Theoremata circa Divisores Numerorum

Auctore L. Eulero

Theorems on Divisors of Numbers

Translated by David Zhao
Department of Computer Science
University of Texas at Austin

Abstract

This work contains Euler's second proof Fermat's Little Theorem, as a consequence of the theorem that $(a+b)^p = a^p + b^p \pmod{p}$, as §10. Euler's second major result (§29) is that $a^{2^m} + b^{2^m}$ has no divisors except for $2^{m+1}n+1$, which he then uses to provide an additional refutation of Fermat's conjecture that $2^{2^n}+1$ is a prime number, for all n, which he had originally discovered to be false several years earlier.

Euler then ends the paper with several other theorems, and leaves off with several conjectures, concerning division modulo some given primes.

According to C. G. J. Jacobi, a treatise with this title was read to the Berlin Academy on March 23, 1747; and according to the records, this paper was presented to the St. Petersburg Academy on September 2, 1748. It was originally published in *Commentarii academiae scientiarum Petropolitanae* 1, 1750, pp. 20–48, and appeasr in Series 1, Volume 2, pp. 62–85 of the *Opera Omnia.* Finally, its Eneström index is 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,

Some time ago, the greatest geometers recognized that many distinguished properties lay hidden in the nature of numbers, the knowledge of which would increase the boundaries of mathematics in no moderate way. At first glance, the theory of numbers seems only to deal with the elements of arithmetic, and hardly anything that requires any expertise or a method of analysis. But as it turns out, this theory has produced not only proofs of very difficult truths, but also statements whose certainty seems clear, even though proofs for them have yet to be found.

The famous geometer Fermat produced many theorems of the latter kind, whose truth, even though a proof was lacking, seemed no less certain. And this especially merits all attention, insofar as truths of this kind in pure mathematics exist, which seem true to us, even though we are unable to prove them. And this happens so much in arithmetic, which is considered to be the most basic and best known theory among all areas of mathematics, that it would be hard for me to deny that similar truths might be discovered in the other areas.

Certainly in geometry, there is no proposition for which neither its truth nor falsity can be established by the firmest reasoning. Thus, since the more abstruse a truth may be, the less evident an approach to its proof should be, we would not be able to deny that arithmetic especially, which deals itself with the nature of numbers, contains the most abstruse truths of all.

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 abhorere 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 obrem non inviliter me operam ac studium in indagatione demonstrationum quarumdam 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 formua $a^n \pm b^n$ 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.

Theorema 1.
1. Si p fuerit numerus primus, omnis 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 $(a+b)^p = a^p + \frac{p}{1} \cdot a^{p-1}b + \frac{p(p-1)}{1\cdot 2} \cdot a^{p-2}b^p + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3} \cdot a^{p-3}b^3 + \ldots + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3} \cdot a^3b^{p-3} + \frac{p(p-1)}{1\cdot 2} \cdot a^2b^{p-2} + \frac{p}{1} \cdot ab^{p-1} + b^p$, qua expressione substituta, binisque terminis, qui easdem habent uncias; coniunctis, erit $(a+b)^p - a^p - b^p = \frac{p}{1}ab(a^{p-2} + b^{p-2}) + \frac{p(p-1)}{1\cdot 2}a^2b^2(a^{p-4} + b^{p-4}) + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}a^3b^3(a^{p-6} + b^{p-6}) + \frac{p(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3\cdot 4}(a^{p-8} + b^{p-8})a^4b^4 +$ 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

And even some of the greatest mathematicians have fallen short, because they judge truths of this sort to be entirely unfruitful and for that reason unworthy, and have given no effort towards their investigation. And more than that, as knowledge of every truth is a worthy matter in itself, even of those which seem unrelated to popular use; we have seen that all truths, at least those which we are able to understand, are so greatly connected with one another, that we cannot consider any of them altogether useless without some rashness.

And so, even if a certain proposition seems to be this way, so that regardless of whether it turns out to be true or false, it would be of no benefit to us anyway, still the method itself, by which we would establish its truth or falsity, nevertheless may be useful in opening up the way for us to discover other, more useful truths. For that reason, I firmly believe that I have not uselessly expended work and effort in investigating the proofs of these certain propositions. Hence, this theory of divisors does not lack any use, but rather may at some time show a utility in analysis that cannot be scorned.

I am also especially certain that the method of calculation which I have used here can at some point contribute no small amount of aid to other, more serious investigations. Moreover, the propositions for which I provide proofs here, deal with divisors of numbers of the form $a^n \pm b^n$, on some of which the aforementioned Fermat has published, albeit without proof.

Lastly, since this paper deals entirely with whole numbers, all letters of the alphabet will always denote whole numbers here.

Theorem 1.
1. If p is a prime number, then every number of the form $(a+b)^p - a^p - b^p$ is divisible by p.

Proof.
If the binomial $(a+b)^p$ is expanded in the usual manner, we have $(a+b)^p = a^p + \frac{p}{1} \cdot a^{p-1}b + \frac{p(p-1)}{1\cdot 2} \cdot a^{p-2}b^p + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3} \cdot a^{p-3}b^3 + \ldots + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3} \cdot a^3b^{p-3} + \frac{p(p-1)}{1\cdot 2} \cdot a^2b^{p-2} + \frac{p}{1} \cdot ab^{p-1} + b^p$. And then by making the substitution of combining all the terms that have the same power, we arrive at $(a+b)^p - a^p - b^p = \frac{p}{1}ab(a^{p-2} + b^{p-2}) + \frac{p(p-1)}{1\cdot 2}a^2b^2(a^{p-4} + b^{p-4}) + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}a^3b^3(a^{p-6} + b^{p-6}) + \frac{p(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3\cdot 4}(a^{p-8} + b^{p-8})a^4b^4 +$ etc.

