CONCERNING CERTAIN OUTSTANDING PROPERTIES ARISING FROM THE DIVISORS OF POWERS

E 557

Opuscula Analytica 1, 1783, p. 242-295

[Presented to the St. Petersburg Academy on the 25th of January 1773]

l. It is agreed all geometric progressions, such as 1, a, a^2, a^3, a^4 etc., to be prepared thus, so that, provided the individual terms are divided by some number N, which shall be prime to a, the remainders after a certain interval revert again to the same order ; and since the first remainder is unity, a power of this kind a^n always will be given, which divided by N may again leave the remainder unity ; truly the following powers a^{n+1}, a^{n+2}, a^{n+3} etc. will produce the same remainders, which have arisen from the terms a, a^2, a^3 etc. Then it is required to demonstrate also, if N were a prime number, then again the power a^{N-1} always shows unity for the remainder. But most often that power a^{N-1} is the smallest, which leaves unity on division by N ; truly meanwhile also it happens usually, that a smaller power a^n presents the same; but then n is equal always to some part of the power $N-1$; and hence the question arising is worthy of our attention:

What shall be the minimum power a^n , for any divisor N you please, from which the remainder $=1$ may arise ?

And this question can be proposed otherwise extended more widely :

What shall be the lowest power a^n, which divided by the given number N , shall leave the remainder r?

Which question is reduced to this, so that the minimum formula may be shown $a^x - r$, which would be divisible by the given number N. Indeed at this point also the more general question can be proposed, so that

the exponent x may be investigated, by which this formula $fa^x + g$ may be returned divisible by the given number N.

2. In the first place, the solution of this problem is required to be investigated for perfect numbers. For since the form of these numbers shall be $2^{n-1}(2^n - 1)$, whenever $2^n - 1$ shall be a prime number, it is evident at once this cannot happen, unless the

exponent *n* itself were a prime number ; since a form of this kind $2^{\alpha\beta}-1$ always has the divisors $2^{\alpha}-1$ and $2^{\beta}-1$. Truly nor does it follow in turn, that if n were a prime number, then also the formula 2^n-1 may become a prime number. Indeed many cases have been investigated now, for which this does not happen; such as if there were $n=11,\ n=23;$ likewise $n=29,\ n=37$; and besides without doubt for more cases, which all have not yet been able to be examined. But other ways for investigating these cases was not apparent besides that, which I have used formerly, which themselves were had thus: A divisor of the formula 2^n-1 may be devised, if that has to be a prime number of the form $2p+1$; and since the formula $2^{2p}-1$ always may have a divisor $2p+1$, it follows this cannot happen, unless *n* were some part of $2p,$ or $2p$ a multiple of n itself. Therefore on taking $p=\lambda n,$ the divisor will become $2\lambda n+1$; from which it is concluded, if the formula 2^n-1 shall not be a prime number, that certainly cannot have other divisors, other than those which may be expressed in the form $2\lambda n+1$; and I have used this principle formerly in the investigation of prime numbers. Since at one time in a similar manner I had examined the assertion of Fermat, by which he asserted, the formula 2^n+1 always to be a prime number, whenever the exponent *n* were itself a power of two, I have brought in the question mentioned above as an aid, from which after several calculations I found at last the formula $2^{32}+1$ to have the divisor 641; from which now the question can be formed: what shall be the smallest powers of two, which increased by one may be divisible by 641 ? Indeed the method, which I used formerly, proceeded by a most tedious calculation; but now another much simpler method has presented itself to me, and to be more expedite not only for those cases mentioned concerning the resolution of powers of two, but also could be applied to that most general question, from which evidently the smallest power a^x is sought, so that the formula fa^x+g may become divisible by a given number N. Therefore I am going to set out this new method briefly here ; moreover to this end the following lemmas are required to established:

LEMMA 1

3. If some number *A* divided by another number *N* may leave the remainder *r,* then all these numbers also : $r\mp N,\ r\mp 2N,\ r\mp 3N$ and in general $r\mp\lambda N$,can be regarded equally as remainders, since these formulas themselves divided by *N* leave behind the remainder *r*.

LEMMA 2

4. If the number *A* divided by the number *N* may leave the remainder *a,* truly the number *B* divided by the same, the remainder *b,* then the product *AB* divided by *N* will leave the remainder *ab.* Therefore hence the powers $A^2,\ A^3,\ A^4$ etc. will give the remainders $a^2,\ a^3, a^4$ etc., which as it pleases, on division by *N*, may be allowed to be reduced to the smallest values.

LEMMA 3

5. If the power a^x by the divisor N may give the remainder $= r$, truly the power a^y the remainder $= s$, then the power a^{x+y} will give the remainder $= rs$; from which also these powers a^{2x}, a^{3x}, a^{4x} etc. will produce the remainders r^2, r^3, r^4 etc.

LEMMA 4

6. If as before, the power a^x may present the remainder r for the divisor N, truly the power a^y the remainder s, hence also it will be able to assign the remainder corresponding to the power a^{x-y}, which indeed may become $= \frac{r}{s}$, if r may be divided by s. But because in place of r it will be allowed to suppose $r \mp \lambda N$, λ will always be able to be defined thus, so that this form $r \mp \lambda N$ may be able to be divided by s, and then the quotient will give the remainder of the corresponding power a^{x-y}.

LEMMA 5

7. If the power a^x may leave r for the divisor N, and there may become $r \mp \lambda N = a^\alpha s$, thus so that $a^\alpha s$ may be able to be considered as the remainder, then the power $a^{x-\alpha}$ will leave the remainder s, since the dividend and the remainder will be permitted always to be made smaller by the common divisor.

GENERAL PROBLEM

8. *With the formula $fa^x + g$ proposed, to find the minimum exponent x, by which this formula may be divided by the given number N, if indeed that were possible.*

SOLUTION

Therefore the question is reduced to this, so that the form fa^x divided by the given number N may leave the remainder $= -g$. Now since by the first lemma $-g \mp \lambda N$ also may be had for the remainder, thus it will be easy to be able to assume λ, so that this formula may contain the factor a, or thus its higher power a^α. Therefore there shall be $-g \mp \lambda N = a^\alpha r$, and by the last lemma the quantity $fa^{x-\alpha}$ divided by N will leave the remainder $= r$. Now in a similar manner there may become $r \mp \lambda N = a^\beta s$, and the quantity $fa^{x-\alpha-\beta}$ will give the remainder s, and thus it will be allowed to progress further, by assuming $s \mp \lambda N = a^\gamma t$; then truly also $t \mp \lambda N = a^\delta u$; again, $u \mp \lambda N = a^\varepsilon v$ etc. ; with which being agreed, the quantity $a^{x-\alpha-\beta-\gamma-\varepsilon}$ divided by N will

leave the remainder $= v$; and these operations may be continued to that point, while it may arrive at the remainder $= f$; thus so that this quantity $fa^{x-\alpha-\beta-\gamma-\text{etc.}}$ may give the remainder $= f$; which always happens, if indeed the question were possible ; and thus with this being subtracted from the previous exponent of the number , $\alpha+\beta+\gamma+\delta+\varepsilon+\text{etc.}$ will surpass the number $N-1$, since if the exponents of *a* itself may be continued beyond this limit, the same remainders will recur. But if such a case may have arisen, where the remainder is f, since this happens, if the exponent of *a* itself were $= 0$, hence we will conclude $x = \alpha+\beta+\gamma+\delta+\text{etc.}$ Therefore it will be an aid for all these operations to be represented succinctly:

$$\begin{aligned} -g \mp \lambda N &= a^{\alpha} r \\ r \mp \lambda N &= a^{\beta} s \\ s \mp \lambda N &= a^{\gamma} t \\ t \mp \lambda N &= a^{\delta} u \\ &\cdots\cdots\cdots \\ z \mp \lambda N &= a^{\zeta} f \end{aligned}$$

and hence the conclusion is deduced $x = \alpha+\beta+\gamma+\delta+\cdots+\zeta$. But if at no time may such a remainder f be arrived at, before the sum $x = \alpha+\beta+\gamma+\delta+\cdots$ may rise as far as $N-1$, then the problem is considered to be impossible.

Though these operations may readily be put in place, yet these very often will be easily allowed to be contracted, especially if a small remainder such as *t* has arisen, corresponding to the formula $fa^{x-\delta}$, by putting $\delta = \alpha+\beta+\gamma$; then indeed its square t^2 will correspond to the formula $f^2a^{2x-2\delta}$, which may be divided by the first, so that the formula $fa^{x-2\delta}$ may correspond to the remainder $\frac{t^2}{-g}$, which if it were not an integer, by writing $t^2 \mp \lambda N$ in place of t^2 it is reduced readily to that. Indeed also the cube of the remainder t^3 will correspond to the formula $f^3a^{3x-3\delta}$, which divided by the square of the first will give the remainder $= \frac{t^3}{g^2}$ of the formula $fa^{x-3\delta}$. Indeed also two different formulas g will be allowed to multiply each other in turn, and on dividing by the first again it may come to a new formula of this kind. But this compendium especially will establish the maximum use, where it will have arisen for small enough remainders ; greater powers of which also are taken easily, and in addition the smallest remainder $-g$ were a small enough number or unity at this point.

