New Commentaries of the St.Petersburg Academy of Sciences 1 (1747/48) 1750, pp. 20 - 48. ***Translated and annotated by Ian Bruce.***

THEOREMS CONCERNING THE DIVISORS OF NUMBERS

L. Euler (*E134*)

In any time you please the greatest geometers have recognised that the most outstanding properties are hidden in the nature of numbers, the recognition of which would greatly extend the boundaries of mathematics. Indeed in the first place the theory of numbers is seen on consideration to refer to the principles of arithmetic and scarcely anything which may require any cleverness or analytical strength is thought to be present in that. But those who have been concerned more carefully with this generation, have not only uncovered the most difficult truths by demonstration, but also truths of such a kind of which the certainty is perceived, even if that may not be demonstrated. Most theorems of this kind have been advanced by the distinguished geometer Fermat, the truth of which, although the demonstration may be hidden, none the less is seen to prevail. And this especially deserves all the attention that truths be given in such a manner in pure mathematics, which may be permitted to be recognised by us, since we may not yet be able to demonstrate these ; and this thus arises from the use of arithmetic, which is accustomed still to be used and considered before the remaining parts of mathematics; I do not intend to confirm readily to this view [*i.e*. that proofs may be generated from arithmetic], nor to that view that similar truths may be found from the remaining parts of mathematics [*i.e*. because those may be more difficult]. Certainly in geometry no proposition occurs, of which either the truth or falseness cannot be shown by the strongest reasoning. Therefore since any more abstruse truth may be considered there, so that its demonstration may appear less accessible, certainly in arithmetic we will not be able to avoid all abstruseness, since it depends on the nature of numbers. Indeed these truths are not absent in the great mathematical works of men, who judge truths of this kind completely sterile and thus unworthy, on an investigation of which in any work it may be put in place; but beyond which because knowledge of all truth shall itself be remarkable, even if it may be seen to be abhorred in common use, all truths, which it is allowed for us to know, are taken to be so greatly interconnected that nothing without fear may be repudiated evidently as useless. Thereupon also a certain proposition may be considered to be prepared thus, so that either it shall be true or false, thence nothing shall be in excess to our usefulness, yet the method itself, by which the truth or falseness is shown, is accustomed generally to reveal a way for us for other useful truths becoming known.

Hence on this account I believe to have expended my work and study in a useful manner in the investigation of demonstrations of certain propositions, in which certain properties about the divisors of numbers may be included. Nor truly is this teaching about divisors without any use, moreover sometimes in analysis the usefulness is outstanding and not to be belittled. Truly without doubt in the first place, why may not a method of reasoning for which I have a use not be able to bring a little help in other more serious investigations.

New Commentaries of the St.Petersburg Academy of Sciences 1 (1747/48) 1750, pp. 20 - 48. ***Translated and annotated by Ian Bruce.***

Moreover the propositions which I demonstrate here, consider the divisors of numbers contained in this formula $a^n + b^n$, some of which now have been published by the aforementioned Fermat, but without demonstration. Therefore because here the discussion put in place continually concerns whole numbers , all the letters of the alphabet here will indicate whole numbers constantly.

THEOREM 1

1. *If p were a prime number, any number held in this form* $(a+b)^p - a^p - b^p$ *will be divisible by p.*

DEMONSTRATION

If the binomial $(a+b)^p$ may be set out in the usual manner, there will be

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

with which expression substituted and with the two terms, which have the same fraction taken together, there will be

$$(a+b)^p - a^p - b^p = \tfrac{p}{1}ab\left(a^{p-2} + b^{p-2}\right) + \tfrac{p(p-1)}{1\cdot 2}a^2b^2\left(a^{p-4} + b^{p-4}\right)$$
$$+ \tfrac{p(p-1)(p-2)}{1\cdot 2\cdot 3}a^3b^3\left(a^{p-6} + b^{p-6}\right) + \tfrac{p(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3\cdot 4}a^4b^4\left(a^{p-8} + b^{p-8}\right) + \text{etc.}$$

Here it is required to note in the first place, all the fractions under whatever form of fraction they may appear, nevertheless are whole numbers, since they may show, as agreed, figured numbers. Therefore any fraction, since it may have the factor *p,* will be divisible by *p,* unless that somewhere either may be taken away or divided completely by a factor of the denominator. But all the factors of the denominator everywhere are less than *p*, which thus cannot increase beyond $\frac{1}{2}p$, and thus the factor *p* of the numerator never can be removed by division. Thereupon since *p* by hypothesis shall be a prime number, that can never be diminished by division. On account of which the individual fractions $\frac{p}{1}$, $\frac{p(p-1)}{1\cdot 2}$, $\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}$ etc. and hence the whole expression $(a+b)^p - a^p - b^p$ will be divided always by the number *p,* if indeed it were a prime number. Q. E. D.

COROLLARY 1

2. Therefore if there may be put $a=1$ and $b=1$, there will be 2^p-2 divisible always by *p,* if *p* were a certain prime number. Therefore since there shall be $2^p-2=2\left(2^{p-1}-1\right)$, the other factor of this is required to be divisible by *p*. But unless there shall be $p=2$, the first factor 2 is not divisible by *p*; from which it follows the form $2^{p-1}-1$ is always divisible by *p,* if *p* were a prime number besides two.

COROLLARY 2

3. Therefore with prime numbers put for *p* successively, there will be 2^2-1 divisible by 3, 2^4-1 by 5, 2^6-1 by 7, $2^{10}-1$ by 11 etc., which with small numbers becomes evident by itself, but it will be sure equally with the biggest numbers. Thus since 641 shall be a prime number, this number $2^{640}-1$ by necessity will be divisible by 641, or if the power 2^{640} may be divided by 641, after the division there will be left over the remainder $=1$.

THEOREM 2

4. *If each of these formulas* a^p-a and b^p-b *were divisible by the prime number p, then this formula also* $(a+b)^p-a-b$ *will be divisible by the same prime number p.*

DEMONSTRATION

Since by § 1 $(a+b)^p-a^p-b^p$ shall be divisible by the number *p,* if it were prime, and here the formulas a^p-a and b^p-b may be assumed divisible by *p,* also the sum of these three formulas, evidently $(a+b)^p-a-b$, will be divisible by *p,* if it were prime. Q. E. D.

COROLLARIUM 1

5. If there may be put $b=1$ since $1^p-1=0$ shall be divisible by *p,* it follows, if the formula a^p-a were divisible by *p,* then also the formula $(a+1)^p-a-1$ becomes divisible by *p*.

COROLLARY 2

6. Therefore since with the formula a^p-a assumed to be divisible by *p* there shall also be the formula $(a+1)^p-a-1$ divisible by *p,* in a similar manner from the same hypothesis there will be also the formula $(a+2)^p-a-2$ and hence again this $(a+3)^p-a-3$ etc., and generally this c^p-c will be divisible by *p.*

THEOREM 3

7. *If p were a prime number, each number of this form* $c^p - c$ *will be divisible by p.*

DEMONSTRATION

If in § 6 there may be put $a = 1$, since $a^p - a = 0$ shall be divisible by p, it follows that also two formulas $2^p - 2$, $3^p - 3$, $4^p - 4$ etc. and hence generally $c^p - c$ to be divisible by the prime number *p*. Q. E. D.

COROLLARY 1

8. Therefore any whole number may be assumed for *c*, with *p* denoting a prime number all the numbers contained in this form $c^p - c$ will be divisible by *p*.

COROLLARY 2

9. But since there shall be $c^p - c = c\left(c^{p-1} - 1\right)$, either the number *c* or $c^{p-1} - 1$ will be divisible by *p*. But it is evident each cannot likewise be divisible by *p*. Whereby if the number *c* were not divisible by *p*, this form $c^{p-1} - 1$ surely will be divisible by *p*.

COROLLARY 3

10. Therefore if *p* were a prime number, all the numbers contained in this form $a^{p-1} - 1$ will be divisible by *p* with these cases excepted, in which the number *a* itself is divisible by *p*.

THEOREM 4

11. *If neither of the numbers a and b were divisible by the prime number p, then each number of this form* $a^{p-1} - b^{p-1}$ *will be divisible by p.*

DEMONSTRATION

Since neither *a* nor *b* shall be divisible by *p* and *p* may denote a prime number, then this form $a^{p-1} - 1$ as well as this $b^{p-1} - 1$ will be divisible by p. Hence therefore the difference of these formulas $a^{p-1} - b^{p-1}$ also will be divisible by *p*. Q. E. D.

COROLLARY 1

12. Since each prime number besides two, of which the ratio on being divided by itself is evident, shall be odd, $2m + 1$ may be put for *p* and it will be evident all the numbers contained in this form $a^{2m} - b^{2m}$ are divisible by $p = 2m + 1$, if indeed neither *a* nor *b* separately were divisible by $2m + 1$.

COROLLARY 2

13. Because *b* is not divisible by $2m+1$, also b^{2m} and $2b^{2m}$ will not be divisible by $2m+1$. Whereby if $2b^{2m}$ may be added to the formula $a^{2m}-b^{2m}$, which is divisible by $2m+1$, the formula $a^{2m}+b^{2m}$ will be produced, which will not be divisible by $2m+1$, unless each number *a* and *b* separately shall be divisible by $2m+1$.

COROLLARIUM 3

14. Because on account of the even number *2m*, the formula $a^{2m}-b^{2m}$ has factors $\left(a^m-b^m\right)\left(a^m+b^m\right)$, it is necessary that of these factors one shall be divisible by $2m+1$; but both likewise shall be unable to be divided by the number $2m+1$. Whereby if $2m+1$ were a prime number and neither *a* nor *b* shall be divisible by $2m+1$, then either a^m-b^m or a^m+b^m will be divisible by $2m+1$.

COROLLARY 4

15. If *m* shall be an even number, consider $=2n$, and a^m-b^m or $a^{2n}-b^{2n}$ divisible by $2m+1=4n+1$, then because of the same reason either a^n-b^n or a^n+b^n will be divisible by the prime number $4n+1$.

THEOREM 5

16. *The sum of two squares* $aa+bb$ *at no time can be divided by any prime number of this form* $4n-1$, *unless the root of each a and b separately shall be divided by* $4n-1$.

DEMONSTRATION

If $4n-1$ were a prime number and *a* and *b* shall not be divisible by that, then $a^{4n-2}-b^{4n-2}$ will be divisible by $4n-1$ (§ 11) and hence this formula $a^{4n-2}+b^{4n-2}$ will not be divisible by $4n-1$ [§ 13] nor therefore any factor of that. But since $4n-2=2\left(2n-1\right)$ shall be an even number multiplied oddly, the formula $a^{4n-2}+b^{4n-2}$ has the factor $aa+bb$*;* whereby it is unable to happen, that this factor $aa+bb$, that is any sum of two squares, shall be divisible by $4n-1$.
Q. E. D.

[Thus, there will be $a^{4n-2}+b^{4n-2}=\left(a^2+b^2\right)\left(a^{4n-4}-a^{4n-6}b^2+a^{4n-8}b^4+\cdots+b^{4n-4}\right)$, etc.]

COROLLARY 1

17. Since all prime numbers may be recalled to the form $4n+1$ or to this $4n-1$, if $4n-1$ were not a prime number, it will have a divisor of the form $4n-1$; in as much as a number of the form $4n-1$ at no time can result from pure numbers of the form $4n+1$. Whereby since the sum of two squares will be able to be divided by no prime number of

the form $4n-1$, also by it will be unable to be divided by any number of the form $4n-1$, even if it shall not be prime.