First note that all the terms, even though they appear as fractions, are all nevertheless whole numbers, as they remain whole numbers when evaluated. Therefore, since each term has a factor of p, each is divisible by p, unless it is somewhere either entirely removed or divided by a factor in the denominator. But in each term, all the factors of the denominator are less than quia adeo non ultra $\frac{1}{2}p$ crescunt, ideoque factor numeratorum p nusquam per divisionem tollitur. Deinde cum p sit per hypoth. numerus primus, is nusquam per divisionem minuetur. Quocirca singulae unciae $\frac{p}{2}$; $\frac{p(p-1)}{1\cdot 2}$; $\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}$; 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 $2^p - 2 = 2(2^{p-1} - 1)$: 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 sit 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 assumpta formula $a^p - a$ per p divisibili, sit quoque formula $(a+1)^p - a - 1$ per p divisibilis; simili modo in eadem hyphothesi 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.

p becasue they cannot grow to be greater than $\frac{p}{2}$, and so for that reason a factor of p in the numerator is never removed through the division. Therefore, since p is a prime number by assumption, it is never reduced by division. And on that account, the single terms $\frac{p}{1}$, $\frac{p(p-1)}{1\cdot 2}$, $\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}$, etc., which form the expression $(a+b)^p - a^p - b^p$, is always divisible by p, provided that p is prime. □

Corollary 1.
2. So if we let $a = 1$ and $b = 1$, then $2^p - 2$ is divisible by p, if p is prime. Also, since $2^p - 2 = 2(2^{p-1} - 1)$, the second factor is also divisible by p. And unless $p = 2$, the first factor of 2 is not divisible by p, and so it follows that $2^{p-1} - 1$ is always divisible by p, so long as p is a prime number other than 2.

Corollary 2.
3. Taking p to be successive prime numbers, it follows that 3 divides $2^2 - 1$; 5 divides $2^4 - 1$; 7 divides $2^6 - 1$; 11 divides $2^{10} - 1$, and so on; which for smaller numbers is clear, now for larger numbers equally clear. Thus, since 641 is a prime number, the number $2^{640} - 1$ is necessarily divisible by 641. Or if we divide 2^{640} by 641, then after the division, the remaining residual is equal to 1.

Theorem 2.
4. If either $a^p - a$ or $b^p - b$ are divisible by a prime p, then $(a+b)^p - a - b$ is also divisible by the same prime p.

Proof.
Since by § 1, the formula $(a+b)^p - a^p - b^p$ is divisible by p, if p is prime, and since both $a^p - a$ and $b^p - b$ are assumed to be divisible by p, then the sum of these three formulas, $(a+b)^p - a - b$, is certainly divisible by p, if it is a prime number. □

Corollary 1.
5. If we let $b = 1$, then since $1^p - 1 = 0$ is divisible by p, it follows that if $a^p - a$ is divisible by p, then $(a+1)^p - a - 1$ is also divisible by p.

Corollary 2.
6. If we assume that $a^p - a$ is divisible by p, then $(a+1)^p - a - 1$ is also divisible by p; and in the same way, $(a+2)^p - a - 2$, and moreover $(a+3)^p - a - 3$, etc., and in general $c^p - c$, is divisible by 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 divisibiliem. 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 $c^p - c = c(c^{p-1} - 1)$, 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 divisibiles.

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 $p2m + 1$, 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

Theorem 3.
7. If p is a prime number, then every number of the form $c^p - c$ is divisible by p.

Proof.
If we let $a = 1$ in § 6, then since $a^p - a = 0$ is divisible by p, it follows that $2^p - 2$, $3^p - 3$, $4^p - 4$, etc., and in general $c^p - c$ is divisible by p. □

Corollary 1.
8. So whatever we take c to be, when p is prime, every number of the form $c^p - c$ is divisible by p.

Corollary 2.
9. Since $c^p - c = c(c^{p-1} - 1)$, then either c itself or $c^{p-1} - 1$ is divisible by p, but not both; because if c is not divisible by p, then $c^{p-1} - 1$ is certainly divisible by p.

Corollary 3.
10. If p is a prime number, then every number of the form $a^{p-1} - 1$ is divisible by p, except those cases, in which the number a itself is divisible by p.

Theorem 4.
11. If neither a nor b is divisible by a prime number p, then every number of the form $a^{p-1} - b^{p-1}$ is divisible by p.

Proof.
Since neither a nor b is divisible by p, and since p is assumed to be prime, both $a^{p-1} - 1$ and $b^{p-1} - 1$ are divisible by p. Therefore, the difference of these numbers, $a^{p-1} - b^{p-1}$, is divisible by p. □

Corollary 1.
12. Since every prime number except 2 (whose remainder in division is clear in itself) is odd, let $p = 2m + 1$. Then it is clear that every number of the form $a^{2m} - b^{2m}$ is divisible by $2pm + 1$, provided that neither a nor b itself is divisible by $2m + 1$.

Corollary 2.
13. As b is not divisible by $2m + 1$, neither b^{2m} nor $2b^{2m}$ is divisible by $2m + 1$; because adding $2b^{2m}$ to $a^{2m} - b^{2m}$, which is divisble by $2m + 1$ results in the number $a^{2m} + b^{2m}$, which is not divisible by $2m + 1$; unless both a and b are divisible by $2m + 1$.

per $2m+1$ sit divisibilis.

Corollarium 3.
14. Quoniam ob $2m$ numerum parem formula $a^{2m}-b^{2m}$ factores habet $(a^m-b^m)(a^m+b^m)$, 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 sue $a^{2n}-b^{2n}$ 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 $4n-1$, neque propterea ullus eius factor. At cum $4n-2=2(2n-1)$ 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.

Corollary 3.
14. Since $a^{2m}-b^{2m}$ factors into $(a^m-b^m)(a^m+b^m)$ (because $2m$ is an even number), it follows that one of these factors is divisible by $2m+1$, although both cannot be divisible by $2m+1$ at the same time. This is because if $2m+1$ is a prime number, and neither a nor b is divisible by $2m+1$, then either a^m-b^m or a^m+b^m is divisible by $2m+1$.

Corollary 4.
15. If $m=2n$ and either a^m-b^m, or $a^{2n}-b^{2n}$ is divisible by $2m+1=4n+1$, then by the same reasoning either a^n-b^n or a^n+b^n is divisible by the prime number $4n+1$.

Theorem 5.
16. The sum of two squares a^2+b^2 can never be divided by any prime number of the form $4n-1$, unless both a and b are divisible by $4n-1$.