COROLLARY

9. Because we have described these operations clearly, we may apply these to more special cases. And indeed in the first place the formula $2^x \mp 1$ occurs. Therefore we may seek the exponent x for the various divisors, so that the power 2^x may leave the remainder ∓ 1. But it will suffice for this remainder $+1$ to be put in place ; indeed if 2^x were the smallest power giving the remainder $= +1$, then the power $2^{\frac{1}{2}x}$ by necessity will give the remainder $= -1$, if indeed x were an even number; but if x were odd, this case plainly is impossible.

EXAMPLE 1

10. The smallest power 2^x may be sought, which divided by 23 may leave 1, or so that $2^x - 1$ may become divisible by 23. Therefore here [from $fa^x + g$] there is $N = 23,\ a = 2$ and the first remainder $= 1$; from which our operations may proceed in the following manner :

$$+1 + 23 = +24 = +\ 2^3 \cdot 3; \left[-g \mp \lambda N = a^\alpha r \right]$$
$$+3 - 23 = -20 = -2^2 \cdot 5; \left[r \mp \lambda N = a^\beta s \right]$$
$$-5 - 23 = -28 = -2^2 \cdot 7; \left[s \mp \lambda N = a^\gamma t \right]$$
$$-7 + 23 = +16 = +\ 2^4 \cdot 1; \left[z \mp \lambda N = a^\zeta f \right]$$
$$\left[x = \alpha + \beta + \gamma + \zeta . \right]$$

Thus now the chosen remainder $+1$ has been arrived at , on account of $f = 1$; and thus we may conclude $x = 11$. Therefore since the formula $2^{11} - 1$ shall be divisible by 23 and 11 is an odd number, clearly no formula $2^x + 1$ is given divisible by 23.

EXAMPLE 2

11. The divisor 41 may be proposed, by which the formula $2^x - 1$ must be rendered divisible. Therefore on account of $\mathrm{N} = 41,\ a = 2,\ f = 1$ and the first remainder $= 1$, we will have :

$$+1-41=-40=-2^3\cdot 5$$
$$-5+41=+36=+\,2^2\cdot 9$$
$$+9-41=-32=-2^5\cdot 1.$$

Now we are able to stop here; since indeed the power 2^{x-10} leaves the remainder -1, the square of which 2^{2x-20} will leave $+1$, and by dividing into the first form 2^{x-20}, $+1$ will produce for the chosen remainder ; and thus we have $x=20$. But likewise hence it is apparent for the power 2^{10} to bring the remainder -1, thus so that the most simple formulas divisible by 41 shall be $2^{10}+1$ and $2^{20}-1$.

EXAMPLE 3

12. For the divisor 73 the most simple formula $2^x \mp 1$ is sought divisible by that. Here there is $N=73,\ a=2$ and on taking the first divisor $=+1$ becomes

$$+1-73=-72=-2^3\cdot 9$$
$$-9+73=+64=+2^6\cdot 1,$$

where now it will be allowed to stop, and there will be $x=9$, from which the formula 2^9-1 is divisible by 73 ; and because 9 is an odd number, clearly no formula 2^x+1 is given divisible by the same number *N*.

EXAMPLE 4

13. The divisor may be proposed $N=77$, and with the first remainder taken $=1$, the calculation will give:

$$\begin{aligned}
+\ 1-77 &= -\ 76 = -2^2\cdot 19\\
-19-77 &= -\ 96 = -2^5\cdot\ 3\\
-\ 3-77 &= -\ 80 = -2^4\cdot 5\\
-\ 5+77 &= +\ 72 = +2^3\cdot 9\\
+\ 9-77 &= -\ 68 = -2^2\cdot 17\\
-17+77 &= +\ 60 = +2^2\cdot 15\\
+15+77 &= +\ 92 = +2^2\cdot 23\\
+23+77 &= +100 = +2^2\cdot 25\\
+25-77 &= -\ 52 = -2^2\cdot 13\\
-13+77 &= +\ 64 = +2^6\cdot\ 1,
\end{aligned}$$

from which $x=30$; thus so that $2^{30}-1$ shall be the simplest form divisible by 77. Hence yet it does not follow $2^{15}+1$ itself to be divisible by 77, therefore as 77 is not a prime number; and indeed if $2^{30}-1$ is divisible by 77, by no means does it follow either its factor $2^{15}+1$ or $2^{15}-1$ must be divisible, just as it would be allowed to conclude accordingly, if the divisor were a prime number ; indeed in this case it can happen, so that either it shall be divisible by the factor 7, or truly by the other factor 11; and actually, since 2^5+1 shall be divisible by 11, also $2^{15}+1$ will be divisible by 11; but truly the other formula $2^{15}-1$ is divisible by 7, since it has the factor $2^3-1=7$.

EXAMPLE 5

14. The divisor shall be $N=89$, and again by taking the first remainder $=1$, we will make:

$$\begin{aligned}
+\ 1-89 &= -\ 88 = -2^3\cdot 11\\
-11-89 &= -100 = -2^2\cdot 25\\
-25+89 &= +\ 64 = +2^6\cdot 1.
\end{aligned}$$

Hence therefore $x=11$, and thus the formula $2^{11}-1$ has the divisor 89; but no formula of the other kind $2^{11}+1$ may be given.

EXAMPLE 6

15. The divisor shall be $N = 105$, and there will be :

$$+\ 1 - 105 = -104 = -\ 2^3 \cdot 13$$
$$-13 + 105 = +\ 92 = +\ 2^2 \cdot 23$$
$$+23 + 105 = +128 = +\ 2^7 \cdot 1.$$

The sum of the exponents $= 12$; therefore $x = 12$, and the formula $2^{12} - 1$ will be divisible by 105. But since 105 is not a prime number, it does not follow $2^6 + 1$ to become divisible by 105. Indeed it can be divided only by 5, while the other formula $2^6 - 1$ is divisible by $3 \cdot 7$.

EXAMPLE 7

16. There shall be $N = 223$ and the first remainder $= 1$, there will become :

	Sum of the exponents
$+\ 1 + 223 = +224 = +2^5 \cdot\ 7$	5
$+\ 7 - 223 = -216 = -2^3 \cdot 27$	8
$-27 + 223 = +196 = +2^2 \cdot 49$	10
$+49 + 223 = +272 = +2^4 \cdot 17$	14
$+17 + 223 = +240 = +2^4 \cdot 15$	18
$+15 - 223 = -208 = -2^4 \cdot 13$	22
$-13 - 223 = -236 = -2^2 \cdot 59$	24
$-59 + 223 = +164 = +2^2 \cdot 41$	26
$+41 + 223 = +264 = +2^3 \cdot 33$	29
$+33 + 223 = +256 = +\ 2^8 \cdot 1$	37

The sum of the exponents $= 37$, therefore $x = 37$, and the formula $2^{37} - 1$ is divisible by 223. Hence since 37 is an odd number, it is certain no formulas $2^x + 1$to be given divisible by 223.

17. So that now it may be apparent, how these operations may be able to be supported, we may stop now at the fifth [in the above table § 16], where the remainder 15 appears and the sum of the exponents $= 18$; from which this power 2^{x-18} gives the remainder 15. The square may be taken, and the power 2^{2x-36} gives the remainder 225 or 2; this now

divided by the prime produces the remainder $2 = 2^1 \cdot 1$ for the power 2^{x-18}, therefore the power 2^{x-37} produces the remainder 1, from which there is now apparent to be $x = 37$.

EXAMPLE 8

18. Let $N = 641$ and the first remainder $= 1$, there will become :

	Sum of the exponents
$+1-641=-640 = -2^7 \cdot 5$	7
$-5+641=+636 = +2^2 \cdot 159$	9
$+159+641=+800=+2^5 \cdot 25$	14
$+25-641=-616=-2^3 \cdot 77$	17
$-77+641=+564=+2^2 \cdot 141$	19
$+141-641=-500=-2^2 \cdot 125$	21
$-125+641=+516=+2^2 \cdot 129$	23
$+129-641=-512=-2^9 \cdot 1$	32

where now we can stop. Because indeed the remainder is -1, if we might have taken -1 for the first remainder, so that the formula will be sought $2^x + 1$ divisible by 641, all the following remainders shall be produced with the opposite sign in place and the final remainder may become $+1$; from which we may conclude correctly to be $x = 32$, thus so that the formula $2^{32} + 1$ shall be divisible by 641. Moreover it is evident for the smallest formula of this form $2^x - 1$ to become $x = 64$.

19. But it may be possible to condense this labour greatly. For immediately after the first operation we may stop, which presents the remainder -5 for the power 2^{x-7}. At once we may put in place the fourth power, and for 2^{4x-28} we will have the remainder 625, or $-16 = -2^4 \cdot 1$, thus so that 2^{4x-32} may agree with the remainder -1. Therefore by dividing by the cube of the first, or 2^{3x}, of which the remainder likewise is 1, also the remainder of its power 2^{x-32} will be -1, which we have elicited by roundabout ways.

