p-1} - 1$, unless $a = p$ or by a multiple of *p*. And this has demonstrated the general theorem, that I undertook to discuss.

Commentaries of the St. Petersburgh Academy of Sciences 6 (1732/3), 1738, p. 103-107 . Translated and annotated by Ian Bruce.

OBSERVATIONES DE THEOREMATE QUODAM FERMATIANO ALIISQUE AD NUMEROS PRIMOS SPECTANTIBUS

Commentarii academiae scientiarum Petropolitanae 6 (1732/3), 1738, p. 103-107

Notum est hanc quantitatem $a^n + 1$ semper habere divisores, quoties *n* sit numerus impar vel per imparem praeter unitatem divisibilis. Namque $a^{2m+1}+1$ dividi potest per $a+1$ et $a^{p(2m+1)}+1$per a^{p+1}, quicunque etiam numerus loco *a* substituatur. Contra vero si *n* fuerit eiusmodi numerus, qui per nullum numerum imparem nisi unitatem dividi possit, id quod evenit, quando *n* est dignitas binarii, nullus numeri a^n+1potest assignari divisor. Quamobrem si qui sunt numeri primi huius formae a^n+1, ii omnes comprehendantur necesse est in hac forma $a^{2^m}+1$. Neque tamen ex hoc potest concludi $a^{2^m}+1$ semper exhibere numerum primum, quicquid sit *a;* primo enim perspicuum est, si *a* sit numerus impar, istam formam divisorem habituram 2. Deinde quoque, etiamsi *a* denotet numerum parem, innumeri tamen dantur casus, quibus numerus compositus prodit. Ita haec saltem formula a^2+1 potest dividi per 5, quoties est $a=5b\pm 3$, et 30^2+1 potest dividi per 17 et 50^2+1 per 41. Simili modo 10^4+1 habet divisorem 73, 6^8+1habet divisorem 17 et $6^{128}+1$ est divisibilis per 257. At huius formae $2^{2^m}+1$, quantum ex tabulis numerorum primorum, quae quidem non ultra 100000 extenduntur, nullus detegitur casus, quo divisor aliquis locum habeat.

Hac forte aliisque rationibus FERMATIUS adductus enunciare non dubitavit $2^{2^m}+1$ semper esse numerum primum hocque ut eximium theorema WALLISIO aliisque Mathematicis Anglis demonstrandum proposuit. Ipse quidem fatetur se eius demonstrationem non habere, nihilo tamen minus asserit esse verissimum. Utilitatem eius autem hanc potissimum praedicat, quod eius ope facile sit numerum primum quovis dato maiorem exhibere, id quod sine huiusmodi universali theoremate foret difficillimum. Leguntur haec in WALLISII *Commercio Epistolico* tomo eius Operum secundo inserto, epistola penultima. Extant etiam in ipsius FERMATII operibus p. 115 sequentia : "Cum autem numeros a binario quadratice in se ductos et unitate auctos esse semper numeros primos apud me constet et iam dudum Analystis illius theorematis veritas fuerit significata, nempe esse primos 3, 5, 17, 257, 65537 etc. in infinit., nullo negotio etc." Veritas istius theorematis elucet, ut iam dixi, si pro *m* ponatur 1, 2, 3 et 4; prodeunt enim hi numeri 5, 17, 257 et 65537, qui omnes inter numeros primos in tabula reperiuntur. Sed nescio, quo fato eveniat, ut statim sequens, nempe $2^{2^5}+1$, cesset esse numerus primus; observavi enim his diebus longe alia agens posse hunc numerum dividi per 641, ut cuique

tentanti statim patebit. Est enim $2^{2^5}+1=2^{32}+1=4294967297$. Ex quo intelligi potest theorema hoc etiam in aliis, qui sequuntur, casibus fallere et hanc ob rem problema de inveniendo numero primo quovis dato maiore etiam nunc non esse solutum.