Proof.
If $4n-1$ is a prime number, and neither a nor b is divisible by it, then $a^{4n-2}-b^{4n-2}$ is divisible by $n-1$ (11), and hence $a^{4n-2}+b^{4n-2}$ is not divisible by $4n-1$, and for that reason neither is any factor of it. And since $4n-2=2(2n-1)$ is a even number times an odd number, $a^{4n-2}+b^{4n-2}$ has a^2+b^2 as a factor; since it cannot be the case that a^2+b^2 is any sum of two squares divisible by $4n-1$. □

Corollary 1.
17. Since all prime numbers can be written either as $4n+1$ or $4n-1$, if $4n-1$ is not a prime number, then it has a divisor of the form $4n-1$; because a number of the form $4n+1$ can never be derived from whole numbers of the form $4n+1$. On this account, since the sum of two squares cannot be divided by any prime number of the form $4n-1$, it is not divisible by any number of the form $4n-1$, even if that number is not prime.

Corollary 2.
18. So the sum of two squares a^2+b^2 is not divisible by any term in the series:

3, 7, 11, 15, 19, 23, 27, 31, 35, etc.

Hence, all prime numbers (except 2) that can be divisors of this sum of two squares have the form $4n+1$; provided that a and b have no common divisors.

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 oritur forma $4a+4b+1$ seu $4n+1$, ideoque nullus numerus huius formae $4n-1$ summa duorum quadratorum esse potest.

Quod vero summa duorum quadratorum ne divisorem quidem formae $4n-1$ admittat, ab omnibus scriptoribus methodi Diophanteae 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 vero 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, nisi uterque numerus a et b

Corollary 3.

19. Since every number is either a prime or a product of primes, the sum of two squares cannot have a prime number as a divisor, unless it is expressible in the form $4n+1$. Therefore, prime divisors of the sum of two squares are contained in the series:

2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc.

Discussion.

20. It is easy to see that a number of the form $4n-1$ can never be the sum of two squares. Squares are either even or odd: the former have form $4a$, the latter $4b+1$. For this reason, for the sum of two squares to be odd, it must be that one is even and the other odd, from which we have $4a+4b+1$ or $4n+1$, and thus no number of the form $4n-1$ can be the sum of two squares.

Next, that the sum of two squares also does not admit any divisor of the form $4n-1$, has always been affirmed by all the authors of the Diophantine method: but no one at all, as far as I know, has proven it, except Fermat, who however never published his proof, so that it now seems to me that I am the first to have published a proof of the truth that no number either of the form $4n-1$ or divisible by a number of the same form can ever be the sum of two squares.

Therefore, from this it follows that every sum of two relatively prime squares either is itself a prime number or has no divisors except for two, unless they can be written in the form $4n+1$.

Theorem 6.

21. All divisors of the sum of two relatively prime numbers to the fourth power are either 2 or have the form $8n+1$.

Proof.

Let a^4 and b^4 be two primes to the fourth power. Then either both are odd, or one is even and the other odd. In the first case, 2 is a divisor of the sum a^4+b^4, and in the other case, the odd divisors, if they exist, are of the form $4n+1$. This is because no divisor of the form $4n-1$ is possible (16), since fourth powers are also squares; and because numbers of the form $4n+1$ can be expressed either as $8n+1$ or as $8n-3$.

However, I claim that no number of the form $8n-3$ can be a divisor of the sum of two fourth powers. For the proof, first, if $8n-3$ be a prime number, then a number of the form $a^{8n-4}+b^{8n-4}$ is divisible by it, from which it follows that a number of the form $a^{8n-4}+b^{8n-4}$ is thus not divislbe by the number $8n-3$, unless both a

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: $8n \pm 1$ et $8n \pm 3$: 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 si 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 confideratione 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^7 alios non admittet divisorse, 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

and b are separately divisible by it. However, that case is excluded by the assumption that the numbers a and b are relatively prime.

Therefore, since $a^{8n-4}+b^{8n-4} = a^{4(2n-1)}+b^4(2n-1)$ is not divisible by $8n-3$, it also cannot be divided by any factor fo $8n-3$. Then, since $2n-1$ is an odd number, it is a factor of a^4+b^4, which is therefore not divisible by any prime number of the form $8n-3$. Thus, all prime numbers except for two, which divides a^4+b^4, are of the form $8n+1$. Moreover, a number of the form $8n-3$ never arisesfrom the multiplication of two or more sum divisors: and so it follows that no number of the form $8n-3$ that is either prime or composite divides the sum of two relatively prime numbers to the fourth power. □

Corollary 1.
22. Since all odd numbers can be written in one of the following forms: $8n \pm 1$ and $8n \pm 3$: except numbers of the form $8n+1$ no other can be a divisor of the sum of two numbers to the fourth power.

Corollary 2.
23. Therefore, all prime divisors of the sum of two relatively prime numbers to the fourth power are either 2 or contained in the series: 17, 41, 73, 89, 97, 113, 137, 193, etc, which is the series of all prime numbers of the form $8n+1$.

Corollary 3.
24. Therefore, if any number n is the sum of two numbers to the fourth power, then it is either prime or has no divisors except those which have the form $8n+1$. And so the investigation of divisors is drawn to a marvelous close.

Corollary 4.
25. And so no number that has a divisor expressible in the form $8n+1$ is the sum of two numbers to the fourth power, unless it also has four equal divisors, but those are generally thrown out in considering fourth powers.

Theorem 7.
26. Every divisor of numbers of the form a^8+b^8, given that a and b are relatively prime numbers, is either 2 or of the form $16n+1$.

Proof.
Because a^8 and b^8 are also fourth powers, their sum a^8+b^8 admits no divisors other than those of the form $8n+1$. Numbers of the form $8n+1$ can be written either as $16n+1$ or $16n-7$. If $16n-7$ is a prime number, then a number of the form $a^{16n-8}+b^{16n-8}$ (13)

$a^{16n-8} + b^{16n-8}$ (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 $16n + 1$, 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, cumdemonstratum 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 digitas 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 gener 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 comsumeret, si aliis nu-

or $a^{8(2n-1)} + b^{8(2n-1)}$ is not divisible by it, and therefore neither is any of its factors. But because $2n-1$ is an odd number, it is a divisor of $a^{+}b^8$, which therefore is not divisible by any prime number of the form $16n - 7$, and for that reason, has no prime divisors other than those of the form $16n+1$. Moreover, the multiplication of two or more numbers of the form $16n + 1$ always produces a number of the same form, and so never results in a number of the form $16n-7$. Therefore, since no number of the form $16n - 7$ can be a divisor of $a^8 + b^8$, it follows that all divisors of $a^8 + b^8$, if they exist, whether prime or composite, are always of the form $16n + 1$. □

Corollary 1.
27. Therefore, no number, which is not expressible in the form $16n+1$, can ever be the divisor of two relatively prime numbers to the eighth power.