EXAMPLE 9

20. There shall be $N = 385 = 5 \cdot 7 \cdot 11$ and the first remainder $= 1$, there will be :

		Sum of the powers
+	$1 - 385 = -384 = -2^7 \cdot 3$	7
−	$3 - 385 = -388 = -2^2 \cdot 97$	9
−	$97 + 385 = +288 = +2^5 \cdot 9$	14
+	$9 - 385 = -376 = -2^3 \cdot 47$	17
−	$47 - 385 = -432 = -2^4 \cdot 27$	21
−	$27 - 385 = -412 = -2^2 \cdot 103$	23
−	$103 - 385 = -488 = -2^3 \cdot 61$	26
−	$61 + 385 = +324 = +2^2 \cdot 81$	28
+	$81 - 385 = -304 = -2^4 \cdot 19$	32
−	$19 - 385 = -404 = -2^2 \cdot 101$	34
−	$101 + 385 = +284 = +2^2 \cdot 71$	36
+	$71 + 385 = +456 = +2^3 \cdot 57$	39
+	$57 - 385 = -328 = -2^3 \cdot 41$	42
−	$41 + 385 = +344 = +2^3 \cdot 43$	45
+	$43 + 385 = +428 = +2^2 \cdot 107$	47
+	$107 + 385 = +492 = +2^2 \cdot 123$	49
+	$123 + 385 = +508 = +2^2 \cdot 127$	51
+	$127 + 385 = +512 = +2^9 \cdot 1$	60

therefore $x = 60$, thus so that the formula $2^{60} - 1$ shall be divisible by 385, which thence also may be able to be concluded, because the factors of our divisor are 5, 7, 11, of which the first 5 is a divisor of the formula $2^2 + 1$, the second 7 is a divisor of the formula $2^3 - 1$, the third 11 is divisor of the formula $2^5 + 1$; but the formula cannot be given simpler than $2^{60} - 1$, by these three divisors.

21. We may see now, how these operations may be able to be contracted. The third operation produces the power 2^{x-14} , the remainder giving 9 ; from which its square 2^{2x-28} provides the remainder 81 ; but the cube 2^{3x-42} provides the remainder 729, either 344, or -41 ; hence the fourth power 2^{4x-60} will give the remainder -369, or

$+16 = 2^4 \cdot 1$, therefore on dividing by 2^4 the power 2^{4x-60} will give the remainder $+1$ and on dividing by 2^{3x}, of which the remainder also is $+1$, the power 2^{x-60} will give the remainder $+1$, just as we have found.

EXAMPLE 10

Let $N = 311$, and there will become:

	Sum of the exponents
$+\ \ 1+311=+312=+2^3\cdot 39$	3
$+\ 39-311=-272=-2^4\cdot 17$	7
$-\ 17-311=-328=-2^3\cdot 41$	10
$-\ 41-311=-352=-2^5\cdot 11$	15
$-\ 11+311=+300=+2^2\cdot 75$	17
$+\ 75-311=-236=-2^2\cdot 59$	19
$-\ 59+311=+252=+\ 2^2\cdot 63$	21
$+\ 63-311=-\ 248=-2^3\cdot 31$	24
$-\ 31+311=+280=+2^3\cdot 35$	27
$+\ 35-311=-276=-2^2\cdot 69$	29
$-\ 69-311=-380=-2^2\cdot 95$	31
$-\ 95+311=+216=+2^3\cdot 27$	34
$+\ 27-311=-284=-2^2\cdot 71$	36
$-\ 71+311=+240=+2^4\cdot 15$	40
$+\ 15-311=-296=-2^3\cdot 37$	43
$-\ 37-311=-348=-2^2\cdot 87$	45
$-\ 87+311=+224=+2^5\cdot\ 7$	50
$+\ \ 7-311=-304=-2^4\cdot 19$	54
$-\ 19+311=+292=+2^2\cdot 73$	56
$+\ 73+311=+384=+2^7\cdot\ \ 3$	63
$+\ \ 3-311=-308=-2^2\cdot 77$	65
$-\ 77-311=-388=-2^2\cdot 97$	67
$-\ 97-311=-408=-2^3\cdot 51$	70
$-\ 51+311=+260=+2^2\cdot 65$	72
$+\ 65+311=+376=+2^3\cdot 47$	75
$+\ 47-311=-264=-2^3\cdot 33$	78
$-\ 33-311=-344=-2^3\cdot 43$	81
$-\ 43+311=+268=+2^2\cdot 67$	83
$+\ 67-311=-244=-2^2\cdot 61$	85

$$\begin{aligned}
-61-311 &= -372 = -2^2\cdot 93 && 87\\
-93-311 &= -404 = -2^2\cdot 101 && 89\\
-101-311 &= -412 = -2^2\cdot 103 && 91\\
-103+311 &= +208 = +2^4\cdot 13 && 95\\
+13+311 &= +324 = +2^2\cdot 81 && 97\\
+81+311 &= +392 = +2^3\cdot 49 && 100\\
+49+311 &= +360 = +2^3\cdot 45 && 103\\
+45+311 &= +356 = -2^2\cdot 89 && 105\\
+89+311 &= +400 = +2^4\cdot 25 && 109\\
+25+311 &= +336 = +2^4\cdot 21 && 113\\
+21+311 &= +332 = +2^2\cdot 83 && 115\\
+83-311 &= -228 = -2^2\cdot 57 && 117\\
-57-311 &= -368 = -2^4\cdot 23 && 121\\
-23+311 &= +288 = +2^5\cdot 9 && 126\\
+9+311 &= +320 = +2^6\cdot 5 && 132\\
+5+311 &= +316 = +2^2\cdot 79 && 134\\
+79-311 &= -232 = -2^3\cdot 29 && 137\\
-29-311 &= -340 = -2^2\cdot 85 && 139\\
-85-311 &= -396 = -2^2\cdot 99 && 141\\
-99+311 &= +212 = +2^2\cdot 53 && 143\\
+53+311 &= +364 = +2^2\cdot 91 && 145\\
+91-311 &= -220 = -2^2\cdot 55 && 147\\
-55+311 &= +256 = +2^8\cdot 1 && 155
\end{aligned}$$

therefore $x = 155$, and thus the smallest formula divisible by 311 is $2^{155}-1$. If we may stop at the 25th operation, we would have 2^{x-75}, and its remainder 47 ; and with the square taken 2^{2x-150}, or on being divided by the principle, 2^{x-150} with the remainder 2209, or $32 = 2^5\cdot 1$; from which the power 2^{x-155} produces the remainder chosen $+1$. But if we may stop at the 17th operation, we would have 2^{x-50} with the remainder 7, and with the cube taken 2^{3x-150} with the remainder 343, or $32 = 2^5\cdot 1$; thus so that now

2^{3x-155}, or also 2^{2x-155} will give the remainder $+1$; from which there follows $x = 155$, as before.

EXAMPLE 11

23. The first divisor shall be $N = 233$, and with the first remainder $= 1$, we will make:

	Sum of the exponents
$+\ 1 - 233 = -232 = -2^3 \cdot 29$	3
$-29 + 233 = +204 = +2^2 \cdot 51$	5
$+51 + 233 = +284 = +2^2 \cdot 71$	7
$+71 + 233 = +304 = +2^4 \cdot 19$	11
$+19 + 233 = +252 = +2^2 \cdot 63$	13
$+63 + 233 = +296 = +2^3 \cdot 37$	16
$+37 - 233 = -196 = -2^2 \cdot 49$	18
$-49 + 233 = +184 = +2^3 \cdot 23$	21
$+23 + 233 = +256 = +28 \cdot 1$	29

[therefore $x = 29$, and thus the smallest formula divisible by 233 is $2^{29} - 1$].

SCHOLIUM

24. Therefore for any divisor N, the simplest formula $2^x \pm 1$ divisible by that may be computed easily by this method. Apart from this consideration, the table is added here, in which the simplest formulas may be shown for all the prime numbers as far as to 400 ; but the prime divisors may conveniently be distributed into four orders, according to the forms $8n+1,\ 8n-1,\ 8n+3$ and $8n-3$:

N $8n+1$	$2^x \pm 1$	N $8n-1$	$2^x \pm 1$
1	$2^0 - 1$	7	$2^3 - 1$
17	$2^4 + 1$	23	$2^{11} - 1$
41	$2^{10} + 1$	31	$2^5 - 1$
73	$2^9 - 1$	47	$2^{23} - 1$
89	$2^{11} - 1$	71	$2^{35} - 1$
97	$2^{24} + 1$	79	$2^{39} - 1$
113	$2^{14} + 1$	103	$2^{51} - 1$
137	$2^{34} + 1$	127	$2^7 - 1$
193	$2^{48} + 1$	151	$2^{15} - 1$

233	$2^{29}-1$	167	$2^{83}-1$
241	$2^{12}+1$	191	$2^{95}-1$
257	$2^{8}+1$	199	$2^{99}-1$
281	$2^{35}+1$	223	$2^{37}-1$
313	$2^{78}+1$	239	$2^{119}-1$
337	$2^{21}-1$	263	$2^{131}-1$
353	$2^{44}+1$	271	$2^{135}-1$
401	$2^{100}+1$	311	$2^{155}-1$
		359	$2^{179}-1$
		367	$2^{183}-1$
		383	$2^{191}-1$
		431	$2^{215}-1$

N	$2^{x}+1$	N	$2^{x}+1$
$8n+3$		$8n-3$	
3	$2^{1}+1$	5	$2^{2}+1$
11	$2^{5}+1$	13	$2^{6}+1$
19	$2^{9}+1$	29	$2^{14}+1$
43	$2^{7}+1$	37	$2^{18}+1$
59	$2^{29}+1$	53	$2^{26}+1$
67	$2^{33}+1$	61	$2^{30}+1$
83	$2^{41}+1$	101	$2^{50}+1$
107	$2^{53}+1$	109	$2^{18}+1$
131	$2^{65}+1$	149	$2^{74}+1$
139	$2^{69}+1$	157	$2^{26}+1$
163	$2^{81}+1$	173	$2^{86}+1$
179	$2^{89}+1$	181	$2^{90}+1$
211	$2^{105}+1$	197	$2^{98}+1$
227	$2^{113}+1$	229	$2^{38}+1$
251	$2^{25}+1$	269	$2^{134}+1$
283	$2^{47}+1$	277	$2^{46}+1$
307	$2^{51}+1$	293	$2^{146}+1$
331	$2^{10}+1$	317	$2^{158}+1$
347	$2^{173}+1$	349	$2^{174}+1$
371	$2^{185}+1$	373	$2^{186}+1$
379	$2^{189}+1$	389	$2^{194}+1$
		397	$2^{22}+1$

These cases being properly considered, we will be able to establish the following theorem with a firm demonstration, which therefore is seen to be more noteworthy, which it needs even now.