COROLLARY 2

18. Therefore the sum of two squares $aa+bb$ is divisible by no number of this series 3, 7, 11, 15, 19, 23, 27, 31, 35 etc.. Therefore all the prime numbers beyond two, which at no time can be the divisors of the sum of two squares, may be contained in this form $4n+1$, if indeed the numbers *a* and *b* do not have a common divisor between themselves.

COROLLARY 3

19. Since each number shall be either a prime or a product from primes, the sum of two squares will have no prime number for a divisor, unless the ones which are contained in this form $4n+1$. Therefore the prime divisors of the sum of two squares will be contained in this series 2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc.

SCHOLIUM

20. Because it is understood easily that a number of this form $4n-1$ at no time will be able to be the sum of two squares. Indeed square numbers shall be either even or odd ; those may be contained in this form 4*a*, these truly in this $4b+1$. Whereby so that the sum of two squares shall be an odd number, there is required to be one part even, the other odd ; hence the form $4a+4b+1$ or $4n+1$ arises and thus no number of this form $4n-1$ can be the sum of two squares. Because truly the sum of two squares indeed allows no divisors of the form $4n-1$, it has always been confirmed from all the writers of the method of Diophantine ; but no one at any time, as far as I know, has demonstrated that except for Fermat, but who at no time published his demonstration, thus so that I may be considered the first indeed to have demonstrated this truth publicly : *No number either of this form* $4n-1$ *or by a number divisible of the same form at any time is able to divide the sum of two squares.* Hence it follows therefore each sum of two squares of primes between themselves or to be a prime number, or with two excepted not to have other divisors, unless those which may be present in the form $4n+1$.

THEOREM 6

21. *All the divisors of the sum of two biquadratics prime between themselves are either* 2 *or numbers of this form* $8n+1$.

DEMONSTRATION

Let a^4 and b^4 be two biquadratics prime between themselves [*i.e.* relatively prime] ; each will be either odd or one even and the other odd; in the first case the divisor of the sum a^4+b^4 will be 2, truly in the other case odd divisors, if there were which, will be contained in this form $4n+1$. For since the biquadratics likewise shall be squares, no factor of the form $4n-1$ will be present (§ 16). But the numbers $4n+1$ are recalled either to this form $8n+1$ or to this $8n-3$. But I say no number of the form $8n-3$ is able to be a divisor of the sum of two biquadratics. Towards demonstrating this, let $8n-3$ be the first prime number and this form $a^{8n-4}-b^{8n-4}$ will be divisible by $8n-3$, from

which it follows the form $a^{8n-4}+b^{8n-4}$ absolutely will not be divisible by the number $8n-3$ [§13], unless each number *a* and *b* separately may admit division, but which case is excluded from the assumption, because both numbers *a* and *b* shall be prime between themselves. Therefore since the form $a^{8n-4}+b^{8n-4}=a^{4(2n-1)}+b^{4(2n-1)}$ may be unable to be divided by $8n-3$, also no factor of this can be divided by $8n-3$. But on account of the odd number $2n-1$ the factor of that form will be a^4+b^4 which therefore cannot be divided by any prime number of the form $8n-3$. Hence all prime numbers beyond two, which at any time divide the form a^4+b^4, will be of this kind $8n+1$. But from the multiplication of two or more such divisions at no time does a number of the form $8n-3$ arise; from which it follows on no account a number of this form $8n-3$, whether it shall be prime or composite, divides the sum of two squares prime between themselves. Q. E. D.

COROLLARY 1

22. Since all odd numbers may be contained in one of the four forms $8n\pm1$ and $8n\pm3$, besides the numbers contained in the first form $8n+1$ no other is able to be the divisor of the sum of two biquadratics.

COROLLARY 2

23. Therefore all the prime divisors of the sum of two biquadratics prime between themselves will be either 2 or contained in the series 17, 41, 73, 89, 97, 113, 137, 193 etc., which includes all the prime numbers of the form $8n+1$.

COROLLARIUM 3

24. If from which therefore a number, for example *N*, were the sum of two biquadratics, then this either is prime or will not have other divisors, other than those which may be contained in the form $8n+1$; by which the investigation of divisors is concluded in a wonderful manner.

COROLLARY 4

25. Therefore no number, which does not have a divisor contained in the form $8n+1$, will be the sum of two biquadratics, unless perhaps it may have four equal divisors, which in the consideration of biquadratics is normally rejected.

THEOREM 7

26. *All divisors of numbers of such a form* a^8+b^8*, if indeed a and b are numbers prime between themselves, are either* 2 *or may be contained in this form* $16n+1$.

DEMONSTRATION

Because a^8 and b^8 likewise are biquadratics, the sum of these a^8+b^8 does not allow other divisors, unless those which may be contained in the form $8n+1$. But numbers contained in this form $8n+1$ are either $16n+1$ or $16n-7$. Let $16n-7$ be a prime number and the forms $a^{16n-8}+b^{16n-8}$ or $a^{8(2n-1)}+b^{8(2n-1)}$ cannot be divided by that (§ 13) nor

therefore any factor of this. Truly on account of the odd number $2n-1$ this form a^8+b^8 has an odd divisor, which therefore will be divisible by no prime number $16n-7$ and therefore it cannot have other prime divisors , except those which may be contained in the form $16n+1$. But from the multiplication of two or more numbers of such a kind $16n-7$ a product of this form arises always nor at any time can a number of the form $16n-7$ result. From which since no number of the form $16n-7$ will be able to be a divisor a^8+b^8, it is necessary, that all the divisors of this form a^8+b^8, if it has which, whether they shall be prime or composite, may always be contained in this formula $16n+1$.
Q. E. D.

COROLLARY 1

27. Therefore no number, which is not included in this form $16n+1$, can at any time be a divisor of the sum of two powers of the eighth order of primes between themselves.

COROLLARY 2

28. Therefore id from these it should be wished to investigate the divisors of this form a^8+b^8 of a certain number, this division by no other prime numbers except contained in the form $16n+1$ may be considered, since it may be demonstrated that all the remaining prime numbers cannot be divisors of this form.

THEOREM 8

29. *The sum of two powers of this kind* $a^{2^m}+b^{2^m}$, *the exponent of which is a power of two, do not admit other divisors, unless which may be contained in this form* $2^{m+1}n+1$.

DEMONSTRATION

Just as we have shown all the divisors of the form a^2+b^2 to be contained in this form $4n+1$ and hence we have evinced further divisors of the form a^4+b^4 in $8n+1$ and of the form a^8+b^8 contained in $16n+1$, thus in a similar manner it can be shown that the form $a^{16}+b^{16}$ admits no other divisors unless contained in the formula $32n+1$. Thereupon again we understand the forms $a^{32}+b^{32}$, $a^{64}+b^{64}$ etc. cannot have divisors unless which may be included in the form $64n+1$, $128n+1$ etc. And thus in general it will appear no other divisors be given of the form $a^{2^m}+b^{2^m}$, unless which may be contained in the formula $2^{m+1}n+1$. Q. E. D.

COROLLARY 1

30. Therefore no prime number, which is not included in this form $2^{m+1}n+1$, at any time can be a divisor of any number contained in this form $a^{2^m}+b^{2^m}$.

COROLLARY 2

31. Therefore seeking divisors of a number of this kind $a^{2^m}+b^{2^m}$ may be consumed needlessly in its own effort , if it may be wished to test the division by other prime numbers besides those which the form $2^{m+1}n+1$ supplies.

SCHOLIUM 1

32. Fermat had asserted as true that all numbers arising from this form $2^{2^n}+1$ are prime, even if he may have conceded frankly that it cannot itself be demonstrated ; and hence another most difficult problem is attempted to be resolved, from which a prime number will be sought greater than a given prime number. But from the final theorem it is evident, unless the number $2^{m+1}n+1$ shall be prime, besides such it is not possible to have other divisors, which may be contained in the formula $2^{m+1}n+1$. Therefore since I might have wished to examine the truth of this pronouncement of Fermat for the case $2^{32}+1$, I have come upon this huge shortcut, so that I had no need to test the division by other prime numbers besides these which the formula $64n+1$ supplies. Therefore at this point with the inquiry reduced, soon I seized upon the prime number 641 on putting $n=10$ to be the divisor of the number $2^{32}+1$, from which the problem mentioned, whereby from a given prime number a greater may be required, even now remains unsolved.

SCHOLIUM 2

33. The sum of two powers of the same order, as a^m+b^m, always have assignable algebraic divisors, unless *m* shall be a power of two. For if *m* shall be an odd number, then always a^m+b^m has the divisor *a* + *b*, and if *p* were a divisor of *m*, then also a^p+b^p will divide the form a^m+b^m. But if *m* shall be an even number, it will be contained in this formula $2^n p$, thus so that *p* shall be an odd number, and in this case $a^{2^n}+b^{2^n}$ will be a divisor of the form a^m+b^m with $m=2^n p$ present. And if *p* may have the divisor *q*, then also $a^{2^n q}+b^{2^n q}$ will be a divisor of the form a^m+b^m. On account of which a^m+b^m is unable to be a prime number, unless *m* shall be a power of two. Therefore in this case, if a^m+b^m were not a prime number, it cannot have other divisors, except those which may be contained in the formula $2mn+1$.

But on the other hand if the difference of powers of the same order may be proposed, a^m-b^m, these always have the divisor $a-b$ *;* in addition truly if the exponent *m* may have the divisor *p*, a^p-b^p also will be a divisor of the form a^m-b^m. Hence if *m* shall be a prime number, the form a^m-b^m besides $a-b$ will not have another divisor assigned algebraically; whereby if a^m-b^m were a prime number, it is necessary, that *m* shall be a prime number and $a-b=1$. Yet meanwhile in these cases the form a^m-b^m is not always a prime number, but as often as $2m+1$ is a prime number, it will be divisible

by that. Truly in addition it is possible also to have other divisors, which I am about to investigate here.

THEOREMA 9

34. *If the difference of the powers* $a^m - b^m$ *were divisible by the prime number* $2n+1$ *and p shall be the greatest common divisor of the numbers m and* 2*n, then* $a^p - b^p$ *also will be divisible by* $2n+1$.

DEMONSTRATION

Because $2n+1$ is a prime number, $a^{2n} - b^{2n}$ will be divisible by $2n+1$, and since by hypothesis also $a^m - b^m$ shall be divisible by $2n+1$, let $2n = \alpha m + q$ or q shall be the part remaining in the division of *2n* by *m*; and since $a^{\alpha m} - b^{\alpha m}\left[= \left(a^{\alpha}\right)^m - \left(b^{\alpha}\right)^m \right]$ also shall be divisible by $2n+1$, this form may be multiplied by a^q; $a^{\alpha m+q} - a^q b^{\alpha m}$ will be divisible by $2n+1$; but on putting $\alpha m + q$ for *2n* also $a^{\alpha m+q} - b^{\alpha m+q}$ will be divisible by $2n+1$; from which formula if it may be subtracted from the former, the remainder $a^q b^{\alpha m} - b^{\alpha m+q} = b^{\alpha m}\left(a^q - b^q\right)$ also will be divisible by $2n+1$. Hence since *b* by hypothesis may not have the divisor $2n+1$, it is necessary that $a^q - b^q$ shall be divisible by $2n+1$. Again on putting $m = \beta q + r$, and since each formula $a^{\beta q+r} - b^{\beta q+r}$ and $a^{\beta q} - b^{\beta q}$ shall be divisible by *2n* + 1, the latter may be multiplied by a^r and subtracted from the former and the remainder $b^{\beta q}\left(a^r - b^r\right)$ or $a^r - b^r$ equally will be divisible by $2n+1$. It will be apparent in a similar manner, if there were $q = \gamma r + s$, then the formula $a^s - b^s$ becomes divisible by $2n+1$; and if by continued division of this kind the values of the letters *q, r, s, t* etc. may be found, finally the letter corresponding to the greatest common divisor of the numbers *m* and *2n* may be arrived at ; which therefore if it may be put $= p$, $a^p - b^p$ will be divisible by $2n+1$. Q. E. D.