Corollary 2.
28. So if someone wanted to investigate the divisors of any number of the form a^8+b^8, he should try division by no prime numbers other than those of the form $16n+1$, since it was proven that all other prime numbers cannot be divisors of this form.

Theorem 8.
29. The sum of two numbers $a^{2^m} + b^{2^m}$ whose exponent is a power of two admits no divisors other than those of the form $2^{m+1}n + 1$.

Proof.
In the manner that we proved that all divisors of a^2+b^2 are of the form $4n+1$, and from there showed that that divisors of $a^4 + b^4$ are of the form $8n + 1$, and those of the form $a^8 + b^8$ are of the form $16n + 1$; so it can be shown in the same way that $a^{16}+b^{16}$ admits no divisors other than those of the form $32n+1$. From here on, we may further understand that $a^{32} + b^{32}$, $a^{64} + b^{64}$, and so on, can have no divisors other than those of the form $64n + 1$, $128n + 1$, etc. And so in general it is evident that there are no divisors of $a^{2^m} + b^{2^m}$ other than those of the form $2^{m+1}n + 1$. □

Corollary 1.
30. Therefore, no prime number that is not of the form $2^{m+1}n+1$ can ever be a divisor of a number of the form $a^{2^m} + b^{2^m}$.

Corollary 2.
31. Therefore, one investigating the divisors of numbers of the form $a^{2^m} + b^{2^m}$ would be uselessly wasting his ef-

meris primis praeter eos, quas forma $2^{m+1}n+1$ suppeditat, divisionem tentare vellet.

Scholion 1.
32. Fermatius †affirmaverant†, etiamsi id se demonstrare non posse ingenue esset confessus, omnes numeros ex hac forma $2^{2^m}+1$ 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 $2^{2^m}+1$ 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^np continebitur, ita ut p sit numerus impar, hocque casu $a^{2^n}+b^{2^n}$ divisor erit formae a^m+b^m existente $m = 2^np$. 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 $a-b$; praetera 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.

fort, if he wanted to try division by any prime numbers except those expressible in the form $2^{m+1}n+1$.

Discussion 1.
32. Fermat had held, even though he had confessed that he frankly was unable to prove it, that all numbers of the form $2^{2^m}+1$ are prime; and then elsewhere tried to resolve a very difficult problem, which involved finding a prime number greater than a given number. But from the last theorem, it is clear that unless the number $2^{2^m}+1$, it has no divisors other than those which are of the form $2^{m+1}n+1$.

And so since I wanted to examine the truth of this renowned claim of Fermat for the case of $2^{32}+1$, I managed a huge shortening of this, by not having to try division by any prime numbers except those expressible in the form $64n+1$. And so with the problem reduced to this, I soon discovered that by setting $n = 10$, the prime number 641 is a divisor of the number $2^{32}+1$, and so the well-known problem asking for a prime number larger than a given number, still remains unsolved.

Discussion 2.
33. The sum of two numbers a^m+b^m to the same power always has algebraically defined numbers, unless m is a power of two. This is because if m is an odd number, then a^m+b^m always has $a+b$ as a divisor, and if p is a divisor of m, then a^p+b^p will also divide a^m+b^m. But if m is an even number, it can be written in the form 2^np, s that p is an odd number, and in which case $a^{2^n}+b^{2^n}$ is a divisor of a^m+b^m, if $m = 2^np$. And if p has a divisor q, then in that case, $a^{2^n}q+b^{2^n}q$ will be a divisor of a^m+b^m. So on that account, a^m+b^m cannot be a prime number unless m is a power of two. Then in this case, if a^m+b^m is not a prime number, then it has no other divisors except for those expressible as $2mn+1$.

But on the other hand, if the difference a^m-b^m of two numbers to the same power is considered, then it will always have $a-b$ as a divisor; and for the same reason, if the exponent m has a divisor p, then a^p-b^p will also be a divisor of a^m-b^m. And hence, if m is a prime number, then a^m-b^m has no other algebraically defined divisor except for $a-b$, because if a^m-b^m is a prime number, then it is necessary that m is a prime number and $a-b=1$.

However, in these cases a^m-b^m is not even always a prime number, but so long as $2m+1$ is a prime number, then a^m-b^m will be divisible by it. But nevertheless, it could still have other divisors, which I will investigate here.

Theorem 9.

34. Si differentia potestatum $a^m - b^m$ fuerit divisibilis per numerum primum $2n+1$, atque p six maximus communis divisor numerorum m et $2n$, tum quoque $a^p - b^p$ erit divisibilit 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 $\alpha m + q$ pro $2n$ est quoque $a^{\alpha m+q} - b^{\alpha m+q}$ per $2n+1$ divisibilis: a quo formula si prior subtrahatur, residuum $a^q b^{\alpha m} - b^{\alpha m+q} = b^{\alpha m}(a^q - b^q)$ quoque per $2n+1$ erit divisibile.

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 $b^{\beta q}(a^r - b^r)$ seu $a^r - b^r$ pariter per $2n+1$ reit divisibile. Simili modo patebit, si fuerit $q = \gamma r + s$ tam 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 $2n+1$.

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.

Corollarium 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

34. If the difference of two powers $a^m - b^m$ is divisible by a prime number $2n+1$, and p is the greatest common divisor of m and $2n$, then $a^p - b^p$ is also divisible by $2n+1$.

Proof.
Because $2n+1$ is a prime number, $a^{2n} - b^{2n}$ is divisible by it, and by hypothesis $a^m - b^m$ is also divisible by $2n+1$. Let $2n = \alpha m + q$, where q is the residual remaining in the division of $2n$ by m; and since $a^{\alpha m} - b^{\alpha m}$ is also divisible by $2n+1$, if we multiply it by a^q, then $a^{\alpha m+q} - a^q b^{\alpha m}$ is divisible by $2n+1$. Then by setting $\alpha m + q$ as $2n$ $a^{\alpha m+q} - b^{\alpha m+q}$ is also divisible by $2n+1$; and if the previous expression is subtracted from it, then the result $a^q b^{\alpha m} - b^{\alpha m+q} = b^{\alpha m}(a^q - b^q)$ is also divisible by $2n+1$.