THEOREM I

25. *If the prime number* $2p+1$ *were of the form* $8n\mp 1$, *the formula* 2^p-1 *will be divisible by that always* ; *but if it may have this form :* $8n\mp 3$, *the formula* 2^p+1 *will be divisible by that.*

Indeed since the formula $2^{2p}-1$ always will be divisible by the prime number $2p+1$, it is necessary, that one of these formulas : 2^p-1 or 2^p+1 may be able to be divided by the same; which since it may prevail equally with all the other powers $a^{2p}-1$, provided *a* were prime to $2p+1$, just as we may assume more and more values for *a*, the following theorems truly are understood :

THEOREM 2

26. *If the prime number* $2p+1$ *were of the form* $12n\pm 1$, *the formula* 3^p-1 *will always be divisible by that*. *But if it may have the form* $12n\mp 5$, *the formula* 3^p+1 *will be divisible by that*.

THEOREM 3

27. *By taking* $a=5$, *if* $2p+1$ *were a prime number, the following table declares whether the formula* 5^p-1 *or* 5^p+1 *will be divisible by that* :

If $2p+1$ were	the divisible formula will be
$20n\mp 1$	5^p-1
$20n\mp 3$	5^p+1
$20n\mp 7$	5^p+1
$20n\mp 9$	5^p-1

THEOREM 4

28. *By taking* $a = 6$, *if* $2p + 1$ *were a prime number, the following table declares whether the formula* $6^p - 1$ *or* $6^p + 1$ *may be divided by that :*

If $2p+1$ were	the divisible formula will be
$24n \mp 1$	$6^p - 1$
$24n \mp 3$	$6^p + 1$
$24n \mp 7$	$6^p + 1$
$24n \mp 9$	$6^p - 1$

THEOREM 5

29. *By taking* $a = 7$, *if* $2p + 1$ *were a prime number, the following table declares whether the formula* $7^p - 1$ *or* $7^p + 1$ *may be divided by that :*

If $2p+1$ were	the divisible formula will be
$28n \mp 1$	$7^p - 1$
$28n \mp 3$	$7^p + 1$
$28n \mp 7$	$7^p + 1$
$28n \mp 9$	$7^p - 1$
$28n \mp 11$	$7^p + 1$
$28n \mp 13$	$7^p + 1$

THEOREM 6

30. *By taking* $a = 8$, *if* $2p + 1$ *were a prime number, the following table declares whether the formula* $8^p - 1$ *or* $8^p + 1$ *may be divided by that :*

If $2p+1$ were	the divisible formula will be
$32n \mp 1$	$8^p - 1$
$32n \mp 3$	$8^p + 1$
$32n \mp 5$	$8^p + 1$

$32n \mp 7$	$8^p - 1$
$32n \mp 9$	$8^p - 1$
$32n \mp 11$	$8^p + 1$
$32n \mp 13$	$8^p + 1$
$32n \mp 15$	$8^p - 1$

THEOREM 7

31. *By taking* $a = 10$, *if* $2p+1$ *were a prime number, the following table declares whether the formula* $10^p - 1$ *or* $10^p + 1$ *may be divided by that :*

If $2p+1$ were	the divisible formula will be
$40n \mp 1$	$10^p - 1$
$40n \mp 3$	$10^p - 1$
$40n \mp 7$	$10^p + 1$
$40n \mp 9$	$10^p - 1$
$40n \mp 11$	$10^p + 1$
$40n \mp 13$	$10^p - 1$
$40n \mp 17$	$10^p + 1$
$40n \mp 19$	$10^p + 1$

GENERAL THEOREM

32. *Whatever the number a may be, if* $2p+1$ *denotes a prime number and in the case* $p = f$ *it will be required to know, whether the formula* $a^f - 1$, *or the formula* $a^f + 1$ *shall be divisible by* $2f+1$, *then generally a formula of this kind either* $a^p - 1$ *or* $a^p + 1$ *will be divisible by* $2p+1$, *if there were* $2p+1 = 4af \mp (2f+1)$), *whatever number may be taken for n, provided thence* $2p+1$ *may produce a prime number.*

COROLLARY 1

33. It is clear enough from the preceding theorems, for the case $f = 0$ the formula $a^p - 1$ always to become divisible by $2p+1 = 4an \mp 1$, whenever it is evident the number here will have been prime.

COROLLARY 2

34. But if there shall be $f = 1$, provided either $a - 1$, or $a + 1$ can be divided by 3, for the similar case generally either the formula $a^p - 1$ or the formula $a^p + 1$ will be divisible by the prime number $2p + 1$, as often as $2p + 1$ may be expressed in this form : $4an \pm 3$.

SCHOLIUM

35. But the particular theorems advanced are able to be continued further easily, if the following problem may be called in to help, indeed the solution of which is supported by the most solid reasoning.

PROBLEM

36. *Whatever the number a, if* $2p + 1$ *may denote a prime number, in whatever case may be presented to be investigated, either the formula* $a^p - 1$ *or the other* $a^p + 1$ *will be divisible by* $2p + 1$.

SOLUTION

All the remainders are sought, which result from the division of the squares by the number $2p + 1$, which shall be 1, α, β, δ, δ etc. with the number of these $= p$, but the non-remainder numbers different from these will be addressed. With which put in place if the number *a* may be found among the remainders, then the formula $a^p - 1$ will always be divisible; but if the number *a* occurs among the non-remainders, then the other formula $a^p + 1$ will be divisible.

Moreover this rule may be demonstrated thus : If *a* were the remainder arising from any square x^2 divided by $2p + 1$, then $x^2 - a$ will be divisible by $2p + 1$; but if that will be equal to some multiple $m(2p + 1)$, thus so that there becomes $a = x^2 - m(2p + 1)$. Hence therefore there becomes $a^p = (x^2 - m(2p + 1))^p$, which power divided by $2p + 1$ will leave the same remainder as the power $(x^2)^p$; truly this power will change into x^{2p}, which divided by $2p + 1$ certainly will leave the remainder one. From which it follows the power a^p leaves the remainder one also, if the formula $a^p - 1$ shall be divisible.

COROLLARY

37. Since the remainders $1,\ \alpha,\ \beta,\ \delta,\ \delta$ etc. shall be accustomed to be smaller than the divisor $2p+1$, at this point it will be allowed to enumerate from these : $1+(2p+1),\ \alpha+(2p+1),\ \beta+(2p+1)$ etc., which being observed, if the number *a* were greater than the divisor $2p+1$.

SCHOLIUM

38. Therefore since in this business it shall be of the greatest importance to know the remainders as well as the non-remainders, here we may add the following table for the smaller prime divisors; but it would be superfluous to have put the non-remainders in place.

Divisor	Remainder
3	1, 4, 7, 10, 13, 16, 19, 22, 25 etc.
5	1, 4, 6, 9, 11, 14, 16, 19, 21, 24 etc.
7	1, 2, 4, 8, 9, 11, 15, 16, 18, 22 etc.
11	1, 3, 4, 5, 9, 12, 14, 15, 16, 20, 23 etc.
13	1, 3, 4, 9, 10, 12, 14, 16, 17, 22, 23, 25, 27 etc.
17	1, 2, 4, 8, 9, 13, 15, 16, 18, 19, 21, 25, 26, 30 etc.
19	1, 4, 5, 6, 7, 9, 11, 16, 17, 20, 23, 24, 25, 26 etc.
23	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18, 24, 25, 26, 27 etc.
29	1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28 etc.
31	1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28 etc.
37	1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 etc.
	etc.

We will be able to derive the following particular theorems most easily with the aid of this table.