COROLLARY 1

35. Therefore if *m* were a number prime to *2n* , the greatest common divisor of these will be unity, and therefore if $a^m - b^m$ were divisible by the prime number $2n+1$, then also $a-b$ will be divisible by $2n+1$.

COROLLARY 2

36. Therefore if the difference of the numbers $a-b$ were not divisible by $2n+1$, then also no form of this kind $a^m - b^m$, where *m* is prime to *2n*, can be divided by $2n+1$.

COROLLARY 3

37. But if therefore *m* were a prime number, the form $a^m - b^m$ cannot be divided by the prime number $2n+1$, unless *m* shall be a divisor of *2n,* because $a-b$ in place cannot be divided by $2n+1$.

COROLLARY 4

38. Therefore with a prime number *m* arising, this form $a^m - b^m$ is unable to have other divisors besides the divisor $a-b$, apart from those which may be included in this formula $mn+1$. From which the divisors of some number held in this certain form $a^m - b^m$ will be found, the division only to be tried by prime numbers contained in the form $mn+1$.

COROLLARY 5

39. Therefore unless the number $2^m - 1$ shall be prime, with the prime number *m* present, it will not have other divisors, except those included in this form $mn+1$.

COROLLARY 6

40. Therefore if *m* shall be a prime number, the divisors of the formula $a^m - b^m$ besides $a-b$, if indeed *a* and *b* were numbers prime between themselves, will be contained in this series

$$2m+1,\ 4m+1,\ 6m+1,\ 8m+1,\ 10m+1 \text{ etc.},$$

if hence non-prime numbers were removed.

THEOREM 10

41. *If the formula* $a^m \pm b^m$ *may have the divisor p, then this expression also* $\left(a \pm \alpha p\right)^m \pm \left(b \pm \beta p\right)^m$ *will be divisible by p.*

DEMONSTRATION

If the powers $\left(a \pm \alpha p\right)^m$ and $\left(b \pm \beta p\right)^m$ may be expanded out in the usual manner, in each series all the terms beyond the first will be divisible by *p.* Clearly the formula $\left(a \pm \alpha p\right)^m \pm \left(b \pm \beta p\right)^m$ will change into this form

$$+a^m \pm ma^{m-1}\alpha p + \frac{m(m-1)}{1\cdot 2}a^{m-2}\alpha^2 p^2 \pm \text{etc.}$$
$$\pm\left(b^m \pm mb^{m-1}\beta p + \frac{m(m-1)}{1\cdot 2}b^{m-2}\beta^2 p^2 \pm \text{etc.}\right).$$

From which it is evident : if $a^m \pm b^m$ were divisible, then also this form

$(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ will be divisible by *p*. Q. E. D.

COROLLARY 1

42. If therefore $a^m \pm 1$ were divisible by *p*, then also this formula $(a \pm \alpha p)^m \pm 1$ will be divisible by *p*.

COROLLARY 2

43. If $a^m \pm b^m$ were divisible by *p*, then also this formula $(a \pm \alpha p)^m \pm b^m$ or this $a^m \pm (b \pm \beta p)^m$ will be divisible by *p*.

SCHOLIUM

44. In the same manner also it can be shown, if $Aa^m \pm Bb^m$ were divisible by *p*, then also this form $A(a \pm \alpha p)^m \pm B(b \pm \beta p)^m$ is divisible by *p*. And this truth also will find a place, if *p* shall be a prime or otherwise. Also there is no need indeed, that the exponent *m* of each power shall be the same, but even if they may be unequal, the conclusion likewise will prevail. Then indeed also, if *m* were an even number, from the divisibility of the formula $a^m + b^m$ by the number *p*, the divisibility also of this formula $(\alpha p \pm a)^m \pm (\beta p \pm b)^m$ follows. Truly these and others similar are apparent at once from the algebra of the elements.

THEOREM 11

45. *If* $a = ff \pm (2m+1)\alpha$ *and* $2m+1$ *were a prime number, then that expression* $a^m - 1$ *will be divisible by* $2m+1$.

DEMONSTRATION

Since $2m+1$ shall be a prime number, this formula $f^{2m} - 1$, or $(ff)^m - 1$, will be divided by this $2m+1$. Hence by the preceding theorem also that formula $(ff \pm (2m+1)\alpha)^m - 1$ will be divisible by $2m+1$. Whereby if there were $a = ff \pm (2m+1)\alpha$, the formula $a^m - 1$ can be divided by the prime number $2m+1$. Q. E. D.

COROLLARY 1

46. If therefore there were either $a = (2m+1)\alpha + 1$, or $a = (2m+1)\alpha + 4$, or $a = (2m+1)\alpha + 9$, or $a = (2m+1)\alpha + 16$, etc., then the formula $a^m - 1$ will always be divisible by $2m+1$, if indeed $2m+1$ were a prime number.

COROLLARY 2

46a. Since the case, in which the number *a* is divisible by $2m+1$ may itself be excluded, it is evident in the formula $ff \pm (2m+1)\alpha$ the number f cannot be divisible by $2m+1$. Hence all numbers can be assumed for *f*, which shall not be divisible by $2m+1$.

COROLLARY 3

47. Therefore the numbers to be assumed for f are

$$(2m+1)k \pm 1,\ (2m+1)k \pm 2,\ (2m+1)k \pm 3,\ \cdots (2m+1)k \pm m\ ;$$

for all the numbers contained in these formulas are not divisible by $2m+1$. Hence with the squares of the forms of *a* taken, if indeed the parts divisible by $2m+1$may be collected into one, there will be the following

$$(2m+1)p+1,\ (2m+1)p+4,\ (2m+1)p+9,\cdots (2m+1)p+mm,$$

of which the number is *m.*

COROLLARY 4

48. Therefore according to the values of a required to be found, so that $a^m - 1$ may become divisible by the number $2m+1$, it is required to investigate the remainders, which are left in the division of the square of each number by $2m+1$. If indeed *r* were a remainder of such a kind, a suitable value for *a* will be $(2m+1)p+r$.

COROLLARY 5

49. Moreover all these remainders *r* will be less than $2m+1$, nor yet will all the values less than $2m+1$ be values of *r*, because the number *r* is unable to be greater than *m.* Therefore numbers *m* will be given always, which will be unable to be given for *r*.

COROLLARY 6

50. Truly in the first place the values of *r* will be all the square numbers less than $2m+1$itself, then indeed the remainder, which are left in the division of the greater squares by $2m+1$; nor yet at any time the number of all the divisors of the values of *r* will be able to be greater than the number *m.*

SCHOLIUM

51. So that the use of this theorem may appear clearer and it will be able to be illustrated by numerical examples, it has been considered to add the following problems, from which not only the truth of the theorem may be seen more clearly, but also it will become apparent in turn, whenever *a* will not have this value assigned, so also the formula $a^m - 1$ cannot be divided by $2m+1$. Therefore since this formula $a^{2m} - 1$ always shall be

divisible by $2m+1$, as many times as a^m-1 will not be permitted to be divided by $2m+1$, so as often a^m+1 will be required to be divided by $2m+1$.

EXAMPLE 1

52. *To find the values of a, so that* a^2-1 *becomes divisible by 5.*

The remainders which are left from the division of squares by 5, are 1 and 4; hence it necessary, that there shall be either $a=5p+1$, $a=5p+4$ or $a=5p-1$. In the first case there becomes $aa-1$ or $(a-1)(a+1)=5p(5p+2)$, but in the second $=(5p-2)5p$; therefore in each division by 5 is seen. But if there were either $a=5p+2$ or $a=5p+3$, in neither case will the formula $aa-1$ be divisible by 5.

EXAMPLE 2

53. *To find the values of a, so that this form* a^3-1 *becomes divisible by* 7.

The three remainders, which are left in the division of all squares by 7 are 1, 2, 4. Hence the values of a are $7p+1$, $7p+2$ and $7p+4$; but if there were either $a=7p+3$ or $7p+5$ or $7p+6$, then the proposed formula a^3-1 is not divisible by 7, but this a^3+1 becomes divisible by 7.

EXAMPLE 3

54. *To find the values of a, so that this form* a^5-1 *becomes divisible by* 11.

Square numbers divided by 11 will give 5 different remainders, which are 1, 3, 4, 5, 9. Hence the formula a^5-1 will be divisible by 11, if there were $a=11p+r$ with r each one from the numbers 1, 3, 4, 5, 9. But if a certain number may be taken for a from these numbers 2, 6, 7, 8, 10 increased by some multiple of 11, then a^5+1 will be divisible by 11.

THEOREM 12

55. *If there were* $a=f^3\pm(3m+1)\alpha$ *with the prime number* $3m+1$ *present, then this form* a^m-1 *always will be divisible by* $3m+1$.

DEMONSTRATION

On account of the prime number $3m+1$, $f^{3m}-1$ will be divisible by $3m+1$. [Recall that a^p-a is divisible by the prime number p; if we set $p=3m+1$, and $a=f$ then $f^{3m+1}-f=f\left(f^{3m}-1\right)$ is divisible by $3m+1$; if f and $3m+1$ are relatively prime, then the result follows.] But there is $f^{3m}-1=\left(f^3\right)^m-1$, from which this formula too

$\left(f^3 \pm (3m+1)\alpha\right)^m - 1$ will be divisible by $3m+1$. Whereby if there is assumed $a = f^3 \pm (3m+1)\alpha$, then this formula $a^m - 1$ will be divisible by $3m+1$. Q. E. D.

COROLLARY 1

56. Therefore according to the values of *a* requiring to be found, all the remainders which arise, if the cubes be divided by $3m+1$, must be known. For each of those remainders increased by some multiple of $3m+1$ will give a suitable value for *a*.

COROLLARIUM 2

57. Since $3m+1$ must be a prime number, it is necessary that *m* shall be an even number, and thus the prime number $3m+1$ will exceed a multiple of six by one. Hence the numbers for *m* and $3m+1$ required to be given will be the following :

$m = 2, 4, 6, 10, 12, 14, 20, 22, 24, 26, 32$ etc.,
$3m+1 = 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97$ etc.

COROLLARY 3

58. Therefore if the cubic numbers may be divided by these prime numbers $3m+1$, the following remainders will be left:

Divisors	Remainders
7	1, 6
13	1, 5, 8, 12
19	1, 7, 8, 11, 12, 18
31	1, 2, 4, 8, 15, 16, 23, 27, 29, 30
37	1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36

etc.

In the first place in these remainders all the cubes occur smaller with the divisors, then if a certain remainder were *r* for the divisor $3m+1$, then also another will the remainder $= 3m+1-r$; for if the cube f^3 will give the remainder *r*, the cube $\left(3m+1-f\right)^3$ will give the remainder $-r$ or $3m+1-r$.

SCHOLIUM

59. Here it is noteworthy the number of remainders always to be $= m$, if the divisor were $= 3m+1$. Therefore the cubes always give three, of which the remainders shall be $< 3m+1$, from which the same remainder results. Clearly these three cubes 1^3, 2^3, 4^3 divided by 7 give the same remainder $= 1$ and these three cubes 2^3, 5^3 and 6^3 divided by 13 give the same remainder 8. Beyond that here it is agreed to be noted, if for *a* other values may be taken besides those assigned, then $a^m - 1$ is not divisible by $3m+1$; because even if the truth is understood easily, yet the demonstration of this does not follow from the preceding and this truth belongs to that kind [of proposition] which is

known to us, but which it is not possible to demonstrate. Therefore in these cases in which $a^m - 1$ is not divisible by $3m+1$, this formula $a^{2m} + a^m + 1$ will allow division.