Hence, since b is not divisible by $2n+1$ by hypothesis, it is necessary that $a^q - b^q$ is divisible by $2n+1$. Furthermore, set $m = \beta q + r$, and since both the formulas $a^{\beta q+r} - b^{\beta q+r}$ and $a^{\beta q} - b^{\beta q}$ are divisible by $2n+1$, multiply the latter by a^r and subtract it from the first. Then the result $b^{\beta q}(a^r - b^r)$ or $a^r - b^r$ is equally divisible by $2n+1$. In a similar manner, it is evident that if $q = \gamma r + s$, then the expression $a^s - b^s$ is also divisible by $2n+1$; and if we examine the values of the variables q, r, s, t, etc. through repeated divisions of the same kind, then it is clear that if we let the greatest common divisor of the numbers m and $2n$ be p, then $a^p - b^p$ is divisible by $2n+1$.

Corollary 1.
35. Therefore if m is a number relatively prime to $2n$, then their greatest common divisor is unity, and for that reason if $a^m - b^m$ is divisible by the prime number $2n+1$, then $a - b$ is also divisible by $2n+1$.

Corollary 2.
36. So if the difference of two numbers $a - b$ is not divisible by $2n+1$, then there is also no number of the form $a^m - b^m$, for m relatively prime to $2n$, that can be divisible by $2n+1$.

Corollary 3.
37. But if m is a prime number, then the form $a^m - b^m$ cannot be divided by the prime number $2n+1$ unless m is also a divisor of $2n$; because $a - b$ is not divisible by $2n+1$.

Corollary 4.
38. Thus if m is a prime number, then the form $a^m - b^m$ has no divisors except for $a - b$, unless they are expressible in the form $mn+1$. For that reason, investigation of the divisors of any number of the form $a^m - b^m$ should be confined to only those prime numbers of the form

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 includantur 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 evoluantur, 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:

$$\begin{aligned}&+a^m \pm ma^{m-1}\alpha p + \tfrac{m(m-1)}{1\cdot 2}a^{m-2}\alpha^2p^2 \pm \text{ etc.}\\ &\pm (b^m \pm mb^{m-1}\beta p - \tfrac{m(m-1)}{1\cdot 2}b^{m-2}\beta^2p^2 \pm \text{etc.})\end{aligned}$$

Unde perspicuum est si a^m-b^m fuerit divisibile, tum quoque haec forma $(a \pm \alpha p)^m - (b \pm \beta p)^m$ 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 $(a \pm \alpha p)^m \pm b^m$, vel haec $a^m \pm (b \pm \beta p)^m$ 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 $A(a \pm \alpha p)^m \pm B(b \pm \beta p)^m$ fore per p divisibilem. Hancque 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 $a^m \pm b^m$ per numerum p, divisibilitas etiam huius formulae $(\alpha p \pm a)^m \pm (\beta p \pm b)^m$ sequitur. Verum haec aliaque similia ex algebrae elementis sponte patent.

$mn+1$.

Corollary 5.
39. So unless the number 2^m-1 is prime, with m being a prime number, it cannot have any divisors other than those expressible in the form $mn+1$.

Corollary 6.
40. Therefore if m is a prime number, the divisors of a^m-b^m, except for $a-b$, and given that a and b are relatively prime, are contained in the series:

$$2m+1;\ 4m+1;\ 6m+1;\ 8m+1;\ 10m+1;\ \text{etc.}$$
if the prime numbers are not discarded from it.

Theorem 10.
41. If the expression $a^m \pm b^m$ has a divisor p, then the expression $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ is also divisible by p.

Proof.
If $(a \pm \alpha p)^m$ and $(b \pm \beta p)^m$ are expanded in the usual method, then all the terms in each series except for the first are divisible by p. That is, the expression $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ changes into this form:

$$\begin{aligned}&+a^m \pm ma^{m-1}\alpha p + \tfrac{m(m-1)}{1\cdot 2}a^{m-2}\alpha^2p^2 \pm \text{ etc.}\\ &\pm (b^m \pm mb^{m-1}\beta p - \tfrac{m(m-1)}{1\cdot 2}b^{m-2}\beta^2p^2 \pm \text{etc.})\end{aligned}$$

From there, it is clear that if a^m-b^m is divisible by p, then the expression $(a \pm \alpha p)^m - (b \pm \beta p)^m$ is also divisible by p. □

Corollary 1.
42. Therefore if $a^m \pm 1$ is divisible by p, then $(a \pm \alpha p)^m \pm 1$ is also divisible by p.

Corollary 2.
43. If $a^m \pm b^m$ is divisible by p, then the expression $(a \pm \alpha p)^m \pm b^m$, or $a^m \pm (b \pm \beta p)^m$, is also divisible by p.

Discussion.
44. In the same manner, it can be proved generally that if $Aa^m \pm Bb^m$ is divisible by p, then $A(a \pm \alpha p)^m \pm B(b \pm \beta p)^m$ is also divisible by p. And this truth holds equally whether p is prime or otherwise. But indeed, there is no need for both powers to be the same exponent m, because even if the exponents were unequal, the conclusion still holds in like manner. And then if m is also an even number in the divisibility of the formula $a^m \pm b^m$ by the number p, then the divisibility of the formula $(\alpha p \pm a)^m \pm (\beta p \pm b)^m$ follows. And other similar facts are evident in the elements of algebra in itself.

Theorema 11.
45. Si fuerit $a = ff \pm (2m+1)\alpha$, 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 $f^{2^m} - 1$, seu haec $(ff)^m - 1$. Hinc per theorema praecedens quoque ista formula $(ff \pm (2m+1)\alpha)^m - 1$ erit divisibilis per $2m+1$. Quare si fuerit $a = ff \pm (2m+1)\alpha$, formula $a^m - 1$ per numerum primum $2m+1$ dividi poterit. Q.E.D.

Corollarium 1.
46. Si ergo fuerit vel $a = (2m+1)\alpha + 1$ vel $a = (2m+1)\alpha + 4$, vel $a = (2m+1)\alpha + 9$; vel $a = (2m+1)\alpha + 16$ vel etc. tum formula $a^m - 1$ semper erit divisibilis per $2m_1$, si quidem $2m+1$ fuerit numerus primus.