THEOREM 8

39. *By taking* $a=11$, *if* $2p+1$ *were a prime number, the following table shows whether the formula* 11^p-1, *or* 11^p+1 *shall be divisible by that:*

If $2p+1$ were	the divisible formula will be :
$44n\pm1$	11^p-1
$44n\pm3$	11^p+1
$44n\pm5$	11^p-1
$44n\pm7$	11^p-1
$44n\pm9$	11^p-1

$44n \pm 13$	$11^p + 1$
$44n \pm 15$	$11^p + 1$
$44n \pm 17$	$11^p + 1$
$44n \pm 19$	$11^p - 1$
$44n \pm 21$	$11^p + 1$

THEOREM 9

40. *By taking* $a = 12$, *if* $2p+1$ *were a prime number, it will be apparent from the following table, whether the form* $12^p + 1$ *or* $12^p - 1$ *shall be divisible by that number :*

If $2p+1$ were	the divisible formula will be :
$48n \pm 1$	$12^p - 1$
$48n \pm 5$	$12^p + 1$
$48n \pm 7$	$12^p + 1$
$48n \pm 11$	$12^p - 1$
$48n \pm 13$	$12^p - 1$
$48n \pm 17$	$12^p + 1$
$48n \pm 19$	$12^p + 1$
$48n \pm 23$	$12^p - 1$

THEOREM 10

41. *By taking successively* $a = 13,\ 14,\ 15$, *if* $2p+1$ *were a prime number, from the following table it will be apparent whether it shall be divisible either by the form* $a^p + 1$ *or* $a^p - 1$:

$a=13$		$a=14$		$a=15$	
$2p+1$		$2p+1$		$2p+1$	
	$13^p - 1$	$56n \pm 1$	$14^p - 1$	$60n \pm 1$	$15^p - 1$
$52n \pm 3$	$13^p - 1$	$56n \pm 3$	$14^p + 1$	$60n \pm 7$	$15^p - 1$
$52n \pm 5$	$13^p + 1$	$56n \pm 5$	$14^p - 1$	$60n \pm 11$	$15^p - 1$
$52n \pm 7$	$13^p + 1$	$56n \pm 9$	$14^p - 1$	$60n \pm 13$	$15^p + 1$
$52n \pm 9$	$13^p - 1$	$56n \pm 11$	$14^p + 1$	$60n \pm 17$	$15^p - 1$
$52n \pm 11$	$13^p + 1$	$56n \pm 13$	$14^p - 1$	$60n \pm 19$	$15^p + 1$
$52n \pm 15$	$13^p + 1$	$56n \pm 15$	$14^p + 1$	$60n \pm 23$	$15^p + 1$
$52n \pm 17$	$13^p - 1$	$56n \pm 17$	$14^p + 1$	$60n \pm 29$	$15^p + 1$
$52n \pm 19$	$13^p + 1$	$56n \pm 19$	$14^p + 1$		
$52n \pm 21$	$13^p + 1$	$56n \pm 23$	$14^p + 1$		
$52n \pm 23$	$13^p - 1$	$56n \pm 25$	$14^p - 1$		
$52n \pm 25$	$13^p - 1$	$56n \pm 27$	$14^p + 1$		

IN ADDITION

What have been treated so far and generally, hitherto are destitute in rigorous demonstrations ; but all doubts will be refuted in the main part by the following propositions, by which likewise all the evidence will be raised to a much higher level.

THEOREM 1

1. *If the formula* $4p+(2q+1)^2$ *were a prime number, and all the squares may be divisible by that, both* $+p$ *as well as* $-p$ *will occur among the remainders.*

DEMONSTRATION.

In the first place all the smaller squares occur with these remainders, in as much as they are from the divisor itself, which we may designate by *D,* with the letter *q* ; besides truly from the greater squares such as Q^2, the remainders Q^2-D or $Q^2-\lambda D$ arise. There is no reason also why all the remainders may not be referred to the formulas $Q^2 \mp D$. Therefore there may be taken $Q^2=(2q+1)^2$, and on account of $D=4p+(2q+1)^2$ the remainder $-4p$ will be produced; therefore also there will be $-p$ among the remainders, because generally, if $\alpha^2\beta$ were among the remainders, then likewise β always will be found too. Again since here the divisor $4p+(2q+1)^2$ is expressed in the form $4n+1$, now it has been shown the individual remainders are found and each with the sign + or − attached; from which it is evident in our case both the $+p$ as well as the $-p$ remainders must be found.

COROLLARY 1

2. Because both $+p$ as well as $-p$ is a remainder, the formulas will give both $xx+pyy$ as well as $xx-pyy$ divisible by the proposed divisor *D*.

COROLLARY 2

3. But since these formulas $xx+pyy$ and $xx-pyy$ do not allow other divisors, except those which may be present in certain formulas, it is necessary, that also all the prime numbers may be taken under the same formulas.

COROLLARY 3

4. Because, by putting the divisor $=2m+1$, the number of all the remainders is $=m$ only, while all the remaining numbers shall be referred to as non-remainders, hence it follows also the formula p^m-1 to be divisible by $2m+1$, provided $2m+1$ were a prime

number. Indeed because all the powers of p are remainders too, of which the number as much as m, it is necessary, that the power p^m again may be reduced to unity, or p^0, and hence $p^m - 1$ will be able to be divided by the divisor $2m+1$.

THEOREM 2

5. *If the formula* $4p-(2q+1)^2$ *were a prime number, and all the squares may be divided by that, the number p always will occur in the remainders; but its negative* $-p$, *if the same returns* $D-p$, *with D denoting a divisor, is referred to the non-remainders.*

DEMONSTRATION

Besides these squares with the smaller divisors, also with the divisor increased, the square $(2q+1)^2$ and thus $4p$ occurs among the remainders ; therefore, by the reasoning advance before, the number p will occur also. And because here $4p-(2q+1)^2$ is a number of the form $4n-1$, where no remainder occurs either with the $+$ and $-$ sign attached, it follows $-p$ must be found among the non-remainders.

COROLLARY 1

6. Therefore because certainly p is a remainder, it will give the formula $xx-pyy$ divisible by our divisor, from which also the divisor will be had of this kind, which the divisors of the formula $xx-pyy$ demand.

COROLLARY 2

7. But since $-p$ is a non-remainder, no formula will give $xx+pyy$ divisible by our divisor, from which also the divisor from our general formula is excluded, which includes all the divisors of $xx+pyy$.

COROLLARY 3

8. On account of the argument advanced before, if we may call the divisor $2m+1$, the formula p^m-1 must be divisible by that; nor truly will this formula $(-p)^m-1$ be divisible, which by itself is evident. Since indeed the divisor may have our form $4n-1$, there will become $m=2n-1$, and thus an odd number, and $(-p)^m=-p^m$; whereby since p^m-1 shall be divisible, certainly this formula $-p^m-1$ or p^m+1 will not be divisible.

THEOREM 3

9. *If* $4n+1$ *were a prime number, and all the squares may be divided by that, among the remainders all the numbers occur to be expressed either in this general form :* $n-qq-q$, *or in this:* $qq+q-n$.

DEMONSTRATION

It is evident our divisor $4n+1$ can be reduced in innumerable ways to the form $4p+(2q+1)^2$. Indeed on putting $4n+1=4p+(2q+1)^2$ there becomes $n=p+q^2+q$, and thus $p=n-q^2-q$; from which it follows, if any number may be accepted for q, the number $n-qq-q$ to be found among the remainders ; then since also $-p$ is a remainder (§ 1), it is evident all the numbers in this form $qq+q-n$ also to become remainders.

COROLLARY 1

10. Therefore in this manner, while all the numbers 0, 1, 2, 3, 4, 5 etc. may be accepted successfully for q indefinitely, the numbers will be produced referring to the remainders, which yet all may be allowed to be reduced to a multiple of $2n$, since more different remainders are not given as multiples of $2n$.

COROLLARY 2

11. Therefore it is necessary, so that all the numbers to be expressed either in the form $n-qq-q$ or in the form $qq+q-n$, clearly all conveniently will produce remainders of the divisor $4n+1$. So that also from some other remainders of this kind the rest arise at once, since just as some of the individual powers also, as well as the products from two or more must occur equally in the remainders; from which it is apparent, if now the remainders $\alpha\gamma$ and $\beta\gamma$ will have arisen, then also the remainder to become $\alpha\beta$. Because indeed the product $\alpha\beta\gamma^2$ is the remainder, with the square γ^2 omitted, $\alpha\beta$ also will be the remainder.

COROLLARY 3

12. So that if therefore the remainder $\alpha\beta$ were prepared, from the one case the remainder α may be produce, but also from the other the factor β will be the remainder.

SCHOLIUM

13. Since with more combinations of two remainders of this kind, more correctly it may be able to be put in place infinitely many kinds, hence now it may seem especially

plausible, besides these numbers expressed in the formulas $n-qq-q$ and $qq+q-n$ also the prime factors of these occur in the remainders, whether or not which fundamental conjecture may be relied on, we may investigate in the following examples. To this end we may set out the numbers expressed in the formula $qq+q$ which are,

0, 2, 6, 12, 20, 30, 42, 56, 72, 90, 110, 132, 156,
182, 210, 240, 272, 306, 342, 380, 420 etc.,

and just as we may designate the remainders hence arisen by the letter *p*, or thus we may indicate the prime remainder by the letter *r*, and so that all the factors of the numbers *p* may be seen more clearly also to be remainders, we may represent the numbers *p* by their prime factors :

1°. Let $4n+1=5$; there will be $n=1$. [*i.e.* $p=qq+q-n$]

$p=1,\ 1,\ 5,\ 11,\ 19,\ 29,\ 41,\ 5\cdot 11,\ 71$ etc.

$r=1,\ 5,\ 11,\ 19,\ 29,\ 41,\ 71$ etc.,

where it is apparent of the composite number *p,* which is one of a kind $5\cdot 11$, the factors themselves to be remainders also.

2°. Let $4n+1=13; n=3$.

$p=3,\ 1,\ 3,\ 3^2,\ 17,\ 3^3,\ 3\cdot 13,\ 53,\ 3\cdot 23$ etc.