THEOREM 13

60. *If there were* $a = f^n \pm (mn+1)\alpha$ *with the prime number* $mn+1$ *present, then this form* $a^m - 1$ *will be divisible by* $mn+1$.

DEMONSTRATION

On account of the prime number $mn+1$, $f^{mn} - 1$ will be divisible by $mn+1$. But there is $f^{mn} - 1 = \left(f^n\right)^m - 1$, from which also this form $\left(f^n \pm (mn+1)\alpha\right)^m - 1$ will be divisible by $mn+1$. Whereby there may be put $a = f^n \pm (mn+1)\alpha$, this formula $a^m - 1$ will be able to be divided by $mn+1$. Q. E. D.

COROLLARY 1

61. Therefore if the powers of the exponent *n* may be divided by the prime number $mn+1$, the individual remainders either from that or from some multiple of $mn+1$ increased will give suitable values for *a,* so that $a^m - 1$ may be divisible by $mn+1$.

COROLLARY 2

62. Hence if $a^m - 1$ were not divisible by $mn+1$, then the value of *a* will not be contained in this expression $f^n \pm (mn+1)\alpha$ or no power of the exponent n will be given, which divided by $mn+1$ may abandon *a.*[*i.e.* the expression cannot be divided.]

SCHOLIUM

63. The converse of this proposition also truly is understood, if all may be examined in this way ; thus so that, as often as $a^m - 1$ shall be divisible by $mn+1$, as often too the value of *a* may be contained in the formula $f^n \pm (mn+1)\alpha$; or as many times will give the power f^n, which divided by $mn+1$ leaves a for the remainder. Thus, since I may have observed the formula $2^{64} - 1$ to be divisible by 641, on account of $m = 64$ there becomes $n = 10$ [for by inspection, we can examine numbers of the form $64n+1$ until we find one that fits.], also a power of the tenth degree will be given, which divided by 641 will leave 2. And actually a power of this kind is taken to be 96^{10}. Truly besides since $2^{32} - 1$ shall not be divisible by 641, in this case there becomes $m = 32$ and $n = 20$; therefore no power of the twentieth degree is given, which divided by 641 will leave the remainder 2. The truth of this latter to be asserted has been proven rigorously, but at this point the demonstration of these converses of positions is desired : evidently if $a^m - 1$ were divisible by the prime number $mn+1$, then also always *a* is a number taken to be in

this $f^n \pm (mn+1)\alpha$, and if *a* were not contained in the formula $f^n \pm (mn+1)\alpha$, then also $a^m - 1$ cannot be divided by $mn+1$. Of which propositions if the one may be demonstrated, likewise the truth of the other may prevail. Moreover the theorem demonstrated here may be returned thus, so that as often as $f^n - a$ were divisible by $mn+1$, so too the formula $a^m - 1$ shall be divisible by $mn+1$. In this more generally the following theorem is apparent.

THEOREM 14

64. *If $f^n - ag^n$ were divisible by the prime number $mn+1$, then also $a^m - 1$ will be divisible by $mn+1$.*

DEMONSTRATION

Since the formula $f^n - ag^n$ may be put divisible by $mn+1$, also this formula $f^{mn} - a^m g^{mn}$, evidently which can be divided by $f^n - ag^n$, shall be divisible by $mn+1$. But since $mn+1$ shall be a prime number, this form $f^{mn} - g^{mn}$ will be divisible by that [due to the remainder 1 on dividing a^m]; from which also the difference $g^{mn}\left(a^m - 1\right)$ or that formula $a^m - 1$ will be divisible by $mn+1$, because therefore g is not able to be divided by $mn+1$, unless likewise f may be divided by the same, which case always is excluded in our reasoning. Q. E. D.

COROLLARY 1

65. Therefore if $a^m - 1$ were not divisible by $mn+1$, then also no numbers *f* and *g* can be given, so that this formula $f^n - ag^n$ is made divisible by $mn+1$.

COROLLARY 2

66. If the converse of the further above proposition could be demonstrated, then also it would prevail, as often as $f^n - a$ may be unable to be divided by $mn+1$, then indeed the formula $f^n - ag^n$ does not admit to division by $mn+1$; truly likewise it may become apparent, if $f^n - ag^n$ shall be divisible by $mn+1$, then also a formula of such a kind is given $f^n - a$, which shall be divisible by $mn+1$.

THEOREM 15

67. *If a formula of this kind $af^n - bg^n$ were divisible by the prime number $mn+1$, then also this $a^m - b^m$ will be divisible by $mn+1$.*

DEMONSTRATION

If $af^n - bg^n$ were divisible by $mn+1$, then also this formula $a^m f^{mn} - b^m g^{mn}$ will be divisible by $mn+1$. But on account of the prime number $mn+1$ there will be this

formula $f^{mn} - g^{mn}$ and as well as this $a^m f^{mn} - a^m g^{mn}$ thus also divisible by $mn+1$; the latter may be subtracted from the former $a^m f^{mn} - b^m g^{mn}$ and the remainder $g^{mn}\left(a^m - b^m\right)$ or $a^m - b^m$ will be divisible by $mn+1$. Q. E. D.

COROLLARY 1

68. And thus if $a^m - b^m$ were not divisible by $mn+1$, then no numbers will be given requiring to be substituted for f and g, so that a formula of this kind $g^{mn}\left(a^m - b^m\right)$ shall be divisible by $mn+1$.

COROLLARY 2

69. The converse of this proposition truly is seized upon, which may be examined in some manner, if the formula $a^m - b^m$ were divisible by mn+1, likewise there may be given numbers f and g, so that $af^n - bg^n$ truly is made divisible by $mn+1$. Yet meanwhile the demonstration of this even now may be desired.

SCHOLIUM

70. The case of the inverse of this proposition can be demonstrated, so that the numbers m and n are prime between themselves ; for always in this case numbers of such a kind μ and v can be shown, so that there shall be $\mu n \pm 1 = vm$. For if this operation may be put in place between the numbers m and n, which is accustomed to be used for putting the greatest common divisor in place, and as often as it may be noted from these and the fractions close to $\frac{m}{n}$ may be sought, finally there will be $\frac{m}{n}$, and if the penultimate ratio were $\frac{\mu}{v}$ there will be $\mu n \pm 1 = vm$. Therefore with this lemma established the converse of the proposition thus will be had, in which m and n shall be numbers prime between themselves.

THEOREM 16

71. *If m and n were numbers prime between themselves and this formula $a^m - b^m$ shall be divisible by the number $mn+1$, then the formula $af^n - bg^n$ will be given divisible by $mn+1$.*

DEMONSTRATION

There may be put $f = a^\mu$ and $g = b^\mu$ and the formula $af^n - bg^n$ will change into this $a^{\mu n+1} - b^{\mu n+1}$; whereby if μ were taken thus, so that there shall be $\mu tn + 1 = vm$, there will be $a^{vm} - b^{vm}$; which since it shall be divisible by $a^m - b^m$, it shall be divisible also by $mn+1$ and thus there will be given the case, in which $af^n - bg^n$ will be divisible by $mn+1$.

But if there were $\mu n - 1 = \nu m$, then there may be taken $f = b^{\mu}$ and $g = a^{\mu}$ and there becomes $af^n - bg^n = ab^{\mu n} - ba^{\mu n} = ab\left(b^{\mu n-1} - a^{\mu n-1}\right) = -ab\left(a^{\nu m} - b^{\nu m}\right)$ and thus it will be divisible by $mn+1$. Q. E. D.

COROLLARY 1

72. Therefore if m and n were numbers prime between themselves and $mn+1$ a prime number, then these propositions have been demonstrated :

1. *If $af^n - bg^n$ were divisible by $mn + 1$, then also $a^m - b^m$ will be divisible by $mn+1$, and if that formula in no manner may be divisible by $mn+1$, then also this will not be divisible.*

II. *If $a^m - b^m$ were divisible by $mn+1$, then a number of this form $af^n - bg^n$ will be given divisible by $mn+1$, and if $a^m - b^m$ may not admit to division by $mn+1$, then no number will be given of the form $af^n - bg^n$ divisible by $mn+1$.*

COROLLARY 2

73. If m shall be an even number, then b can be taken equally negative and positive ; therefore in this case if $a^m - b^m$ were divisible by $mn+1$, then also a formula of this kind $af^n + bg^n$ will be assigned divisible by $mn+1$; that which also thus may be apparent, because n shall be an odd number and thus the power g^n may be able to become negative.

COROLLARY 3

74. It will be demonstrated in a similar manner, if as before m and n were numbers prime between themselves and this formula $a^m - b^m$ shall be divisible by $mp + 1$, then also it can be shown the formula of this kind can be divisible $af^n - bg^n$ by $mp + 1$.

New Commentaries of the St.Petersburg Academy of Sciences 1 (1747/48) 1750, pp. 20 - 48. ***Translated and annotated by Ian Bruce.***

THEOREMATA CIRCA DIVISORES NUMERORUM

L. Euler (E134)

Quovis tempore summi Geometrae agnoverunt in natura numerorum plurimas praeclarissimas proprietates esse absconditas, quarum cognitio fines Matheseos non mediocriter esset amplificatura. Primo quidem intuitu doctrina numerorum ad Arithmeticae elementa referenda videtur atque vix quicquam in ea inesse putatur, quod ullam sagacitatem aut vim Analyseos requirat. Qui autem diligentius in hoc genere sunt versati, non solum veritates demonstratu difficillimas detexerunt, sed etiam eiusmodi, quarum certitudo percipiatur, etiamsi demonstrari nequeat. Plurima huiusmodi theoremata sunt prolata ab insigni Geometra FERMATIO, quorum veritas, quamvis demonstratio lateat, non minus evicta videtur. Atque hoc imprimis omnem attentionem meretur in Mathesi adeo pura eiusmodi dari veritates, quas nobis cognoscere liceat, cum tamen eas demonstrare non valeamus; atque hoc adeo in Arithmetica usu venit, quae tamen prae reliquis Matheseos partibus maxime pertractata ac perspecta haberi solet; neque facile affirmare ausim, an similes veritates in reliquis partibus reperiantur. In Geometria certe nulla occurit propositio, cuius vel veritas vel falsitas firmissimis rationibus evinci nequeat. Cum igitur quaevis veritas eo magis abstrusa censeatur, quo minus ad eius demonstrationem aditus pateat, in Arithmetica certe, ubi natura numerorum perpenditur, omnium abstrusissimas contineri negare non poterimus. Non desunt quidem inter summos Mathematicos Viri, qui huiusmodi veritates prorsus steriles ideoque non dignas iudicant, in quarum investigatione ulla opera collocetur; at praeterquam quod cognitio omnis veritatis per se sit excellens, etiamsi ab usu populari abhorrere videatur, omnes veritates, quas nobis cognoscere licet, tantopere inter se connexae deprehenduntur, ut nulla sine temeritate tanquam prorsus inutilis repudiari possit. Deinde etsi quaepiam propositio ita comparata videatur, ut, sive vera sit sive falsa, nihil inde ad nostram utilitatem redundet, tamen ipsa methodus, qua eius veritas vel falsitas evincitur, plerumque nobis viam ad alias utiliores veritates cognoscendas patefacere solet.