Considerabo nunc etiam formulam 2^n-1, quae, quoties *n* non est numerus primus, habet divisores, neque tantum 2^n-1, sed etiam a^n-1. Sed si *n* sit numerus primus, videri posset etiam 2^n-1 semper talem exhibere; hoc tamen asseverare nemo est ausus, quantum scio, cum tam facile potuisset refelli. Namque $2^{11}-1$, i. e. 2047, divisores habet 23 et 89, et $2^{23}-1$ dividi potest per 47. Video autem Cel. WOLFIUM non solum hoc in *Elem. Matheseos* editione altera non advertisse, ubi numeros perfectos investigat atque 2047 inter primos numerat, sed etiam 511 seu 2^9-1 pro tali habet, cum tamen sit divisibilis per 2^3-1, i. e. 7. Dat autem $2^{n-1}\left(2^n-1\right)$ numerum perfectum, quoties 2^n-1 est primus; debet ergo etiam *n* esse numerus primus. Operae igitur pretium fore existimavi eos notare casus, quibus 2^n-1 non est numerus primus, quamvis *n* sit talis. Inveni autem hoc semper fieri, si sit $n=4m-1$ atque *8m* - 1 fuerit numerus primus; tum enim 2^n-1 semper poterit dividi per *8m* -1. Hinc excludendi sunt casus sequentes: 11, 23, 83, 131, 179, 191, 239 etc., qui numeri pro *n* substituti reddunt 2^n-1 numerum compositum. Neque tamen reliqui numeri primi omnes loco *n* positi satisfaciunt, sed plures insuper excipiuntur; sic observavi $2^{37}-1$ dividi posse per 223, $2^{43}-1$ per 431, $2^{29}-1$ per 1103, $2^{73}-1$ per 439; omnes tamen excludere non est in potestate. Attamen asserere audeo praeter hos casus notatos omnes numeros primos minores quam 50 et forte quam 100 efficere $2^{n-1}\left(2^n-1\right)$ esse numerum perfectum sequentibus numeris pro *n* positis 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47, unde 11 proveniunt numeri perfecti. Deduxi has observationes ex theoremate quodam non ineleganti, cuius quidem demonstrationem quoque non habeo, verum tamen de eius veritate sum certissimus.

Theorema hoc est: *a^n-b^n semper potest dividi per $n+1$, si $n+1$ fuerit numerus primus atque a et b non possint per eum dividi;* eo autem difficiliorem puto eius demonstrationem esse, quia non est verum, nisi $n+1$ sit numerus primus. Ex hoc statim sequitur 2^n-1 semper dividi posse per $n+1$, si fuerit $n+1$ numerus primus, seu, cum omnis primus sit impar praeter 2 hicque ob conditiones theorematis, quia est $a=2$, non possit adhiberi, poterit $2^{2^m}-1$ semper dividi per $2m+1$, si $2m+1$ sit numerus primus. Quare etiam vel 2^m+1 vel 2^m-1 dividi poterit per $2m+1$. Deprehendi autem $2m+1$ posse dividi, si fuerit $m=4p+1$ vel $4p+2$; at $2^{2^m}-1$ habebit divisorem $2m+1$, si $m=4p$ vel $4p-1$. Haec persecutus in multa alia incidi theoremata non minus elegantia, quae eo magis aestimanda esse puto, quod vel demonstrari prorsus nequeant vel ex eiusmodi propositionibus sequantur, quae demonstrari non possunt; primaria igitur hic adiungere visum est.