$r=1,\ 3,\ 13,\ 17,\ 23,\ 53$ etc.

3°. Let $4n+1=17; n=4$.

$p=2^2,\ 2,\ 2,\ 2^3,\ 2^4\ ,\ 2\cdot 13,\ 2\cdot 19,\ 2^2\cdot 13,\ 2^2\cdot 17,\ 2\cdot 43$ etc.

$r=1,\ 2,\ 13,\ 17,\ 19,\ 43$ etc.

4°. Let $4n+1=29$; $n=7$.

$p=7,\ 5,\ 1,\ 5,\ 13,\ 23,\ 5\cdot 7,\ 7^2\ ,\ 5\cdot 13,\ 83,\ 103$ etc.

$r=1,\ 5,\ 7,\ 13,\ 23,\ 83,\ 103$ etc.

5°. Let $4n+1=37$; $n=9$.

$p=3^2,\ 7,\ 3,\ 3,\ 11,\ [3\cdot 7,]\ 3\cdot 11,\ 47,\ \left[3^2\cdot 7,\right]\ 3^4,\ 101$ etc.

$r=1,\ 3,\ 7,\ 11,\ 47,\ 101$ etc.

6°. Let $4n+1=41; n=10$.

$p=2\cdot 5,\ 2^3,\ 2^2,\ 2,\ 2\cdot 5,\ 2^2\cdot 5,\ 2^5,\ 2\cdot 23,\ 2\cdot 31,\ 2^4\cdot 5,\ 2^2\cdot 5^2$ etc.

$r=1,\ 2,\ 5,\ 23,\ 31$ etc.,

where it is apparent no prime factors to be seen in the numbers *p*, which shall not likewise be remainders.

7°. Let $4n+1=53; n=13$

$p = 13,\ 11,\ 7,\ 1,\ 7,\ 17,\ 29,\ 43,\ 59,\ 7\cdot 11,\ 97$ etc.

$r = 1, 7,\ 11,\ 13,\ 17,\ 29,\ 43,\ 59,\ 97$ etc.

8^{o} Let $4n+1 = 61$; $n = 15$.

$p = 3\cdot 5,\ 13,\ 3^2,\ 3,\ 5,\ 3\cdot 5,\ 3^3,\ 41,\ 3\cdot 19,\ 3\cdot 5^2,\ 5\cdot 19$ etc.

$r = 1,\ 3,\ 5,\ 13,\ 19,\ 41$ etc.

9°. Let $4n+1 = 73; n = 18$.

$p = 2\cdot 3^2,\ 2^4,\ 2^2\cdot 3,\ 2\cdot 3,\ 2,\ 2^2\cdot 3,\ 2^3\cdot 3,\ 2\cdot 19,\ 2\cdot 3^3\ ,\ 2^3\cdot 3^2,\ 2^2\cdot 23$ etc.

$r = 1,\ 2,\ 3,\ 19,\ 23$ etc.

10°. Let $4n+1 = 89; n = 22$.

$p = 2\cdot 11,\ 2^2\cdot 5,\ 2^4,\ 2\cdot 5,\ 2,\ 2^3,\ 2^2\cdot 5,\ 2\cdot 17,\ 2\cdot 5^2,\ 2^2\cdot 17,\ 2^3\cdot 11$ etc.

$r = 1,\ 2,\ 5,\ 11,\ 17$ etc.

11°. Let $4n+1 = 97; n = 24$.

$p = 2^3\cdot 3,\ 2\cdot 11,\ 2\cdot 32,\ 2^2\cdot 3,\ 2^2,\ 2\cdot 3,\ 2\cdot 3^2,\ 2^5,\ 2^4\cdot 3,\ 2\cdot 3\cdot 11,\ 2\cdot 43$ etc.

$r = 1,\ 2,\ 3,\ 11,\ 43$ etc.

12°. Let $4n+1 = 101; n = 25$.

$p = 5^2,\ 23,\ 19,\ 13,\ 5,\ 5,\ 17,\ 31,\ 47,\ 5\cdot 13,\ 5\cdot 17$ etc.

$r = 1,\ 5,\ 13,\ 17,\ 19,\ 23,\ 31,\ 47$ etc.

13°. Let $4n+1 = 109; n = 27$.

$p = 3^3,\ 5^2,\ 3\cdot 7,\ 3\cdot 5,\ 7,\ 3,\ 3\cdot 5,\ 29^2,\ 32\cdot 5,\ 32\cdot 7,\ 83$ etc.

$r = 1,\ 3,\ 5,\ 7,\ 29^3,\ 83$ etc.

14°. Let $4n+1 = 113; n = 28$.

$p = \ 2^2\cdot 7,\ 2\cdot 13,\ 2\cdot 11,\ 2^4,\ 2^3\ ,\ 2,\ 2\cdot 7,\ 2^2\cdot 7,\ 2^2\cdot 11,\ 2\cdot 31,\ 2\cdot 41$ etc.

$r = 1,\ 2,\ 7,\ 11,\ 13,\ 31,\ 41$ etc.

15°, Let $4n+1 = 137; n = 34$.

$p = 2\cdot 17,\ 2^5\ ,\ 2^2\cdot 7,\ 2\cdot 11,\ 2\cdot 7,\ 2^2\ ,\ 2^3\ ,\ 2\cdot 11,\ 2\cdot 19,\ 23\cdot 7,\ 22\cdot 19$ etc.

$r = 1,\ 2,\ 7,\ 11,\ 17,\ 19$ etc.

16°. Let $4n+1 = 149; n = 37$.

$p = \ 37,\ 5\cdot 7,\ 31,\ 5^2\ ,\ 17,\ 7,\ 5,\ 19,\ 5\cdot 7,\ 53,\ 73$ etc.

$r = \ 1,\ 5,\ 7,\ 17,\ 19,\ 31,\ 37,\ 53,\ 73$ etc.

17°. Let $4n+1 = 157; n = 39$.

$p = 3\cdot 13,\ 37,\ 3\cdot 11,\ 3^3\ ,\ 19,\ 3^2,\ 3,\ 17,\ 3\cdot 11,\ 3\cdot 17,\ 71$ etc.

$r = 1,\ 3,\ 11,\ 13,\ 17,\ 19,\ 37,\ 71$ etc.

18°. Let $4n+1 = 173; n = 43$.

$p = \ 43,\ 41,\ 37,\ 31,\ 23,\ 13,\ 1,\ 13,\ 29,\ 47,\ 67$ etc.

$r = 1,\ 13,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 67$ etc.

19°. Let $4n+1=181; n=45$.

$p = 3^2\cdot 5,\ 43,\ 3\cdot 13,\ 3\cdot 11,\ 5^2,\ 3\cdot 5,\ 3,\ 11,\ 3^3,\ 3^2\cdot 5,\ 5\cdot 13$ etc.

$r = 1,\ 3,\ 5,\ 11,\ 13,\ 43$ etc.

20°. Let $4n+1=193; n=48.$

$p = 2^4\cdot 3,\ 2\cdot 23,\ 2\cdot 3\cdot 7,\ 2^2\cdot 3^2,\ 2^2\cdot 7,\ 2\cdot 3^2,\ 2\cdot 3,\ 2^3,\ 2^3\cdot 3,\ 2\cdot 3\cdot 7,\ 2\cdot 31$ etc.

$r = 1,\ 2,\ 3,\ 7,\ 23,\ 31$ etc.

21. Let $4n+1=197; n=49$.

$p = 7^2,\ 47,\ 43,\ 37,\ 29,\ 19,\ 7,\ 7,\ 23,\ 41,\ 61$ etc.

$r = 1,\ 7,\ 19,\ 23,\ 29,\ 37,\ 41,\ 43,\ 47,\ 61$ etc.

SCHOLIUM

14. Clearly, from all these examples, it will be apparent no prime numbers occur as factors under the letter p, which likewise shall not be remainders; which truth certainly thus may deserve the more attention, which has been concluded from induction alone, nor even now corroborated by a rigorous demonstration; because in all the examples yet brought forwards it is presented so very well, it may be seen by no means to be despairing. But anyone who would want to undertake this investigation, may consider this outstanding property only then may have a place, when $4n+1$ is a prime number; for if it is not a prime number, numerous cases occur, by which this may happen otherwise. There is an example of this kind when $n = 11$; for then it produces $p = 11,\ 3^2,\ 5,\ 1,\ 3^2,\ 19,\ 31,\ 3^2\cdot 5,\ 61,\ 79,\ 3^2\cdot 11$ etc., from which plainly nothing can be concluded for the number 3, whether or not anything may pertain to the remainder three? But because in the cases, in which $4n+1$ is a prime number, it may be succeed always, perhaps the reasoning in that is required to be sought, because for the divisor $2n + 1$ the number of remainders is n always, while on the other hand, if $2n+1$ is not prime, the number of remainders is much smaller; that which may be seen to be in the cause, because in the example brought forward nothing may be decided about the number 3. But whatever it shall be, clearly no doubt may be seen to remain, by which the following may be less rigorous.

CONCLUSION

15. As often as the number $4n+1$ were prime, and all the squares may be divided by that, not only all the numbers expressed in this formula: $n-qq-q$, but also in this : $qq+q-n$, occur among the remainders themselves, but also clearly all the prime factors, from which these shall be composed.

THEOREM 4

16. *If* $4n-1$ *were a prime number and all the squares may be divided by that, among the remainders all the numbers occur expressed in this formula* $n+qq+q$.