Hanc ob rem non inutiliter me operam ac studium in indagatione demonstrationum quarundam propositionum impendisse confido, quibus insignes circa divisores numerorum proprietates continentur. Neque vero haec de divisoribus doctrina omni caret usu, sed nonnunquam in Analysi non contemnendam praestat utilitatem. Imprimis vero non dubito, quin methodus ratiocinandi, qua sum usus, in aliis gravioribus investigationibus aliquando non parum subsidii afferre possit.

Propositiones autem, quas hic demonstratas exhibeo, respiciunt divisores numerorum in hac formula $a^n + b^n$ contentorum, quarum nonnullae iam ab ante memorato FERMATIO, sed sine demonstratione, sunt publicatae. Quoniam igitur hic perpetuo de numeris integris sermo instituetur, omnes alphabeti litterae hic constanter numeros integros indicabunt.

New Commentaries of the St.Petersburg Academy of Sciences 1 (1747/48) 1750, pp. 20 - 48. ***Translated and annotated by Ian Bruce.***

THEOREMA 1

1. *Si p fuerit numerus primus, omnis numerus in hac forma* $(a+b)^p - a^p - b^p$ *contentus divisibilis erit per p.*

DEMONSTRATIO

Si binomium $(a+b)^p$ modo consueto evolvatur, erit

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

qua expressione substituta binisque terminis, qui easdem habent uncias, coniunctis erit

$$(a+b)^p - a^p - b^p = \tfrac{p}{1}ab\left(a^{p-2}+b^{p-2}\right) + \tfrac{p(p-1)}{1\cdot 2}a^2b^2\left(a^{p-4}+b^{p-4}\right)$$
$$+ \tfrac{p(p-1)(p-2)}{1\cdot 2\cdot 3}a^3b^3\left(a^{p-6}+b^{p-6}\right) + + \tfrac{p(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3\cdot 4}a^4b^4\left(a^{p-8}+b^{p-8}\right) + \text{etc.}$$

Hic primo notandum est omnes uncias, quamquam sub forma fractionum apparent, nihilominus esse numeros integros, cum exhibeant, uti constat, numeros figuratos. Quaelibet ergo uncia, cum factorem habeat *p*, divisibilis erit per *p*, nisi is alicubi per factorem denominatoris vel prorsus tollatur vel dividatur. At ubique omnes factores denominatorum minores sunt quam *p*, quia adeo non ultra $\frac{1}{2}p$ crescunt, ideoque factor numeratorum *p* nusquam per divisionem tollitur. Deinde cum *p* sit per hypothesin numerus primus, is nusquam per divisionem minuetur. Quocirca singulae unciae $\frac{p}{1}$, $\frac{p(p-1)}{1\cdot 2}$, $\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}$ etc. hincque tota expressio $(a+b)^p - a^p - b^p$ perpetuo per numerum *p*, siquidem fuerit numerus primus, erit divisibilis.
Q. E. D.

COROLLARIUM 1

2. Si ergo ponatur $a=1$ et $b=1$, erit $2^p - 2$ semper divisibilis per *p*, si quidem fuerit *p* numerus primus. Cum igitur sit $2^p - 2 = 2\left(2^{p-1}-1\right)$, alterum horum factorum per *p* divisibilem esse oportet. At nisi sit $p=2$, prior factor 2 per *p* non est divisibilis; unde sequitur formam $2^{p-1}-1$, perpetuo per *p* esse divisibilem, si *p* fuerit numerus primus praeter binarium.

COROLLARIUM 2

3. Ponendis ergo pro *p* successive numeris primis erit 2^2-1 divisibile per 3, 2^4-1 per 5, 2^6-1 per 7, $2^{10}-1$ per 11 etc., quod in minoribus numeris per se fit perspicuum, in maximis autem aeque erit certum. Sic cum 641 sit numerus primus, iste numerus $2^{640}-1$ necessario per 641 erit divisibilis, seu si potestas 2^{640} per 641 dividatur, post divisionem supererit residuum $=1$.

THEOREMA 2

4. *Si utraque harum formularum* a^p-a et b^p-b *fuerit divisibilis per numerum primum p, tum quoque ista formula* $(a+b)^p-a-b$ *divisibilis erit per eundem numerum primum p.*

DEMONSTRATIO

Cum per § 1 $(a+b)^p-a^p-b^p$ sit divisibilis per numerum *p,* si fuerit primus, atque hic formulae a^p-a et b^p-b per *p* divisibiles assumantur, erit quoque summa istarum trium formularum, nempe $(a+b)^p-a-b$, per *p,* si fuerit numerus primus, divisibilis. Q. E. D.

COROLLARIUM 1

5. Si ponatur $b=1$ cum $1^p-1=0$ sit divisibile per *p,* sequitur, si formula a^p-a fuerit divisibilis per *p,* tum quoque formulam $(a+1)^p-a-1$ fore per *p* divisibilem.

COROLLARIUM 2

6. Cum igitur assumta formula a^p-a per *p* divisibili sit quoque formula $(a+1)^p-a-1$ per *p* divisibilis, simili modo in eadem hypothesi erit haec quoque formula $(a+2)^p-a-2$ hincque porro haec $(a+3)^p-a-3$ etc. atque generaliter haec c^p-c divisibilis per *p.*

THEOREMA 3

7. *Si p fuerit numerus primus, omnis numerus huius formae* $c^p - c$ *per p erit divisibilis.*

DEMONSTRATIO

Si in § 6 ponatur $a = 1$, cum sit $a^p - a = 0$ per *p* divisibilis, sequitur has quoque formulas $2^p - 2$, $3^p - 3$, $4^p - 4$ etc. , et generatim hanc $c^p - c$ fore per numerum primum *p* divisibilem. Q. E. D.

COROLLARIUM 1

8. Quicunque ergo numerus integer pro *c* assumatur, denotante *p* numerum primum omnes numeri in hac forma $c^p - c$ contenti erunt divisibiles per *p.*

COROLLARIUM 2

9. Cum autem sit $c^p - c = c\left(c^{p-1} - 1\right)$, vel ipse numerus *c* vel $c^{p-1} - 1$ divisibilis erit per *p.* Utrumque autem simul per *p* divisibilem esse non posse manifestum est. Quare si numerus *c* non fuerit divisibilis per *p,* haec forma $c^{p-1} - 1$ certe per *p* erit divisibilis.

COROLLARIUM 3

10. Si ergo *p* fuerit numerus primus, omnes numeri in hac forma contenti $a^{p-1} - 1$ erunt divisibiles per *p* exceptis iis casibus, quibus ipse numerus *a* per *p* est divisibilis.

THEOREMA 4

11. *Si neuter numerorum a et b divisibilis fuerit per numerum primum p, tum omnis numerus huius formae* $a^{p-1} - b^{p-1}$ *erit divisibilis per p.*

DEMONSTRATIO

Cum neque *a* neque *b* sit divisibilis per *p* atque *p* denotet numerum primum, tam haec forma $a^{p-1} - 1$ quam haec $b^{p-1} - 1$ erit divisibilis per *p.*
Hinc ergo quoque differentia istarum formularum $a^{p-1} - b^{p-1}$ erit divisibilis per *p.* Q. E. D.

COROLLARIUM 1

12. Cum omnis numerus primus praeter binarium, cuius ratio dividendi per se est manifesta, sit impar, ponatur $2m+1$ pro *p* atque perspicuum erit omnes numeros in hac forma $a^{2m} - b^{2m}$ contentos esse divisibiles per $p = 2m+1$, siquidem neque *a* neque *b* seorsim fuerit per $2m+1$ divisibilis.

COROLLARIUM 2

13. Quia *b* non est divisibilis per $2m+1$, etiam b^{2m} et $2b^{2m}$ non divisibile erit per $2m+1$. Quare si $2b^{2m}$ addatur ad formulam $a^{2m}-b^{2m}$, quae est divisibilis per $2m+1$, prodibit formula $a^{2m}+b^{2m}$, quae per $2m+1$ non erit divisibilis, nisi uterque numerus *a* et *b* seorsim per $2m+1$ sit divisibilis.

COROLLARIUM 3

14. Quoniam ob *2m* numerum parem formula $a^{2m}-b^{2m}$ factores habet $\left(a^m-b^m\right)\left(a^m+b^m\right)$, necesse est, ut horum factorum alter sit divisibilis per $2m+1$; ambo autem simul per numerum $2m+1$ divisibiles esse nequeunt. Quare si $2m+1$ fuerit numerus primus et neque *a* neque *b* divisibile sit per $2m+1$, tum vel a^m-b^m vel a^m+b^m erit divisibile per $2m+1$.

COROLLARIUM 4

15. Si *m* sit numerus par, puta $=2n$, atque a^m-b^m seu $a^{2n}-b^{2n}$ divisibilis per $2m+1=4n+1$, tum ob eandem rationem vel a^n-b^n vel a^n+b^n divisibile erit per numerum primum $4n+1$.

THEOREMA 5

16. *Summa duorum quadratorum* $aa+bb$ *per nullum numerum primum huius formae* $4n-1$ *unquam dividi potest, nisi utriusque radix seorsim a et b sit divisibilis per* $4n-1$.

DEMONSTRATIO

Si $4n-1$ fuerit numerus primus neque *a* et *b* per illum sint divisibiles, tum $a^{4n-2}-b^{4n-2}$ erit divisibile per $4n-1$ (§ 11) hincque ista formula $a^{4n-2}+b^{4n-2}$ non erit divisibilis per $4n-1$ [§ 13] neque propterea ullus eius factor. At cum $4n-2=2\left(2n-1\right)$ sit numerus impariter par, formula $a^{4n-2}+b^{4n-2}$ factorem habet $aa+bb$*;* quare fieri nequit, ut iste factor $aa+bb$, hoc est ulla duorum quadratorum summa, sit divisibilis per $4n-1$.
Q. E. D.

COROLLARIUM 1

17. Cum omnes numeri primi vel ad hanc formam $4n+1$ vel ad hanc $4n-1$ revocentur, si $4n-1$ non fuerit numerus primus, divisorem habebit formae $4n-1$; namque ex meris numeris formae $4n+1$ nunquam numerus formae $4n-1$ resultare potest. Quare cum summa duorum quadratorum per nullum numerum primum formae $4n-1$ dividi possit, per nullum quoque numerum eiusdem formae $4n-1$, etiamsi non sit primus, dividi poterit.

COROLLARIUM 2

18. Summa ergo duorum quadratorum $aa+bb$ per nullum numerum huius seriei 3, 7, 11, 15, 19, 23, 27, 31, 35 etc. est divisibilis. Omnes ergo numeri primi praeter binarium, qui unquam divisores esse possunt summae duorum quadratorum, continentur in hac forma $4n+1$, siquidem numeri *a* et *b* inter se communem divisorem non habent.

COROLLARIUM 3

19. Cum omnis numerus sit vel primus vel productum ex primis, summa duorum quadratorum nullum numerum primum pro divisore habebit, nisi qui contineatur in hac forma $4n+1$. Divisores ergo primi summae duorum quadratorum continebuntur in hac serie 2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc.

SCHOLION

20. Quod numerus huius formae $4n-1$ nunquam possit esse summa duorum quadratorum, facile intelligitur. Numeri enim quadrati vel sunt pares vel impares; illi in hac forma *4a,* hi vero in hac $4b+1$ continentur. Quare ut summa duorum quadratorum sit numerus impar, alterum par, alterum impar esse oportet; hinc oritum forma $4a+4b+1$ seu $4n+1$ ideoque nullus numerus huius formae $4n-1$ summa duorum quadratorum esse potest. Quod vera summa duorum quadratorum ne divisorem quidem formae $4n-1$ admittat, ab omnibus scriptoribus methodi Diophantae semper est affirmatum; nemo autem unquam, quantum mihi constat, id demonstravit excepto FERMATIO , qui autem suam demonstrationem nunquam publicavit, ita ut mihi quidem videar primus hanc veritatem publice demonstrasse: *Nullum numerum vel huius formae* $4n-1$ *vel per numerum eiusdem formae divisibilem unquam esse posse summam duorum quadratorum.* Hinc ergo sequitur omnem summam duorum quadratorum inter se primorum vel esse numerum primum vel binario excepto alios divisores non habere, nisi qui in forma $4n+1$ contineantur.