THEOREM 1

Si fuerit n numerus primus, omnis potentia exponentis $n-1$ *per n divisa vel nihil vel* 1 *relinquit.*

THEOREMA 2

Manente n numero primo omnis potentia, cuius exponens est $n^{m-1}(n-1)$,

divisa per n^m *vel* 0 *vel* 1 *relinquit.*

THEOREMA 3

Sint m, n, p, q etc. numeri primi inaequales sitque A minimus communis dividuus eorum unitate minutorum, puta ipsorum $m-1$, $n-1$, $p-1$, $q-1$ *etc.;his positis dico omnem potentiam exponentis A ut* a^A *divisam per* $mnpq$ *etc. vel* 0 *vel* 1 *relinquere, nisi a dividi possit per aliquem horum numerorum m, n, p, q etc.*

THEOREMA 4

Denotante $2n+1$ *numerum primum poterit* 3^n+1 *dividi per* $2n+1$, *si sit vel* $n=6p+2$ *vel* $n=6p+3$; *at* 3^n-1 *dividi poterit per* $2n+1$, *si sit vel* $n=6p$ *vel* $n=6p-1$.

THEOREMA 5

3^n+2^n *potest dividi per* $2n+1$, si *sit n = vel* $12p+3$ *vel* $12p+5$ *vel* $12p+6$ *vel* $12p+8$. Atque 3^n-2^n *potest dividi per* $2n+1$, si *sit n = vel* $12p$ *vel* $12p+2$ *vel* $12p+9$ *vel* $12p+11$.

THEOREMA 6

Sub iisdem conditionibus, quibus 3^n+2^n, *poterit etiam* 6^n+1 *dividi per* $2n+1$; *atque* 6^n-1 *sub iisdem, quibus* 3^n-2^n.

EPISTOLA XLV.

Kenelm Digby ad D. Joh. Wallis.

Noble *Sir,*

I Received lately from Mons. *Fermat,* the enclosed written paper, with a desire from him to conveigh it to my Lord *Brouncker* and your self: I hope you have received mine of the 8 and 25 of May. A main errand of this present Letter is humbly to take my leave of you for some months ; for I am ere long going a journey that will take up all this summer at the least. When I return to *Paris,* I will give you an account of it by presenting my humble respects unto you. In the mean time I cease further troubling you, and remain

Paris 19 *June* *Noble Sir,*

Commentaries of the St. Petersburgh Academy of Sciences 6 (1732/3), 1738, p. 103-107 . Translated and annotated by Ian Bruce.

1658. *Your most humble and most obedient*
servant, that highly honoureth you,
KENELM DIGBY.

EPISTOLA XLVI.

D. Fermatii ad D.Kenelmum Digby.
praecedenti inclusa.

Illustrissimos Viros Vicecomitem *Brouncker & Johannem Wallisium* quaestionum numericarum a me propositarum solutiones tandem dedisse legitimas libens agnosco, imo & gaudeo. Noluerunt Viri Clarissimi vel unico momento impares sese aut κτλονας questionibus propositis confiteri ; mallem ipsos & quaestiones dignas laboribus Anglicis statim agnovisse, & postquam adepti ipsarum solutiones fuissent, triumphum eo illustriorem egisse quo certamen magis arduum apparuisset. Contrarium ipsis visum est. Id sane gloria Illustrissimae & Ingeniosissimae nationis condonandum. Verum ut deinceps ingenue utrimque agamus, fatentur Galli propositis questionibus satisfecisse Anglos : Sed fateantur vicissim Angli quaestiones ipsas dignas fuisse quae ipsis proponerentur, nec dedignentur in posterum numerorum integrorum naturam accuratius examinare & introspicere, imo & doctrinam istam, qua pollent ingenii vi & subtilitate, propagare. Quod ut ab illis libentius impetremus, *Diophantum* ipsum & celeberrimum illius interpretem *Bachetum* ad authoritatem rei proponimus. Supponit *Diophantus* in plerisque libri 4^{i} & 5^{i} questionibus numerum omnem integrum vel esse quadratum vel ex duobus aut tribus aut quatuor quadratis compositum. Id sibi *Bachetus* in commentariis ad questionem $3l^{am}$ libri 4^{i} perfecta demonstratione assequi nondum licuisse fatetur. Id *Renatus* ipse *Descartes* incognitum sibi ingenue declarat in Epistola quadam quam propediem edendam accepimus, imo & viam qua huc perveniatur difficillimam & abstrusissimam esse non diffitetur. Cur igitur de propositionis illius dignitate dubitemus, non video. Eius tamen perfectam demonstrationem a me inventam moneo Viros Clarissimos. Possem & plerasque adjungere propofitiones non solum celeberrimas, sed & firmissimis demonstrationibus probatas. Exempli causa.