DEMONSTRATION

Here it is clear also, the number $4n-1$ can be represented in an infinite number of ways under this form $4p-(2q+1)^2$; for on putting $4n-1=4p-(2q+1)^2$, there will become $n=p-q^2-q$, or $p=n+q^2+q$. Therefore since $4p-(2q+1)^2$ shall be a prime number, it has been shown before the number *p* to be found among the remainders; on account of which also all the numbers expressed in this formula $n+qq+q$ may be found among the remainders.

COROLLARY 1

17. Therefore if all the numbers 0, 1, 2, 3, 4 etc. may be substituted for *q*, infinitely many numbers of this kind may arise, which yet all can be expressed according to the multitude of $2n-1$, if indeed these numbers themselves $n+qq+q$ may be divided by $4n-1$.

COROLLARY 2

18. Therefore it is necessary all the remainders to be produced in this manner, since also both the powers, as well as the products of the individual numbers themselves are found among the remainders ; from which as it followed before, if now two remainders α and $\alpha\beta$ may be had, then also β to become a remainder; indeed if $\alpha\gamma\gamma$ were a remainder, α itself too will be a remainder.

SCHOLIUM

19. Since two remainders of this kind may be combined in infinitely many ways, the most plausible is suspected besides these numbers expressed in the form $n+qq+q$ also all the prime factors occur in all of these ; whether which conjecture, equally as before, may or may not struggle with the foundation, we will investigate by the following examples. But now above we have set out numbers expressed by the formula $qq+q$, from which for any simple prime number remainder, equally as before, we will indicate by the letter *r*.

1°. Let $4n-1=3$; there will be $n=1$.

$p = 1,\ 3,\ 7,\ 13,\ 3\cdot 7,\ 31,\ 43,\ 3\cdot 19,\ 73,\ 7\cdot 13,\ 3\cdot 37$ etc.

$r = 1,\ 3,\ 7,\ 13,\ 19,\ 31,\ 37,\ 43,\ 73$ etc.

2°. Let $4n-1=7$; there will be $n=2$.

$p = 2,\ 2^2,\ 2^3,\ 2\cdot 7,\ 2\cdot 11,\ 2^5,\ 2^2\cdot 11,\ 2\cdot 29,\ 2\cdot 37,\ 2^2\cdot 23,\ 2^4\cdot 7$ etc.

$r = 1,\ 2,\ 7,\ 11,\ 23,\ 29,\ 37$ etc.

3°. Let $4n-1=11$; there will be $n=3$.

$p = 3,\ 5,\ 3^2,\ 3\cdot 5,\ 23,\ 3\cdot 11,\ 3^2\cdot 5,\ 59,\ 3\cdot 5^2,\ 3\cdot 31,\ 113$ etc.

$r = 1,\ 3,\ 5,\ 11,\ 23,\ 31,\ 59,\ 113$ etc.

4°. Let $4n-1=19$; there will be $n=5$.

$p = 5,\ 7,\ 11,\ 17,\ 5^2,\ 5\cdot 7,\ 47,\ 61,\ 7\cdot 11,\ 5\cdot 19,\ 5\cdot 23$ etc.

$r = 1,\ 5,\ 7,\ 11,\ 17,\ 19,\ 23,\ 47,\ 61$ etc.

5°. Let $4n-1=23$; there will be $n=6$.

$p = 2\cdot 3,\ 2^3,\ 2^2\cdot 3,\ 2\cdot 3^2,\ 2\cdot 13,\ 2^2\cdot 3^2,\ 2^4\cdot 3,\ 2\cdot 31,\ 2\cdot 3\cdot 13,\ 2^5\cdot 3,\ 2^2\cdot 29$ etc.

$r = 1,\ 2,\ 3,\ 13,\ 29,\ 31$ etc.

6°. Let $4n-1=31$; there will be $n=8$.

$p = 2^3,\ 2\cdot 5,\ 2\cdot 7,\ 2^2\cdot 5,\ 2^2\cdot 7,\ 2\cdot 19,\ 2\cdot 5^2,\ 2^6,\ 2^4\cdot 5,\ 2\cdot 7^2,\ 2\cdot 59$ etc.

$r = 1,\ 2,\ 5,\ 7,\ 19,\ 59$ etc.

7°. Let $4n-1=43$; there will be $n=11$.

$p = 11,\ 13,\ 17,\ 23,\ 31,\ 41,\ 53,\ 67,\ 83,\ 101,\ 11^2$etc.

$r = 1,\ 11,\ 13,\ 17,\ 23,\ 31,\ 41,\ 53,\ 67,\ 83,\ 101$ etc.

8°. Let $4n-1=47$; $n=12$.

$p = 2^2\cdot 3, 2\cdot 7, 2\cdot 3^2, 2^3\cdot 3, 2^5, 2\cdot 3\cdot 7, 2\cdot 3^3,\ 2^2\cdot 17,\ 2^2\cdot 3\cdot 7,\ 2\cdot 3\cdot 17, 2\cdot 61$etc.

$r = 1,\ 2,\ 3,\ 7,\ 17,\ 61$ etc.

9°. Let $4n-1=59$; $n=15$.

$p = 3\cdot 5,\ 17,\ 3\cdot 7,\ 3^3,\ 5\cdot 7,\ 3^2\cdot 5,\ 3\cdot 19,\ 71,\ 3\cdot 29$ etc.

$r = 1,\ 3,\ 5,\ 7,\ 17,\ 19,\ 29,\ 71$ etc.

10°. Let $4n-1=67$; $n=17$.

$p = 17,\ 19,\ 23,\ 29,\ 37,\ 47,\ 59,\ 73,\ 89,\ 107,\ 127$ etc.

$r = 1,\ 17,\ 19,\ 23,\ 29,\ 37,\ 47,\ 59,\ 73,\ 89,\ 107,\ 127$ etc.

11°. Let $4n-1=71$; $n=18$.

$p = 2\cdot 3^2,\ 2^2\cdot 5,\ 2^3\cdot 3,\ 2\cdot 3\cdot 5,\ 2\cdot 19,\ 2^4\cdot 3,\ 2^2\cdot 3\cdot 5,\ 2\cdot 37,\ 2\cdot 3^2\cdot 5,\ 2^2\cdot 3^3, 2^7,\ 2\cdot 3\cdot 5^2$etc.

$r = 1,\ 2,\ 3,\ 5,\ 19,\ 37$ etc.

12°. Let $4n-1=79$; $n=20$.

$p = 2^2\cdot 5,\ 2\cdot 11,\ 2\cdot 13,\ 2^5,\ 2^3\cdot 5,\ 2\cdot 5^2,\ 2\cdot 31,\ 2^2\cdot 19,\ 2^2\cdot 23,\ 2\cdot 5\cdot 11$ etc.

$r = 1,\ 2,\ 5,\ 11,\ 13,\ 19,\ 23,\ 31$ etc.

13°. Let $4n-1=83$; $n=21$.

$p = 3\cdot 7,\ 23,\ 3^3,\ 3\cdot 11,\ 41,\ 3\cdot 17,\ 3^2\cdot 7,\ 7\cdot 11,\ 3\cdot 31,\ 3\cdot 37$ etc.

$r = 1,\ 3,\ 7,\ 11,\ 17,\ 23,\ 31,\ 37,\ 41$ etc.

14°. Let $4n-1 = 103\,;\ n = 26$.

$p = 2\cdot 13,\ 2^2\cdot 7,\ 2^5,\ 2\cdot 19,\ 2\cdot 23,\ 2^3\cdot 7,\ 2^2\cdot 17,\ 2\cdot 41,\ 2\cdot 7^2,\ 2^2\cdot 29$ etc.

$r = 1,\ 2,\ 7,\ 13,\ 17,\ 19,\ 23,\ 29,\ 41$ etc.

SCHOLIUM

20. From these examples again it is made abundantly plain all these prime numbers contained in the letters *p* themselves to be remainders also. Moreover it is apparent, as this prime would be certain from the smaller numbers, no further doubt would remain from the greater numbers; but truly in the numbers p the number two does not enter, unless now it were by itself in the prime number *n;* moreover three, unless it were present in the two primes, is excluded from the whole series *p*. In the same manner it is apparent of the fifth, unless it may be present in the three primes, also to be excluded ; but the seventh finally is excluded, unless it may occur in the four primes, and thus for the remaining. From which it is apparent in the further continuation of this series no smaller prime numbers can enter, which now had not entered before; which observation perhaps may be able to be deduced for the demonstration. Truly here again this conspicuous property only has a place, as often as $4n-1$ were a prime number; if indeed it were composite, then certainly prime numbers of this kind can appear, from which will it by no means be clear, into which order *r* they shall be required to be referred. Just as if there were $n = 30 = 2\cdot 3\cdot 5$, then the numbers for *p* thus themselves will be had :

$p = 2\cdot 3\cdot 5,\ 2^5,\ 2^2\cdot 3^2,\ 2\cdot 3\cdot 7,\ 2\cdot 5^2,\ 2^2\cdot 3\cdot 5,\ 2^3\cdot 3^2,\ 2\cdot 43,\ 2\cdot 3\cdot 17,\ 23\cdot 3\cdot 5,$
$2^2\cdot 5\cdot 7,\ 2\cdot 3^4$ etc.