THEOREMA 6

21. *Omnes divisores summae duorum biquadratorum inter se primorum sunt vel* 2 *vel numeri huius formae* $8n+1$.

DEMONSTRATIO

Sint a^4 et b^4 duo biquadrata inter se prima; erit vel utrumque impar vel alterum par et alterum impar; priori casu summae a^4+b^4 divisor erit 2, utroque vera casu divisores impares, si qui fuerint, in hac forma $4n+1$ continebuntur. Cum enim biquadrata simul sint quadrata, nullus divisor formae $4n-1$ locum invenit (§ 16). At numeri $4n+1$ vel ad hanc formam $8n+1$ vel ad hanc $8n-3$ revocantur. Dico autem nullum numerum formae $8n-3$ esse posse divisorem summae duorum biquadratorum. Ad hoc demonstrandum sit primo $8n-3$ numerus primus atque per eum divisibilis erit haec forma $a^{8n-4}-b^{8n-4}$, unde haec forma $a^{8n-4}+b^{8n-4}$ per numerum $8n-3$ prorsus non erit divisibilis [§ 13], nisi uterque numerus *a* et *b* seorsim divisionem admittat, qui casus autem assumtione,

quod ambo numeri *a* et *b* sint inter se primi, excluditur. Cum igitur forma $a^{8n-4}+b^{8n-4}=a^{4(2n-1)}+b^{4(2n-1)}$ dividi nequeat per $8n-3$, nullus quoque eius factor per $8n-3$ dividi poterit. At ob $2n-1$ numerum imparem illius formae factor erit a^4+b^4 qui ergo per nullum numerum primum formae $8n-3$ dividi potest. Hinc omnes numeri primi praeter binarium, qui unquam formam a^4+b^4 divident, erunt huiusmodi $8n+1$. Ex multiplicatione autem duorum pluriumve talium divisorum nunquam numerus formae $8n-3$ oritur; ex quo sequitur nullum prorsus numerum huius formae $8n-3$, sive sit primus sive compositus, summam duorum biquadratorum inter se primorum dividere. Q. E. D.

COROLLARIUM 1

22. Cum omnes numeri impares in una harum quatuor formarum contineantur $8n\pm1$ et $8n\pm3$, praeter numeros in forma prima $8n+1$ contentos nullus alius poterit esse divisor summae duorum biquadratorum.

COROLLARIUM 2

23. Omnes ergo divisores primi summae duorum biquadratorum inter se primorum erunt vel 2 vel in hac serie contenti 17, 41, 73, 89, 97, 113, 137, 193 etc.,
quae complectitur omnes numeros primos formae $8n+1$.

COROLLARIUM 3

24. Si quis ergo numerus, puta *N,* fuerit summa duorum biquadratorum, tum is vel erit primus vel alios non habebit divisores, nisi qui in forma $8n+1$ contineantur; unde investigatio divisorum mirum in modum contrahitur.

COROLLARIUM 4

25. Nullus igitur numerus, qui divisorem habet non in forma $8n+1$ contentum, erit summa duorum biquadratorum, nisi forte habeat quatuor divisores aequales, qui autem in consideratione biquadratorum reiici solent.

THEOREMA 7

26. *Omnes divisores huiusmodi numerorum* a^8+b^8 *, si quidem a et b sunt numeri inter se primi, sunt vel* 2 *vel in hac forma* $16n+1$ *continentur.*

DEMONSTRATIO

Quia a^8 et b^8 simul sunt biquadrata, eorum summa a^8+b^8 alios non admittet divisores, nisi qui in forma $8n+1$ contineantur. At numeri in hac forma $8n+1$ contenti sunt vel $16n+1$ vel $16n-7$. Sit $16n-7$ numerus primus ac per eum dividi non poterit forma $a^{16n-8}+b^{16n-8}$ (§ 13) seu $a^{8(2n-1)}+b^{8(2n-1)}$ neque propterea ullus eius factor. Verum ob $2n-1$ numerum imparem haec forma divisorem habet a^8+b^8, quae ergo per nullum numerum primum $16n-7$ erit divisibilis ac propterea alios divisores primos habere nequit, nisi qui in forma $16n+1$ contineantur. Ex multiplicatione autem duorum pluriumve huiusmodi numerorum $16n-7$ perpetuo productum eiusdem formae nascitur neque

unquam numerus formae $16n-7$ resultare potest. Unde cum nullus numerus formae $16n-7$ divisor ipsius a^8+b^8 existere possit, necesse est, ut omnes huius formae a^8+b^8 divisores, si quos habet, sive sint primi sive compositi, perpetuo in hac formula $16n+1$ contineantur.
Q. E. D.

COROLLARIUM 1

27. Nullus igitur numerus, qui in hac forma $16n+1$ non includitur, unquam esse potest divisor summae duarum potestatum octavi gradus inter se primarum.

COROLLARIUM 2

28. Si quis ergo voluerit numeri cuiuspiam huius formae a^8+b^8 divisores investigare, is divisionem per nullos alios numeros primos nisi in hac forma $16n+1$ contentos tentet, cum demonstratum sit omnes reliquos numeros primos huius formae divisores esse non posse.

THEOREMA 8

29. *Summa duarum huiusmodi potestatum $a^{2^m}+b^{2^m}$, quarum exponens est dignitas binarii, alios divisores non admittit, nisi qui contineantur in hac forma $2^{m+1}n+1$.*

DEMONSTRATIO

Quemadmodum demonstravimus omnes divisores formae a^2+b^2 in hac forma $4n+1$ contineri hincque ulterius divisores omnes formae a^4+b^4 in $8n+1$ et formae a^8+b^8 in $16n+1$ contineri evicimus, ita simili modo ostendi potest formam $a^{16}+b^{16}$ nullos alios divisores admittere nisi in formula $32n+1$ contentos. Dehinc porro intelligemus formas $a^{32}+b^{32}$, $a^{64}+b^{64}$ etc. alios divisores habere non posse, nisi qui in formulis $64n+1$, $128n+1$ etc. includantur. Sicque in genere patebit formae $a^{2^m}+b^{2^m}$ alios non dari divisores, nisi qui in formula $2^{m+1}n+1$ contineantur. Q. E. D.

COROLLARIUM 1

30. Nullus ergo numerus primus, qui in hac forma $2^{m+1}n+1$ non includitur, unquam esse potest divisor ullius numeri in hac forma $a^{2^m}+b^{2^m}$ contenti.

COROLLARIUM 2

31. Divisores ergo huiusmodi numeri $a^{2^m}+b^{2^m}$ inquisiturus inutiliter operam suam consumeret, si aliis numeris primis praeter eos, quos forma $2^{m+1}n+1$ suppeditat, divisionem tentare vellet.

New Commentaries of the St.Petersburg Academy of Sciences 1 (1747/48) 1750, pp. 20 - 48. ***Translated and annotated by Ian Bruce.***

SCHOLION 1

32. FERMATIUS affirmaverat, etiamsi id se demonstrare non posse ingenue esset confessus, omnes numeros ex hac forma $2^{2^n}+1$ ortos esse primos ; hincque problema alias difficillimum, quo quaerebatur numerus primus dato numero maior, resolvere est conatus. Ex ultimo theoremate autem perspicuum est, nisi numerus $2^{m+1}n+1$ sit primus, eum alios divisores habere non posse praeter tales, qui in forma $2^{m+1}n+1$ contineantur. Cum igitur veritatem huius effati FERMATIANI pro casu $2^{32}+1$, examinare voluissem, ingens hinc compendium sum nactus, dum divisionem aliis numeris primis praeter eos, quos formula $64n+1$ suppeditat, tentare non opus habebam. Huc igitur inquisitione. reducta mox deprehendi ponendo $n=10$ numerum primum 641 esse divisorem numeri $2^{32}+1$, unde problema memoratum, quo numerus primus dato numero maior requiritur, etiamnum manet insolutum.

SCHOLION 2

33. Summa duarum potestatum eiusdem gradus, uti a^m+b^m, semper habet divisores algebraice assignabiles, nisi *m* sit dignitas binarii. Nam si *m* sit numerus impar, tum a^m+b^m semper divisorem habet *a* + *b*, atque si *p* fuerit divisor ipsius *m*, tum quoque a^p+b^p formam a^m+b^m dividet. Sin autem *m* sit numerus par, in hac formula $2^n p$ continebitur, ita ut *p* sit numerus impar, hocque casu $a^{2^n}+b^{2^n}$ divisor erit formae a^m+b^m existente $m=2^n p$. Atque si *p* habeat divisorem *q*, tum etiam $a^{2^n q}+b^{2^n q}$ erit divisor formae a^m+b^m. Quocirca a^m+b^m numerus primus esse nequit, nisi *m* sit dignitas binarii. Hoc igitur casu, si a^m+b^m non fuerit numerus primus, alios divisores habere nequit, nisi qui formula $2mn+1$ contineantur.

Contra autem si differentia duarum potestatum eiusdem gradus proponatur a^m-b^m, ea semper divisorem habet $a-b$; praeterea vero si exponens *m* divisorem habeat *p*, erit quoque a^p-b^p divisor formae a^m-b^m. Hinc si *m* sit numerus primus, forma a^m-b^m praeter $a-b$ alium divisorem algebraice assignabilem non habebit; quare si a^m-b^m fuerit numerus primus, necesse est, ut *m* sit numerus primus et $a-b=1$. Interim tamen ne his quidem casibus forma a^m-b^m semper est numerus primus, sed quoties $2m+1$ est numerus primus, per eum erit divisibilis. Praeterea vero etiam alios divisores habere potest, quos hic sum investigaturus.

THEOREMA 9

34. *Si differentia potestatum* $a^m - b^m$ *fuerit divisibilis per numerum primum* $2n+1$ *atque p sit maximus communis divisor numerorum m et* $2n$*, tum quoque* $a^p - b^p$ *erit divisibilis per* $2n+1$.

DEMONSTRATIO

Quia $2n+1$ est numerus primus, erit $a^{2n} - b^{2n}$ divisibilis per $2n+1$, et cum per hypothesin $a^m - b^m$ sit quoque divisibilis per $2n+1$, sit $2n = \alpha m + q$ seu q sit residuum in divisione ipsius $2n$ per m remanens; et cum $a^{\alpha m} - b^{\alpha m}$ sit quoque per $2n+1$ divisibilis, multiplicetur haec forma per a^q; erit $a^{\alpha m+q} - a^q b^{\alpha m}$ per $2n+1$ divisibilis; at posito $am+q$ pro $2n$ est quoque $a^{\alpha m+q} - b^{\alpha m+q}$ per $2n+1$ divisibilis; a qua formula si prior subtrahatur, residuum $a^q b^{\alpha m} - b^{\alpha m+q} = b^{\alpha m}\left(a^q - b^q\right)$ quoque per $2n+1$ erit divisiblIe.