Corollarium 2.
46.*** Cum casus, quibus ipse numerus a est divisibilis per $2m+1$ excludantur, manifestum est in formula $ff \pm (2m+1)\alpha$ 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 $(2m+1)k \pm 1$; $(2m+1)k \pm 2$; $(2m+1)k \pm 3$; $\cdots\cdots$ $(2m+1)k \pm m$: 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 unum colligantur, erunt sequentes: $(2m+1)p+1$; $(2m+1)p+4$; $(2m+1)p+q$; $\cdots\cdots$ $(2m+1)p+mm$ quarum numerus est m.

Corollarium 4.
48. Ad valores igitur ipsius a inveniendos, ut $a^m - 1$ per numerum primum $2m+1$ fiat divisibile, investigari oportet residua, quae in divisione cuiusque numeri quadrati per $2m+1$ remanent. Si enim r fuerit huius modi 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 valorum ipsius r maior esse nequit quam m. Dabuntur ergo semper m numeri, qui pro r adhiberi non poterunt.

Corollarium 6.
50. Valores vero ipsius r erunt primo omnes numeri

Theorem 11.
45. If $a = f^2 \pm (2m+1)\alpha$, and $2m+1$ is a prime number, then the expression $a^m - 1$ is divisible by $2m+1$.

Proof.
Since $2m+1$ is a prime number, the formula $f^{2^m} - 1$ or $(f^2)^m - 1$ is divisible by it. Hence by the preceding theorem, the formula $(f^2 \pm 2m+1)\alpha)^m - 1$ is also divisible by $2m+1$. For that reason, if $a = f^2 \pm (2m+1)\alpha$, the formula $a^m - 1$ can be divided by the prime number $2m+1$. □

Corollary 1.
46. Therefore if $a = (2m+1)\alpha + 1$ or $a = (2m+1)\alpha + 4$ or $a = (2m+1)\alpha + 9$ or $a = (2m+1)\alpha + 9$ or $a = (2m+1)\alpha + 16$ or etc., then the formula $a^m - 1$ is always divisible by $2m+1$, provided that $2m+1$ is a prime number.

Corollary 2.
46.*** Since the cases in which the number a itself is divisible by $2m+1$ are excluded, it is clear that the formula $f^2 \pm (2m+1)\alpha$ cannot be divisible by $2m+1$. Hence all numbers which are not divisible by $2m+1$ can be chosen for f.

Corollary 3.
47. Therefore the numbers $(2m+1)k \pm 2$, $(2m+1)k \pm 3, \ldots, (2m+1)k \pm m$ must be chosen for f, because the numbers that are not divisible by $2m+1$ are contained in these expressions. Hence, when all the terms that are divisible by $2m+1$ are collected together, then taking the squares of the number a produces the series: $(2m+1)p+1$, $(2m+1)p+4$, $(2m+1)p+q, \ldots (2m+1)p+mm$, in which there are m terms.

Corollary 4.
48. Therefore, in investigating the values for a for which $a^m - 1$ is divisible by the prime number $2m+1$, one should investigate the residuals that remain after the division by $2m+1$ of each square number. This is because if r is the remainder of this form, then $(2m+1)p + r$ is an appropriate value for a.

Corollary 5.
49. Moreover, all these remainders r are less than $2m+1$, but on the other hand not all numbers less than $2m+1$ are values for r; because the number of values for r cannot be larger than m. Therefore, these are all the values for m that cannot be applied for r.

Corollary 6.
50. Indeed, the values for r are first of all the squares

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 lucelentius 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 $a^{2^m} - 1$ 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 sit $aa-1$ 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 vel† $a = 5p+3$ neutro casu formula $aa-1$ per 5 erit divisibilis.

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 $a^3 - 1$ fiat per* 11 *divisibilis.*

Numeri quadrati per 11 divisi dabunt 5 diversa residua quae sunt: 1, 3, 4, 5, 9. Hinc formula $a^3 - 1$ 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 $a^3 + 1$ 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.

less than $2m+1$, but then also the residuals that remain after the division of greater squares by $2m+1$, and moreover no number among all the different values for r can be greater than the number m.

Discussion.

51. To make the usefulness of this theorem clearer, and to illustrate it by numerical examples, the following problems are presented next, by which not only the truth of the theorem may be more clearly understood, but also by which in turn it will be clear that for as many numbers a that have no value assigned, so many numbers of the form $a^m - 1$ are not divisible by $2m+1$. And so since the formula $a^{2^m} - 1$ is always divisible by $2m+1$, for as many values of $a^m - 1$ that are not divisible by $2m+1$, so many values of $a^m + 1$ are able to be divisible by $2m+1$.

Example 1.

52. *Finding the values of a so that $a^2 - 1$ is divisible by* 5.

The residuals that remain after the division of a square by five is one or four; and so it is necessary either that $a = 5p+1$ or $a = 5p+4$, or that $a = 5p+1$. In the first case $a^2 - 1$ or $(a-1)(a+1) = 5p(5p+2)$, and in the latter case it equals $(5p-2)5p$; and so in both cases divisible by 5. But on the other hand, if either $a = 5p+2$ or $a = 5p+3$, then in no case is the formula $a^2 - 1$ divisible by 5.

Example 2.

53. *Finding the values of a so that the form $a^3 - 1$ is divisible by* 7.

The three residuals that remain after the division of any square by 7 are 1, 2 and 4. Hence the values for a are $7p+1$, $7p+2$ and $7p+4$. But on the other hand, if $a = 7p+3$ or $7p+5$ or $7p+6$, then $a^3 + 1$ rather than $a^3 - 1$ is divisible by 7.

Example 3.

54. *Finding the values of a so that the form $a^3 - 1$ is divisible by* 11.

The square numbers that are divisible by 11 have five different residuals: 1, 3 4, 5, 9. Hence, $a^3 - 1$ is divisible by 11 if $a = 11p + r$, where r is any of the numbers 1, 3 4, 5, or 9. However, if a is set to any of the numbers 2, 6, 7, 8, 10, and multiplied by 11, then $a^3 + 1$ is divisible by 11.

Theorem 12.

55. If $a = f^3 \pm (3m+1)\alpha$, with $3m+1$ a prime number, then $a^m - 1$ is divisible by $3m+1$.

Demonstratio.