Omnis numerus primus qui unitate superat quaternarii multiplicem, est compositus ex duobus quadratis. Huiusmodi sunt 5,13**,** 17, 29, 37,41, &c. Omnis numerus primus qui vel unitate vel ternario superat ternarii multiplicem est: compositus ex quadrato & triplo alterius quadrati, talis sunt 7, 13, 19, 31, 37,43,&c. Omnis numerus primus qui vel unitate vel ternario fuperat octonarii multiplicem, componitur ex quadrato & duplo alterius quadrati, talis sunt 3, 11, 17,19, 41, 43, &c.

Sed & praecedentem *Bacheti* propositionem generaliter olim Domino de *Saint Croise* proposuimus, eiusque demonstrationem non ignoramus.

Omnis numerus integer vel est triangulus, ut ex duobus, aut tribus triangulis compositus.

Est quadratus vel ex duobus, tribus, aut quatuor quadratis compositus.

Est pentagonus vel ex duobus, tribus, quatuor, aut quinque pentagonis compositus.

Est hexagonus vel ex duobus, tribus, quatuor, quinque vel sex hexagonis compositus.

Et sic uniformi in infinitum enuntiatione.

Commentaries of the St. Petersburgh Academy of Sciences 6 (1732/3), 1738, p. 103-107 . Translated and annotated by Ian Bruce.

Haec omnia & alia infinita quae ad numeros integros spectant, quaeque a nobis & inventa & generaliter demonstrata sunt, possemus & proponere viris Clarissimis, & proponendo negotium saltem aliquod ipsius facessere. Sed ingenuitatem Gallicam sapient magis propositiones aliquot quarum demonstrationem a nobis ignorari non diffitemur, licet de earum veritate nobis constet. Meminimus *Archimedem* non dedignatum propositionibus *Canonis*, veris quidem, sed tamen indemonstratis, ultimam manum imponere, earumque veritatem demonstrationibus illis subtilissimis confirmare. Cur igitur simile auxilium a viris Clarissimis non expectem, *Canon* scilicet Gallicus ab *Archimedibus* Anglis?

1. Potestates omnes numeri 2, quarum exponentes sunt termini progressionis Geometricae eiusdem numeri 2, unitate auctae sunt numeri primi.
Exponatur progressio Geometrica 2. cum suis exponentibus.

1	2	3	4	5	6	7	8
2	4	8	16	32	64	128	256

Primus terminus 2. auctus unitate facit 3. qui est numerus primus. Secundus terminus 4. auctus unitate facit 5. qui est pariter numerus primus. Quartus terminus 16 auctus unitate facit 17 numerum primum. Octavus terminus 256. auctus unitate facit 257 numerum primum. Sume generaliter omnes potestates 2. quarum exponentes funt numeri progressionis, idem accidet. Nam si sumas deinde decimum fextum terminum qui est 65536. ille auctus unitate faciet 65537. numerum primum. Hoc pacto potest dari & assignari nullo negotio numerus primus dato quocunque numero major. Quaeritur demonstratio illius propositionis, pulchrae sane sed & verissimae, cuius ope, ut iam diximus, problema alias difficillimum solvi statim potest. Dato quovis numero invenire numerum primum dato numero majorem. Huius clavis beneficio reserabunt fortasse Viri Clarissimi mysterium omne de numeris primis, hoc est Dato numero quovis invenire via brevissima & facillima an sit primus vel compositus.