Hinc cum b per hypothesin divisorem $2n+1$ non habeat, necesse est, ut $a^q - b^q$ per $2n+1$ sit divisibile. Ponatur porro $m = \beta q + r$, et cum utraque haec formula $a^{\beta q+r} - b^{\beta q+r}$ et $a^{\beta q} - b^{\beta q}$ sit per $2n + 1$ divisibilis, multiplicetur posterior per a^r et a priori subtrahatur atque residuum $b^{\beta q}\left(a^r - b^r\right)$ seu $a^r - b^r$ pariter per $2n+1$ erit divisibile. Simili modo patebit, si fuerit $q = \gamma r + s$, tum formulam $a^s - b^s$ per $2n+1$ fore divisibilem; atque si per huiusmodi continuam divisionem valores litterarum q, r, s, t etc. investigentur, tandem pervenietur ad maximum communem divisorem numerorum m et $2n$; qui ergo si ponatur $= p$, erit $a^p - b^p$ divisibile per $2n+1$. Q. E. D.

COROLLARIUM 1

35. Si igitur m fuerit numerus ad $2n$ primus, maximus eorum communis divisor erit unitas, ac propterea si $a^m - b^m$ fuerit divisibile per numerum primum $2n+1$, tum quoque $a-b$ per $2n+1$ erit divisibile.

COROLLARIUM 2

36. Si ergo differentia numerorum $a-b$ non fuerit divisibilis per $2n+1$, tum quoque nulla huiusmodi forma $a^m - b^m$, ubi m est ad $2n$ numerus primus, per $2n+1$ divisibilis esse potest.

COROLLAR1UM 3

37. Quodsi ergo m fuerit numerus primus, forma $a^m - b^m$ per numerum primum $2n+1$ dividi non potest, nisi m sit divisor ipsius $2n$, posito quod $a-b$ non sit divisibile per $2n+1$.

COROLLARIUM 4

38. Existente ergo *m* numero primo haec forma $a^m - b^m$ praeter divisorem $a-b$ alios divisores habere nequit, nisi qui includantur in hac formula $mn+1$. Unde divisores numeri cuiuspiam in hac forma $a^m - b^m$ contenti investigaturus divisionem tantum per numeros primos in forma $mn+1$ contentos tentabit.

COROLLARIUM 5

39. Nisi ergo numerus $2^m - 1$ sit primus existente *m* numero primo, alios divisores habere non poterit, nisi qui includuntur in hac forma $mn+1$.

COROLLARIUM 6

40. Si ergo *m* sit numerus primus, divisores formulae $a^m - b^m$ praeter $a-b$, si quidem *a* et *b* fuerint numeri inter se primi, continebuntur in hac serie

$$2m+1,\ 4m+1,\ 6m+1,\ 8m+1,\ 10m+1 \text{ etc.},$$

si hinc numeri non primi expungantur.

THEOREMA 10

41. *Si formula* $a^m \pm b^m$ *divisorem habeat p, tum quoque haec expressio* $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ *per p erit divisibilis.*

DEMONSTRATIO

Si potestates $(a \pm \alpha p)^m$ et $(b \pm \beta p)^m$ methodo consueta evolvantur, in utraque serie omnes termini praeter primum divisibiles erunt per *p.* Scilicet formula $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ abibit in hanc formam

$$+a^m \pm ma^{m-1}\alpha p + \frac{m(m-1)}{1\cdot 2}a^{m-2}\alpha^2 p^2 \pm \text{etc.}$$
$$\pm\left(b^m \pm mb^{m-1}\beta p + \frac{m(m-1)}{1\cdot 2}b^{m-2}\beta^2 p^2 \pm \text{etc.}\right).$$

Unde perspicuum est: si $a^m \pm b^m$ fuerit divisibile, tum quoque haec forma $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ per *p* erit divisibilis. Q. E. D.

COROLLARIUM 1

42. Si igitur $a^m \pm 1$ fuerit divisibile per *p*, tum quoque haec formula $(a \pm \alpha p)^m \pm 1$ per *p* erit divisibilis.

COROLLARIUM 2

43. Si $a^m \pm b^m$ fuerit divisibile per *p*, tum quoque haec formula $\left(a \pm \alpha p\right)^m \pm b^m$ vel haec $a^m \pm \left(b \pm \beta p\right)^m$ per *p* erit divisibilis.

SCHOLION

44. Eodem quoque modo generaliter demonstrari potest, si fuerit $Aa^m \pm Bb^m$ divisibile per *p*, tum quoque hanc formam $A\left(a \pm \alpha p\right)^m \pm B\left(b \pm \beta p\right)^m$ fore per *p* divisibilem. Haecque veritas aeque locum invenit, sive *p* sit numerus primus sive secus. Quin etiam non opus est, ut utriusque potestatis idem sit exponens *m*, sed etiamsi essent inaequales, conclusio perinde valebit. Tum vero quoque, si *m* fuerit numerus par, ex divisibilitate formulae $a^m + b^m$ per numerum *p* divisibilitas etiam huius formulae $\left(\alpha p \pm a\right)^m \pm \left(\beta p \pm b\right)^m$ sequitur. Verum haec aliaque similia ex algebrae elementis sponte patent.

THEOREMA 11

45. *Si fuerit* $a = ff \pm \left(2m+1\right)\alpha$ *et* $2m+1$ *numerus primus, tum ista expressio* $a^m - 1$ *erit divisibilis per* $2m+1$.

DEMONSTRATIO

Cum sit $2m+1$ numerus primus, per eum dividi poterit haec formula $f^{2m} - 1$ seu haec $\left(ff\right)^m - 1$. Hinc per theorema praecedens quoque ista formula $\left(ff \pm \left(2m+1\right)\alpha\right)^m - 1$ erit divisibilis per $2m+1$. Quare si fuerit $a = ff \pm \left(2m+1\right)\alpha$, formula $a^m - 1$ per numerum primum $2m+1$ dividi poterit. Q. E. D.

COROLLARIUM 1

46. Si ergo fuerit vel $a = \left(2m+1\right)\alpha + 1$ vel $a = \left(2m+1\right)\alpha + 4$ vel $a = \left(2m+1\right)\alpha + 9$ vel $a = \left(2m+1\right)\alpha + 16$ vel etc., tum formula $a^m - 1$ semper erit divisibilis per $2m+1$, si quidem $2m+1$ fuerit numerus primus.

COROLLARIUM 2

46a. Cum casus, quibus ipse numerus *a* est divisibilis per $2m+1$ excludantur, manifestum" est in formula $ff \pm \left(2m+1\right)\alpha$ numerum *f* per $2m+1$ divisibilem esse non posse. Hinc pro *f* omnes numeri assumi possunt, qui per $2m+1$ non sint divisibiles.

COROLLARIUM 3

47. Numeri ergo pro *f* assumendi sunt

$$(2m+1)k \pm 1,\ (2m+1)k \pm 2,\ (2m+1)k \pm 3,\ \cdots (2m+1)k \pm m\ ;$$

in his enim formulis omnes numeri per $2m+1$ non divisibiles continentur. Hinc sumendis quadratis formae ipsius *a,* si quidem partes per $2m+1$ divisibiles in unam colligantur, erunt sequentes

$$(2m+1)p+1,\ (2m+1)p+4,\ (2m+1)p+9,\cdots (2m+1)p+mm,$$

quarum numerus est *m.*

COROLLARIUM 4

48. Ad valores igitur ipsius *a* inveniendos, ut $a^m - 1$ per numerum $2m+1$ fiat divisibile, investigari oportet residua, quae in divisione cuiusque numeri quadrati per $2m+1$ remanent. Si enim *r* fuerit huiusmodi residuum, erit $(2m+1)p+r$ idoneus valor pro *a.*

COROLLARIUM 5

49. Omnia haec residua *r* erunt autem minora quam $2m+1$, neque tamen omnes numeri minores quam $2m+1$ erunt valores ipsius *r,* quia numerus *r* maior esse nequit quam *m.* Dabuntur ergo semper *m* numeri, qui pro *r* adhiberi non poterunt.

COROLLARIUM 6

50. Valores vera ipsius *r* erunt primo omnes numeri quadrati ipso $2m+1$ minores, tum vero residua, quae in divisione maiorum quadratorum per $2m+1$ remanent; neque tamen unquam numerus omnium diversorum valorum ipsius *r* maior esse poterit numero *m.*

SCHOLION

51. Ut usus huius theorematis clarius appareat atque per exempla numerica illustrari possit, sequentia problemata adiicere visum est, ex quibus non solum veritas theorematis luculentius perspicietur, sed etiam vicissim patebit, quoties *a* non habuerit valorem hic assignatum, toties formulam $a^m - 1$ non esse divisibilem per $2m+1$. Cum igitur haec formula $a^{2m} - 1$ semper sit divisibilis per $2m+1$, quoties $a^m - 1$ divisionem per $2m+1$ non admittit, toties $a^m + 1$ per $2m+1$ divisibile esse oportebit.

EXEMPLUM 1

52. *Invenire valores ipsius a, ut* $a^2 - 1$ *fiat divisibile per 5.*

Residua, quae ex divisione quadratorum per 5 remanent, sunt 1 et 4; hinc necesse est, ut sit vel $a = 5p+1$ vel $a = 5p+4$ sive $a = 5p-1$. Priori casu fit $aa-1$ seu $(a-1)(a+1) = 5p(5p+2)$, posteriori autem $= (5p-2)5p$; utroque ergo divisibilitas per 5 perspicitur. Sin autem fuerit vel $a = 5p+2$ vel $a = 5p+3$, neutro casu formula $aa-1$ per 5 erit divisibilia.

EXEMPLUM 2

53. *Invenire valores ipsius a, ut haec forma* a^3-1 *fiat per* 7 *divisibilis.*

Tria residua, quae in divisione omnium quadratorum per 7 remanent, sunt 1, 2, 4. Hinc valores ipsius *a* sunt $7p+1$, $7p+2$ et $7p+4$; sin autem fuerit vel $a=7p+3$ vel $7p+5$ vel $7p+6$, tum non formula proposita a^3-1, sed haec a^3+1 per 7 fiet divisibilis.

EXEMPLUM 3

54. *Invenire valores ipsius a, ut haec forma* a^5-1 *fiat per* 11 *divisibilis.*

Numeri quadrati per 11 divisi dabunt 5 diversa residua, quae sunt 1, 3, 4, 5, 9. Hinc formula a^5-1 per 11 erit divisibilis, si fuerit $a=11p+r$ denotante *r* unumquemque ex numeris 1, 3, 4, 5, 9. Sin autem pro *a* sumatur quidam ex his numeris 2, 6, 7, 8, 10 multiplo quocunque ipsius 11 auctus, tum a^5+1 per 11 erit divisibile.

THEOREMA 12

55. *Si fuerit* $a=f^3\pm(3m+1)\alpha$ *existente* $3m+1$ *numero primo, tum haec forma* a^m-1 *semper erit per* $3m+1$ *divisibilis.*

DEMONSTRATIO

Ob $3m+1$ numerum primum erit $f^{3m}-1$ divisibile per $3m+1$. At est $f^{3m}-1=\left(f^3\right)^m-1$, unde quoque haec formula $\left(f^3\pm(3m+1)\alpha\right)^m-1$ erit divisibilis per $3m+1$. Quare si surnatur $a=f^3\pm(3m+1)\alpha$, tum haec formula a^m-1 erit per $3m+1$ divisibilis. Q. E. D.

COROLLARIUM 1

56. Ad valores ergo ipsius *a* inveniendos omnia residua, quae oriuntur, si cubi per $3m+1$ dividantur, notari debent. Unumquodque enim horum residuorum multiplo ipsius $3m+1$ quocunque auctum dabit valorem idoneum pro *a*.