Ob $3m + 1$ numerum primum erit $f^{3m} - 1$ divisibile per $3m + 1$. At est $f^{3m} - 1 = (f^3)^m - 1$, unde quoque haec formula $(f^3 \pm (3m+1)\alpha)^m - 1$ erit divisibilis per $3m + 1$. Quare si sumatur $a = f^3 \pm (3m+1)\alpha$, 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 $3m + 1$ qucunque 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.
$3m+1;$	$7, 13, 19, 31, 37, 43, 61, 67, 63, 79, 97,$ 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 $(3m+1-f)^3$ dabit residuum $-r$ seu $3m+1-r$.

Scholion.

59. Notatu hic dignum est numerus 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

Proof.

Since $3m + 1$ is a prime number, $f^{3m} - 1$ is divisible by $3m + 1$. And $f^{3m} - 1 = (f^3)^m - 1$, and so $(f^3 \pm (3m+1)\alpha)^m - 1$ is also divisible by $3m+1$. Therefore if we set $a = f^3 \pm (3m+1)\alpha$, then $a^m - 1$ is divisible by $3m + 1$. □

Corollary 1.

56. To discover the values for a, every residual which arises from the division of the cubes by $3m + 1$, ought to be considered. Thus, every one of these residuals, when increased by a certain multiple of $3m + 1$, gives a suitable value for a.

Corollary 2.

57. Since $3m + 1$ ought to be a prime number, it is necessary that m be even, and hence the prime number $3m + 1$ is greater than unity by a multiple of six.

Hence the applicable numbers for m and $3m+1$ are the following:

m	$2,\ 4,\ 6,\ 10, 12, 14, 20, 22, 24, 26, 32$ etc.
$3m+1;$	$7, 13, 19, 31, 37, 43, 61, 67, 63, 79, 97,$ etc.

Corollary 3.

58. Thus if cubes are divided by prime numbers of the form $3m + 1$, the following residuals remain:

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 these remainders first occur all cubes smaller than their divisors, and then, if we have some remainder of r for a divisor of the form $3m + 1$, then each other remainder equal to $3m + 1 - r$ is also given. But then if the cube f^3 gives a remainder of r, then the cube $(3m + 1 - f)^3$ gives a remainder of $-r$, or $3m + 1 - r$.

Discussion.

59. It is worth nothing here that the number of remainders is always equal to m, if the divisor is equal to $3m + 1$. Thus there are always three cubes, whose radixes are less than $3m + 1$, from which the same remainder results. Namely, the three cubes are 1^3, 2^3 and

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 $a^{2^m} + a^m + 1$ divisionem admittet.

Theorema 13.
60. Si fuerit $a = f^n \pm (mn + 1)\alpha$ 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 $f^{mn} - 1 = (f^n)^m - 1$, unde quoque haec forma $(f^n \pm (mn + 1)\alpha)^m - 1$ erit divisibilis per $mn + 1$. Quare si ponatur $a = f^n \pm (mn + 1)\alpha$, 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 forma $f^n \pm (mn + 1)\alpha$ contineatur; seu toties dabitur potestas f^n quae per $mn + 1$ divisa relinquat a pro residuo. Ita cum observassem formula $2^{64} - 1$ 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 proposi-

4^3 give the same remainder of 1 when divided by 7, and the three cubes 2^3, 5^3 and 6^3 give the same remainder of 8 when divided by 13.

Moreover, it is proper to note that if values for a other than those assigned are taken, then $a^m - 1$ is not be divisible by $3m + 1$. And even though this can easily be perceived to be true, its proof nevertheless does not follow from the preceding, and this truth is the kind that, while we know it to be true, it is however not proper to prove here. So in these cases, in which $a^m - 1$ is not divisible by $3m + 1$, this form $a^{2m} + a^m + 1$ admits division.

Theorem 13.
60. If $a = f^n \pm (mn + 1)\alpha$, with $mn + 1$ being a prime number, then $a^m - 1$ is divisible by $mn + 1$.

Proof.
Since $mn + 1$ is a prime number, $f^{mn} - 1$ is divisible by $mn + 1$. And $f^{mn} - 1 = (f^n)^m - 1$, and so $(f^n \pm (mn + 1)\alpha)^m - 1$ is also divisible by $mn + 1$. And for this reason, if we set $a = f^n \pm (mn + 1)\alpha$, then $a^m - 1$ can be divided by $mn + 1$. □

Corollary 1.
61. Therefore if the powers of the exponent n are divided by a prime number $mn + 1$, the single remainders, either themselves or increased by a certain multiple fo $mn + 1$, present suitable values for a, so that $a^m - 1$ is divisible by $mn + 1$.

Corollary 2.
62. Hence if $a^m - 1$ is not divisible by $mn + 1$, then the value of a is not contained in the expression $f^n \pm (mn + 1)\alpha$, or rather, or rather, there is no power of the exponent n which leaves a when divided by $mn + 1$.

Discussion.
63. The converse of this proposition, if it is examined in every manner, should also be perceived true; and so as often as $a^m - 1$ is divisible by $mn + 1$, so often is the value of a itself contained in the form $f^n \pm (mn + 1)\alpha$; or rather, so often is there a power of f^n which leaves a as remainder when divided by $mn + 1$. Thus, since I observed that $2^{64} - 1$ is divisible by 641, since $m = 64$ let $n = 10$, there is also a tenth power which leaves a remainder of 2 when divided by 641. And in fact the power of this kind can be seen to be 96^{10}. But on that account, since $2^{32} - 1$ is not divisible by 641, in this case let $m = 32$ and $n = 20$; and so there is no power of 20 that leaves a remainder of 2 when divided by 641.

The truth of this last assertion has been shown rigorously, but a proof of the converse propositions is still tionum 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 $g^{mn}(a^m - 1)$ 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 superioris 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 formula $f^n - a$, 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 $g^{mn}(a^m - b^m)$ seu $a^m - b^m$ per $mn + 1$ erit divisibile. Q.E.D.

needed: namely, if $a^m - 1$ is divisible by a prime number $mn + 1$, then a is also always expressible as a number of the form $f^n \pm (mn + 1)\alpha$. And also, if a is not contained in the form $f^n \pm (mn + 1)\alpha$, then $a^m - 1$ also does not admit division by $mn + 1$. For this reason, if either of the propositions can be proven, then the truth of the other is at the same time clear. Moreover, a theorem here can be proven to the effect that, whenever $f^n - a$ is divisible by $mn + 1$, then $a^m - 1$ is also divisible by $mn + 1$. In this, the following more general theorem is evident.