2. Deinde. Duplum cuislibet numeri primi unitate minoris quam multiplex octonarii, componitur ex tribus quadratis. Esto quilibet numerus primus unitate minor quam octonarii multiplex, (ut sunt 7, 23, 31, 47, &c.) eorum duplum ut 14, 46, 62, 94, componitur ex tribus quadratis. Propositionem illam veram asserimus, sed Cononis modo nondum aut asserente aut demonstrate Arehimede.

3. Si duo numeri primi desinentes aut in 3. aut in 7. & quaternarii multiplicem ternario superantes inter se ducantur. Productum componitur ex quadrato & quintuplo alterius quadrati. Tales funt numeri 3, 7, 23, 43, 47, 67, &c. Sume duos ex illis exempli gratia 7 & 23 quod fub iis sit 161 componetur ex quadrato & quintuplo alterius quadrati; nam 81 quadratus & quintuplum 16 aequantur 161. Id verum asserimus generaliter, & demonstrationem tantum expectamus. Singulorum autem ex ipfis quadrati componuntur ex quadrato &quintuplo alterius quadrati, quod & demonstrandum proponitur.

Sed ne demonstrationibus nimium fortasse deesse videamur, sequentem propositionem & asserimus & possumus demonstrare.

Nullus numerus triangulus praeter unitatem aequatur numero quadrato-quadrato.

Sunt trianguli ut norunt omnes, 1,3,6,10,15,21,28,36,45, &c. Nullus omnino facta in infinitum progressione praeter solam unitatem erit quadrato-quadratus.
etc. etc.

Commentaries of the St. Petersburgh Academy of Sciences 6 (1732/3), 1738, p. 103-107 . Translated and annotated by Ian Bruce.
16

THEOREMATUM QUORUNDAM AD NUMEROS PRIMOS SPECTANTIUM DEMONSTRATIO

Commentaries of the St.Petersburg Academy of Sciences 8 (1736), 1741, p.141-146.
Now accorded the Enestrom index E54.

1. Plurima quondam a FERMATIO theoremata arithmetica, sed sine demonstrationibus in medium sunt prolata, in quibus, si vera essent, non solum eximiae numerorum proprietates continerentur, verum etiam ipsa numerorum scientia, quae plerumque Analyseos limites excedere videtur, vehementer esset promota. Quamvis autem iste insignis Geometra de pluribus, quae proposuit, theorematis asseruerit se ea vel demonstrare posse vel saltem de eorum veritate esse certum, tamen nusquam, quantum mihi constat, demonstrationes exposuit. Quin potius FERMATIUS videtur maximam theorematum suorum numericorum partem per inductionem esse assecutus, quippe quae via fere unica ad huiusmodi proprietates eruendas patere videatur. At vero quam parum inductionibus in hoc negotio tribui possit, pluribus exemplis possem declarare; ex quibus autem unicum ab ipso FERMATIO desumtum attulisse sufficiat. Loquor nimirum de illo theoremate, cuius falsitatem iam aliquot ab hinc annis ostendi, quo FERMATIUS asserit omnes numeros hac forma $2^{2^{n+1}}+1$ comprehensos esse numeros primos. Ad veritatem autem huius propositionis evincendam inductio omnino sufficere videtur. Nam praeterquam quod omnes isti numeri minores quam 100000 sint revera primi, demonstrari etiam facile potest nullum numerum primum 600 non excedentem hanc formulam $2^{2^{n+1}}$, quantumvis magnus etiam numerus pro *n* substituatur, metiri. Cum tamen nihilominus constet hanc propositionem veritati non esse consentaneam, facile intelligitur, quantum inductio in huiusmodi speculationibus valeat.