COROLLARIUM 2

57. Cum $3m+1$ esse debeat numerus primus, necesse est, ut *m* sit numerus par, sicque numerus primus $3m+1$ unitate superabit multiplum senarii. Hinc erunt numeri pro *m* et $3m+1$ adhibendi sequentes:

$m=2,\ 4,\ 6,\ 10,\ 12,\ 14,\ 20,\ 22,\ 24,\ 26,\ 32$ etc.,

$3m+1=7,\ 13,\ 19,\ 31,\ 37,\ 43,\ 61,\ 67,\ 73,\ 79,\ 97$ etc.

COROLLARIUM 3

58. Si ergo numeri cubici per hos numeros primos $3m+1$ dividantur, sequentia residua remanebunt:

Divisores	Residua
7	1, 6
13	1, 5, 8, 12
19	1, 7, 8, 11, 12, 18
31	1, 2, 4, 8, 15, 16, 23, 27, 29, 30
37	1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36

etc.

In his residuis primo occurrunt omnes cubi divisoribus minores, deinde si quodpiam residuum fuerit *r* pro divisore $3m+1$, tum quoque aliud dabitur residuum $=3m+1-r$ *;* si enim cubus f^3 dederit residuum *r*, cubus $\left(3m+1-f\right)^3$ dabit residuum $-r$ seu $3m+1-r$.

SCHOLION

59. Notatu hic dignum est numerum residuorum perpetuo esse $=m$, si divisor fuerit $=3m+1$. Semper ergo dantur tres cubi, quorum radices sint $<3m+1$, ex quibus idem residuum resultat. Scilicet hi tres cubi 1^3, 2^3, 4^3 per 7 divisi idem dant residuum $=1$ et hi tres cubi 2^3, 5^3 et 6^3 per 13 divisi idem dant residuum 8. Praeterea hic notari convenit, si pro *a* alii valores praeter hos assignatos capiantur, tum a^m-1 non esse per $3m+1$ divisibile; quod etsi verum esse facile deprehenditur, tamen eius demonstratio ex praecedentibus non sequitur pertinetque haec veritas ad id genus, quod nobis nosse, non autem demonstrare licet. His ergo casibus, quibus a^m-1 per $3m+1$ non est divisibile, haec formula $a^{2m}+a^m+1$ divisionem admittet.

THEOREMA 13

60. *Si fuerit* $a=f^n\pm\left(mn+1\right)\alpha$ *existente* $mn+1$ *numero primo, tum haec forma* a^m-1 *erit divisibilis per* $mn+1$.

DEMONSTRATIO

Ob $mn+1$ numerum primum erit $f^{mn}-1$ divisibile per $mn+1$. At est $f^{mn}-1=\left(f^n\right)^m-1$, unde quoque haec forma $\left(f^n\pm\left(mn+1\right)\alpha\right)^m-1$ erit divisibilis per $mn+1$. Quare si ponatur $a=f^n\pm\left(mn+1\right)\alpha$, haec formula a^m-1 per $mn+1$ dividi poterit. Q. E. D.

COROLLARIUM 1

61. Si ergo potestates exponentis *n* per numerum primum $mn+1$ dividantur, singula residua vel ipsa vel multiplo ipsius $mn+1$ quocunque aucta idoneos praebebunt valores pro *a*, ut a^m-1 fiat per $mn+1$ divisibile.

COROLLARIUM 2

62. Hinc si a^m-1 non fuerit per $mn+1$ divisibile, tum valor ipsius *a* in hac expressione $f^n \pm (mn+1)\alpha$ non continebitur seu nulla dabitur potestas exponentis *n,* quae per $mn+1$ divisa relinquat *a.*

SCHOLION

63. Propositionis huius conversa, si omni modo examinetur, quoque vera deprehenditur; ita ut, quoties a^m-1 sit divisibile per $mn+1$, toties quoque valor ipsius *a* in formula $f^n \pm (mn+1)\alpha$ contineatur; seu toties dabitur potestas f^n, quae per $mn+1$ divisa relinquat *a* pro residuo. Ita, cum observassem formulam $2^{64}-1$ esse per 641 divisibilem, ob $m=64$ fiet $n=10$, dabitur quoque potestas dignitatis decimae, quae per 641 divisa relinquat 2. Atque revera huiusmodi potestatem deprehendi esse 96^{10}. Praeterea vero cum $2^{32}-1$ non sit divisibile per 641, hoc casu fit $m=32$ et $n=20$; nulla igitur datur potestas dignitatis vicesimae, quae per 641 divisa relinquat 2. Veritas huius posterioris asserti rigorose est evicta, sed adhuc desideratur demonstratio harum propositionum conversarum: scilicet si a^m-1 fuerit divisibile per numerum primum $mn+1$, tum quoque semper *a* esse numerum in hac formula $f^n \pm (mn+1)\alpha$ comprehensum, atque si *a* non contineatur in formula $f^n \pm (mn+1)\alpha$, tum quoque a^m-1 per $mn+1$ divisionem non admittere. Quarum propositionum si altera demonstrari posset, simul veritas alterius esset evicta. Ceterum theorema hic demonstratum huc redit, ut, quoties f^n-a fuerit divisibile per $mn+1$, toties quoque formula a^m-1 sit per $mn+1$ divisibilis. In hoc genere latius patet theorema sequens.

THEOREMA 14

64. *Si fuerit* f^n-ag^n *divisibile per numerum primum* $mn+1$, *tum quoque* a^m-1 *erit divisibile per* $mn+1$.

DEMONSTRATIO

Cum ponatur formula f^n-ag^n divisibilis per $mn+1$, erit quoque haec formula $f^{mn}-a^m g^{mn}$, quippe quae per illam dividi potest, divisibilis per $mn+1$. At cum $mn+1$ sit numerus primus, per eum divisibilis erit haec forma $f^{mn}-g^{mn}$; unde quoque differentia $g^{mn}\left(a^m-1\right)$ seu ipsa formula a^m-1 per $mn+1$ erit divisibilis, propterea quod *g* per $mn+1$ divisionem admittere nequeat, nisi simul *f* per eundem esset divisibile, qui casus in nostro ratiocinio perpetuo excluditur. Q. E. D.

COROLLARIUM 1

65. Si ergo $a^m - 1$ per $mn+1$ non fuerit divisibile, tum quoque nulli dantur numeri *f* et *g*, ut haec formula $f^n - ag^n$ per $mn+1$ fiat divisibilis.

COROLLARIUM 2

66. Si superiorus propositionis conversa demonstrari posset, tum quoque evictum foret, quoties $f^n - a$ per $mn+1$ dividi nequeat, tum ne hanc quidem formulam $f^n - ag^n$ divisionem per $mn+1$ admittere posse; simul vero etiam pateret, si $f^n - ag^n$ sit divisibile per $mn+1$, tum quoque dari huiusmodi formulam $f^n - a$, quae sit per $mn+1$ divisibilis.

THEOREMA 15

67. *Si huiusmodi formula* $af^n - bg^n$ *fuerit divisibilis per numerum primum* $mn+1$, *tum quoque haec formula* $a^m - b^m$ *erit per* $mn+1$ *divisibilis.*

DEMONSTRATIO

Si fuerit $af^n - bg^n$ divisibile per $mn+1$, tum quoque haec formula $a^m f^{mn} - b^m g^{mn}$ erit per $mn+1$ divisibilis. At ob $mn+1$ numerum primum erit quoque haec formula $f^{mn} - g^{mn}$ ideoque et haec $a^m f^{mn} - a^m g^{mn}$ per $mn+1$ divisibilis; subtrahatur haec ab illa $a^m f^{mn} - b^m g^{mn}$ atque residuum $g^{mn}\left(a^m - b^m\right)$ seu $a^m - b^m$ per $mn+1$ erit divisibile. Q. E. D.

COROLLARIUM 1

68. Si itaque $a^m - b^m$ non fuerit per $mn+1$ divisibile, tum nulli dabuntur numeri pro *f* et *g* substituendi, ut huiusmodi formula $g^{mn}\left(a^m - b^m\right)$ sit per $mn+1$ divisibilis.

COROLLARIUM 2

69. Huius propositionis conversa, quod, si fuerit formula $a^m - b^m$ divisibilis per *mn*+1, simul dentur numeri *f* et *g*, ut $af^n - bg^n$ fiat divisibilis per $mn+1$, utcunque examinetur, vera deprehenditur. Interim tamen eius demonstratio etiamnum desideratur.

SCHOLION

70. Casus huius propositionis inversae demonstrari potest, quo numeri *m* et *n* sunt inter se primi; hoc enim casu semper eiusmodi numeri μ et *v* exhiberi possunt, ut sit $\mu n \pm 1 = vm$. Namque si inter numeros *m* et *n* ea operatio instituatur, quae pro maximo communi divisore institui solet, atque quoti notentur ex iisque fractiones ad $\frac{m}{n}$ appropinquantes quaerantur, ultima erit $\frac{m}{n}$, et si penultima fuerit $\frac{\mu}{v}$ erit $\mu n \pm 1 = vm$. Hoc ergo lemmate praemisso demonstratio propositionis conversae, qua *m* et *n* sunt numeri

inter se primi, ita se habebit.

THEOREMA 16

71. *Si m et n fuerint numeri primi inter se atque ista formula* $a^m - b^m$ *divisibilis sit per numerum* $mn+1$, *tum dabitur formula* $af^n - bg^n$ *divisibilis per* $mn+1$.

DEMONSTRATIO

Ponatur $f = a^\mu$ et $g = b^\mu$ atque formula $af^n - bg^n$ abibit in hanc $a^{\mu n+1} - b^{\mu n+1}$; quare si μ ita capiatur, ut sit $\mu tn+1 = vm$, habebitur $a^{vm} - b^{vm}$; quae cum sit divisibilis per $a^m - b^m$, quoque per $mn+1$divisibilis erit sicque dabitur casus, quo $af^n - bg^n$ divisibile erit per $mn+1$.

Sin autem fuerit $\mu n - 1 = vm$, tum sumatur $f = b^\mu$ et $g = a^\mu$ fietque $af^n - bg^n = ab^{\mu n} - ba^{\mu n} = ab\left(b^{\mu n-1} - a^{\mu n-1}\right) = -ab\left(a^{vm} - b^{vm}\right)$ ideoque erit per $mn+1$divisibilis. Q. E. D.

COROLLARIUM 1

72. Si ergo *m* et *n* fuerint numeri inter se primi atque $mn+1$numerus primus, tum istae propositiones sunt demonstratae:

1. *Si* $af^n - bg^n$ *fuerit divisibile per mn* + 1, *tum quoque* $a^m - b^m$ *erit per* $mn+1$ *divisibile, et si illa formula nullo modo sit divisibilis per* $mn+1$, *tum etiam haec non erit divisibilis.*

II. *Si* $a^m - b^m$ *fuerit divisibile per* $mn+1$, *tum dabitur numerus huius formae* $af^n - bg^n$ *per* $mn+1$*divisibilis, atque si* $a^m - b^m$ *per* $mn+1$ *divisionem non admittat, tum nullus dabitur numerus formae* $af^n - bg^n$ *per* $mn+1$*divisibilis.*

COROLLARIUM 2

73. Si *m* sit numerus par, tum *b* aeque negative atque affirmative accipi potest; hoc ergo casu si $a^m - b^m$ fuerit divisibile per $mn+1$, tum etiam eiusmodi formula $af^n + bg^n$ per $mn+1$divisibilis assignari poterit; id quod etiam inde patet, quod *n* sit numerus impar ideoque potestas g^n negativa fieri queat.

COROLLARIUM 3

74. Simili modo demonstrabitur, si fuerint ut ante *m* et *n* numeri inter se primi atque haec formula $a^m - b^m$ sit divisibilis per *mp* + 1, tum quoque exhiberi posse formulam huiusmodi $af^n - bg^n$ divisibilem per *mp* + 1.