Theorem 14.
64. If $f^n - ag^n$ is divisible by a prime number $mn + 1$, then $a^m - 1$ is also divisible by $mn + 1$.

Proof.
Since the formula $f^n - ag^n$ is set to be divisible by $mn + 1$, the formula $f^{mn} - a^m g^{mn}$, which can be divided by it, is certainly divisible by $mn + 1$. And since $mn + 1$ is a prime number, $f^{mn} - g^{mn}$ is divisible by it; and hence the difference $g^{mn}(a^m - 1)$ or rather, the formula $a^m - 1$ itself, is divisible by $mn + 1$, and accordingly, g cannot admit division by $mn + 1$, unless f is divisible at the same time, but this case is excluded in our reasoning. □

Corollary 1.
65. Therefore if $a^m - 1$ is not divisible by $mn + 1$, then there are also no numbers f and g so that $f^n - ag^n$ is divisible by $mn + 1$.

Corollary 2.
66. If the converse of the above proposition could be proven, then it would also be clear that whenever $f^n - a$ cannot be divided by $mn + 1$, then certainly $f^n - ag^n$ cannot admit division by $mn + 1$, and also at the same time it would be clear that if $f^n - ag^n$ is divisible by $mn + 1$, then there is also a formula $f^n - a$, which is divisible by $mn + 1$.

Theorem 15.
67. If the formula $af^n - bg^n$ is divisible b y a prime number $mn + 1$, then $a^m - b^m$ is also divisible by $mn + 1$.

Proof.
If $af^n - bg^n$ is divisible by $mn + 1$, the the formula $a^m f^m mn - b^m g^{mn}$ is also divisible by $mn + 1$. And since $mn + 1$ is a prime number, the formula $f^{mn} - g^{mn}$ is also prime, and for that reason $a^m f^m mn - a^m g^{mn}$ is also divisible by $mn + 1$. Then subtracting it from $a^m f^{mn} - b^m g^{mn}$ and the remainder $g^{mn}(a^m - b^m)$ or $a^m - b^m$ is divisible by $mn + 1$. □

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 $af^n - bg^n$ 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 ν exhiberi possunt, ut sit $\mu n \pm 1 = \nu m$. Namque si inter numeros m et n ea operatio instituatur, quae pro maximo communi divisiore institui solet, atque quoti notentur, ex iisque fractiones ad $\frac{m}{n}$ approprinquantes quaerantur, ultima erit $\frac{m}{n}$, et si penultima fuerit $\frac{\mu}{\nu}$ erit $\mu n \pm 1 = \nu m$. 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 $\mu n + 1 = \nu m$, habebitur $a^{\nu m} - b^{\nu m}$, 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 $\mu n - 1 = \nu m$, tum sumatur $f = b^\mu$ et $g = a^\mu$ fietque $af^n - bg^n = ab^{\mu n} - ba^{\mu n} = ab(b^{\mu n-1} - a^{\mu n-1}) = -ab(a^{\nu m} - b^{\nu m})$ 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. I. 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

Corollary 1.
68. Thus if $a^m - b^m$ is not divisible by $mn + 1$, then there are no numbers substitutable for f and g, so that $af^n - bg^n$ is divisible by $mn + 1$.

Corollary 2.
69. The converse of this proposition, that if $a^m - b^m$ is divisible by $mn + 1$, then at the same time there are numbers f and g, so that $af^n - bg^n$ becomes divisible by $mn + 1$, and whenever it is examined, it will be understood to be true. Meanwhile, however, a proof of this is still to now wanting.

Discussion.
70. A special case of the inverse proposition can be proven, in which the numbers m and n are relatively prime: because in this case certain numbers μ and ν can be found, so that $\mu n \pm 1 = \nu m$. This is because if that relationship between the numbers m and n is applied, which is usually called the greatest common divisor, and then those numbers are taken, and from those fractions equal to $\frac{m}{n}$ are sought, so that the last is $\frac{m}{n}$, and if the one before that is $\frac{\mu}{\nu}$, then $\mu n \pm 1 = \nu m$. So by this previous lemma the proof of the converse proposition, where m and n are relatively prime numbers, follows.

Theorem 16.
71. If m and n are relatively prime numbers, and the formula $a^m - b^m$ is divisible by the number $mn + 1$, then there is a formula $af^n - bg^n$ divisible by $mn + 1$.

Proof.
Let $f = a^\mu$ and $g = b^\mu$, and the formula $af^n - bg^n$ to become $a^{\mu n+1} - b^{\mu n+1}$, whereby if μ is taken so that $\mu n + 1 = \nu m$, then we have ${}^{\nu m} - b^{\nu m}$. And since this is divisible by $a^m - b^m$, then $mn + 1$ is also divisible by $mn + 1$, and thus this is the case, where $af^n - bg^n$ is divisible by $mn + 1$. However, if $\mu n - 1 = \nu m$, then taking $f = b^\mu$ and $g = a^\mu$, it follows that $af^n - bg^n = ab^{\mu n} - ba^{\mu n} = ab(b^{\mu n-1} - a^{\mu n-1}) = -ab(a^{\nu m} - b^{\nu m})$ on that account is divisible by $mn + 1$. □

Corollary 1.
72. Therefore if m and n are relatively prime numbers, and $mn+1$ is a prime number, then the following propositions are proven. I. If $af^n - bg^n$ is divisible by $mn+1$, then $a^m - b^m$ is also divisible by $mn+1$, and if the formula is not diviisble by $mn+1$ in any way, then this is also not divisible. II. If $a^m - b^m$ is divisible by $mn + 1$, then there is a number of the form $af^n - bg^n$ divisible by $mn + 1$, and if $a^m - b^m$ does not admit division, then there is no number of the form $af^n - bg^n$

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 formula huiusmodi $af^n - bg^n$ divisibilem per $mp+1$.

divisible by $mn+1$.

Corollary 2.
73. If m is an even number, then b can equally be taken as either negative or positive, and so in this case if $a^m - b^m$ is divisible by $mn+1$, then the formula $af^n + bg^n$ can also be considered divisible by $mn+1$; and so it is clear that because n is an even number, for that reason the power of g^n can be taken to be negative.

Corollary 3.
74. In a similar manner, it can be proven that if m and n are relatively prime numbers as above, and if $a^m - b^m$ is divisible by $mp+1$, then the formula $af^n - bg^n$ can also be shown to be divisible by $mp+1$.