2. Hanc ob rationem omnes huiusmodi numerorum proprietates, quae sola inductione nituntur, tam diu pro incertis habendas esse arbitror, donec illae vel apodicticis demonstrationibus muniantur vel omnino refellantur. Non plus etiam illis theorematis, quae ego ipse illi schediasmati, in quo de memorato theoremate FERMATIANO numerisque perfectis tractavi, subieci, fidendum esse censerem, si tantum inductionibus, qua via quidem sola tum temporis ad eorum cognitionem perveni, niterentur. Nunc vero, postquam peculiari methodo demonstrationes horum theorematum firmissimas sum adeptus, de veritate eorum non amplius est dubitandum. Quocirca tam ad veritatem illorum theorematum ostendendam quam ad methodum ipsam, qua demonstrationes has inveni, exponendam, quae forte etiam in aliis numerorum investigationibus utilitatem afferre poterit, in hac dissertatione meas demonstrationes explicare constitui.

3. Propositio autem, quam hic demonstrandam suscepi, est sequens:

Significante p numerum primum formula $a^{p-1}-1$ *semper per p dividi poterit, nisi a per p dividi queat.*

Commentaries of the St. Petersburgh Academy of Sciences 6 (1732/3), 1738, p. 103-107 . Translated and annotated by Ian Bruce.

Ex hac enim propositione demonstrata sponte reliquorum theorematum veritas fluit. Casum quidem formulae propositae, quo est $a = 2$, iam ab aliquo tempore demonstratum dedi ; attamen tum demonstrationem ad generalem formulam extendere non licuit. Quamobrem primo huius casus probationem afferre conveniet, quo transitus ad generaliora eo facilior reddatur. Demonstranda igitur erit sequens propositio:

Significante p numerum primum imparem quemcunque formula $2^{p-1}-1$ *semper per p dividi poterit.*

DEMONSTRATIO

Loco 2 ponatur 1 + 1 eritque

$$(1+1)^{p-1} = 1 + \frac{p-1}{1} + \frac{(p-1)(p-2)}{1\cdot 2} + \frac{(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3} + \frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4} + \text{etc.},$$

cuius seriei terminorum numerus est $= p$ et proinde impar. Praeterea quilibet terminus, quamvis habeat fractionis speciem, dabit numerum integrum; quisque enim numerator, uti satis constat, per suum denominatorem dividi potest. Demto igitur seriei termino primo 1 erit

$$(1+1)^{p-1} - 1 = 2^{p-1} - 1 = \frac{p-1}{1} + \frac{(p-1)(p-2)}{1\cdot 2} + \frac{(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3} + \frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4} + \text{etc.},$$

quorum numerus est $= p-1$ et propterea par. Colligantur igitur bini quique termini in unanl summam, quo terminorum numerus fiat duplo minor; erit

$$2^{p-1} - 1 = \frac{p(p-1)}{1\cdot 2} + \frac{p(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3\cdot 4} + \frac{p(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6} + \text{etc.},$$

cuius seriei ultimus terminus ob *p* numerum imparem erit

$$\frac{p(p-1)(p-2)\cdots 2}{1\cdot 2\cdot 3\cdots (p-1)} = p\,.$$

Apparet autem singulos terminos per *p* esse divisibiles; nam cum *p* sit numerus primus et maior quam ullus denominatorum factor, nusquam divisione tolli poterit. Quamobrem si fuerit *p* numerus primus impar, per illum semper $2^{p-1}-1$ dividi poterit. Q. E. D.

ALITER

Si $2^{p-1}-1$ per numerum primum *p* dividi potest, dividi quoque poterit eius duplum $2^p - 2$ et vicissim. At est

$$2^p = (1+1)^p = 1 + \frac{p}{1} + \frac{p(p-1)}{1\cdot 2} + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3} + \cdots + \frac{p}{1} + 1.$$

Quae series terminis primo et ultimo truncata dat

$$\frac{p}{1}+\frac{p(p-1)}{1\cdot 2}+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}+\cdots+\frac{p(p-1)}{1\cdot 2}+p=2^p-2.$$

Perspicuum autem est istius seriei quemvis terminum per p esse divisibilem, siquidem p fuerit numerus primus. Quamobrem etiam semper 2^{p-2} per p et propterea quoque $2^{p-1}-1$ per p dividi poterit, nisi sit $p = 2$. Q. E. D.

4. Cum igitur $2^{p-1}-1$ per numerum primum imparem p dividi queat, facile intelligitur per p quoque dividi posse hanc formulam $2^{m(p-1)}-1$ denotante m numerum quemcunque integrum. Quare sequentes formulae quoque omnes
$4^{(p-1)}-1,\quad 8^{(p-1)}-1,\quad 16^{(p-1)}-1$ etc. per numerum primum p dividi poterunt.
Demonstrata igitur est veritas theorematis generalis pro omnibus casibus, quibus a est quaevis binarii potestas et p quicunque numerus primus praeter binarium.

5. Demonstrato nunc hoc theoremate eius ope sequens quoque demonstrabimus

THEOREMA

Denotante p numerum primum quemcunque praeter 3 *per illum semper haec formula* $3^{p-1}-1$ *dividi poterit.*

DEMONSTRATIO

Si $3^{p-1}-1$ per numerum primum p excepto 3 dividi potest, tum 3^p-3 per p dividi poterit, quoties p fuerit numerus primus quicunque, et vicissim.
Est vero .

$$3^p=(1+2)^p=1+\frac{p}{1}\cdot 2+\frac{p(p-1)}{1\cdot 2}\cdot 4+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}\cdot 8+\cdots+\frac{p}{1}\cdot 2^{p-1}+2^p,$$

cuius seriei singuli termini praeter primum et ultimum per p dividi poterunt, si quidem p fuerit numerus primus. Per p igitur dividi potest ista formula 3^p-2^p-1, quae aequalis est huic

$$3^p-3-2^p+2.$$

At 2^p-2 semper per p numerum primum dividi potest; ergo etiam 3^p-3.
Quare $3^{p-1}-1$ semper per p dividi potest, quoties p fuerit numerus primus excepto 3.
Q. E. D.

6. Eodem modo ulterius progredi liceret ab hoc ipsius a valore ad sequentem unitate maiorem. Sed quo demonstrationem generalis theorematis magis concinnam magisque genuinam efficiam, sequens praemitto

THEOREMA

Commentaries of the St. Petersburgh Academy of Sciences 6 (1732/3), 1738, p. 103-107 . Translated and annotated by Ian Bruce.

Denotante p numerum primum si $a^p - a$ *per p dividi potest, tum per idem p quoque formula* $(a+1)^p - a - 1$ *dividi poterit.*

DEMONSTRATIO

Resolvatur $(a+1)^p$ consueto more in seriem; erit

$$(1+a)^p = 1 + \frac{p}{1}a + \frac{p(p-1)}{1\cdot 2}a^2 + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}a^3 + \cdots + \frac{p}{1}a^{p-1} + a^p,$$

cuius seriei singuli termini per *p* dividi possunt praeter primum et ultimum, si quidem *p* fuerit numerus primus. Quamobrem $(a+1)^p - a^p - 1$ divisionem per *p* admittet; haec autem formula congruit cum hac $(a+1)^p - a - 1 - a^p + a$. At $a^p - a$ per hypothesin per *p* dividi potest, ergo etiam $(a+1)^p - a - 1$. Q. E. D.

7. Cum igitur, posito quod $a^p - a$ per *p* numerum primum dividi queat, per *p* quoque haec formula $(a+1)^p - a - 1$ divisionem admittat, sequitur etiam $(a+2)^p - a - 2$, item $(a+3)^p - a - 3$ et generaliter $(a+b)^p - a - b$ per *p* dividi posse. Posito autem $a = 2$, quia $2^p - 2$, uti iam demonstravimus, per *p* dividi potest, perspicuum est formulam $(b+2)^p - b - 2$ divisionem per *p* admittere debere, quicunque integer numerus loco *b* substituatur.

Metietur ergo *p* formulam $a^p - a$ et consequenter etiam hanc $a^{p-1} - 1$, nisi fuerit $a = p$ vel multiplo ipsius *p.* Atque haec est demonstratio generalis theorematis, quam tradere suscepi.