Here indeed it is apparent at once for the remainders of two to be referred to ; with which removed judgement returns to the following numbers:

$3\cdot 5,\ 3^2,\ 3\cdot 7,\ 5^2,\ 43,\ 3\cdot 17,\ 5\cdot 7,\ 3^4$etc.

Hence moreover in no way can it be concluded either 3, 5, or 7 to be found in the remainders ; and it can happen, that the individual terms may be non-remainders, since the products from two non-remainders may produce a remainder ; truly hence the number $4n-1 = 119$ also is not a prime. But certainly with the primes this may be observed :

CONCLUSION

21. As often as the number $4n-1$ were a prime, and by that all the squares may be divided, not only all the numbers in the form $n+qq+q$ expressed among the remainders themselves occur, but also clearly all the prime factors, from which these are composed.

GENERAL THEOREM

22. *With T denoting some number expressed in this formula* $(2q+1)^2 - 4at$*, if either* $4as+T$ *or* $4as-T$ *were a prime number, and the squares may be divided by that, then the number a will always be found in the remainder.*

DEMONSTRATION

Indeed since there shall be $T = (2q+1)^2 - 4at$, that prime number will be either $4as - 4at + (2q+1)^2$, or $4as + 4at - (2q+1)^2$. In this case we will have $p = a(s-t)$, in the other truly $p = a(s+t)$, and thus in each case p has the factor a, which therefore by the preceding conclusions will occur in the remainders arising from the squares.

COROLLARY I

23. Therefore in this manner the numbers T will be able to be expressed from the squares $(2q+1)^2$ formed below $4a$; and thus a multitude of these values will be reduced to the number requiring to be determined, even if the numbers $(2q+1)^2$ may be progressing to infinity. But with all the values of T found, with themselves smaller than $4a$, if to these continually multiples of $4a$ may be added, these values will be able to continue indefinitely.

COROLLARY 2

24. Because the number a occurs among the remainders of the squares, the formula $xx - ayy$ will be given always divisible by that prime number, whether it shall be divisible by $4as+T$ or by $4as-T$; and if this same prime number may be called $2m+1$, then the formula $a^m - 1$ will have the divisor $2m+1$.

SCHOLIUM

25. But so that the letter T may choose different values below $4a$, that will depend on the nature of the number a, whether this were prime or composite; and this difference is to be observed properly, since the further development of these formulas for the cases, for which a is a composite number, cannot be set out conveniently, except the case in which a is a prime number, as were investigated before.

THEOREM 5

26. *If a were a prime number, for example* $2\alpha+1$ *, then the number of values of the letter T less than* 4*a will be* $=\alpha$*, and just as many numbers of the form* $4n+1$ *thence may be excluded.*

DEMONSTRATION

All the different values of the letter *T* smaller than 4*a* may be deduced from the odd squares smaller than $a^2=(2\alpha+1)^2$, which therefore are 1, 9, 25, 49, ... $(2\alpha-1)^2$, the number of which certainly is α. But it is evident from the squares greater than *a* to result in exactly the same values of *T*, which were produced from the smaller values. Indeed there shall be some greater square $(a+\beta)^2$, and this may be compared with the smaller square $(a-\beta)^2$, and because the difference of these $4a\beta$ is divisible by 4*a,* the same remainder by necessity shall arise on both sides. But again it may be easily understood different remainders must arise from all the squares themselves smaller then a^2. Because now *T* may denote a number of the form $4n+1$, we may see, how many numbers of this kind occur from unity as far as to $4a=8\alpha+4$. But it is readily apparent the number of these to become $=2\alpha+1$, among which one occurs divisible by *a* ; with which excluded the number of the remaining is $=2\alpha$*;* whereby since the number of suitable values of *T* itself shall be $=\alpha$*,* it is evident just as many numbers of the form $4n+1$ thence to be excluded.

COROLLARY 1

27. Since all the values of the letter *T* may be expressed in the form $4n+1$, if all the numbers of this form from unity as far as 4*a* may be written, only the half of these present the true values of the letter *T,* truly all the remainder thence are excluded. Moreover we may use the letter Θ for denoting excluded numbers of this kind.

COROLLARY 2

28. Therefore since all the numbers of the form $4n+1$, which are: 1, 5, 9, 13, 17, 21, 25, 29, 33 etc., for any case of the number *a,* whether they may refer to the order of terms $T=(2q+1)^2-4at$*,* or to the order of the excluded terms Θ , it will be worth the effort to show both these orders for the smaller values of *a*, which indeed shall be primes; and it will be useful to show not only the prime period of these numbers smaller than 4*a*, but also the following periods, by adding 4*a* continually :

1°. Let $a=2$; there will be $4a=8$.

$$\begin{array}{l} T = 1 \\ \Theta = 5 \end{array} \left| \begin{array}{l} 9 \\ 13 \end{array} \right| \left| \begin{array}{l} 17 \\ 21 \end{array} \right| \left| \begin{array}{l} 25 \\ 29 \end{array} \right| \left| \begin{array}{l} 33 \\ 37 \end{array} \right| \text{etc.}$$

2°. Let $a = 3;$ there will be $4a = 12.$

$$\begin{array}{l} T = 1 \\ \Theta = 5 \end{array} \left| \begin{array}{l} 13 \\ 17 \end{array} \right| \left| \begin{array}{l} 25 \\ 29 \end{array} \right| \left| \begin{array}{l} 49 \\ 53 \end{array} \right| \left| \begin{array}{l} 61 \\ 65 \end{array} \right| \text{etc.}$$

Since here a was 3, the squares divisible by 3 will be excluded.

3°. Let $a = 5;$ there will be $4a = 20.$

$$\begin{array}{l} T = 1,9 \\ \Theta = 13,17 \end{array} \left| \begin{array}{l} 21,29 \\ 33,37 \end{array} \right| \left| \begin{array}{l} 41,49 \\ 53,57 \end{array} \right| \left| \begin{array}{l} 61,69 \\ 73,77 \end{array} \right| \left| \begin{array}{l} 81,89 \\ 93,97 \end{array} \right| \text{etc.}$$

Here evidently from the order Θ we exclude the number 5, as equal to a itself.

4°. Let $a = 7;$ there will be $4a = 28.$

$$\begin{array}{l} T = 1,9,25 \\ \Theta = 5,13,17 \end{array} \left| \begin{array}{l} 29,37,53 \\ 33,41,45 \end{array} \right| \left| \begin{array}{l} 57,65,81 \\ 61,69,73 \end{array} \right| \text{etc.}$$

Here in the order Θ we have laid aside 21, as divisible by $a = 7.$

5°. Let $a = 11; 4a = 44.$

$$\begin{array}{l} T = 1, \quad 5, \ 9,25,37 \\ \Theta = 13,17,21,29,41 \end{array} \left| \begin{array}{l} 45,49,53,69,81 \\ 57,61,65,73,85 \end{array} \right| \left| \begin{array}{l} 89, \ 93, \ 97,113,125 \\ 101,105,109,117,129 \end{array} \right| \text{etc.}$$

6°. Let $a = 13; \ 4a = 52.$

$$\begin{array}{l} T = \ 1, 9,17,25,29,49 \\ \Theta = 5,21,33,37,41,45 \end{array} \left| \begin{array}{l} 53,61,69,77,81,101 \\ 57,73,85,89,93, \ 97 \end{array} \right| \text{etc.}$$

7°. Let $a = 17; \ 4a = 68.$

$$\begin{array}{l} T = 1, \quad 9, 13,21,25,33,49,53 \\ \Theta = 5,29,37,41,45,57,61,65 \end{array} \left| \right| \text{etc.}$$

8°. Let $a = 19 \ ; \ 4a = 76.$

$$\begin{array}{l|l} T = & 1,\ 5,\ 9,17,25,45,49,61,73 \\ \Theta = & 13,21,29,33,37,41,53,65,69 \end{array} \begin{array}{l|l} 77,81,\ 85,\ 93,101,\ 121,125,137,149 \\ 89,97,105,109,113,117,129,141,\ 145 \end{array} \text{etc.}.$$

9°. Let $a = 23;\ 4a = 92$.

$$\begin{array}{l|l} T = & 1,\ 9,\ 13,\ 25,\ 29,\ 41,\ 49,\ 73,\ 77,\ 81,\ 85 \\ \Theta = & 5,17,21,\ 33,\ 37,45,\ \ 53,\ 57,\ 61,\ 65,\ 89 \end{array} \text{etc.}$$

10°. Let $a = 29;\ 4a = 116$.

$$\begin{array}{l|l} T = & 1,\ 5,\ \ 9,\ 13,\ 25,\ 33,\ 45,\ 49,\ 53,\ 57,\ 65,\ \ 81,\ \ 93,\ 109 \\ \Theta = & 17,\ 21,\ 37,\ 41,\ 61,\ 69,\ 73,\ 77,\ 85,\ 89,\ 97,\ 101,\ 105,\ 113 \end{array} \text{etc.}$$

SCHOLIUM

29. Hence therefore from these prime numbers *a,* both the values of the letter *T,* as well as of the letter Θ become known, which thus it is fitting to understand, so that, as often as the $4as + T$ or $4as - T$ were a prime number, for example $2m+1$, then always it may be possible to show the formula to be divisible by $xx - ayy$ by $2m+1$; then truly also the formula $a^m - 1$ always will have the same divisor $2m+1$, thus so that now more of the theorems advanced above, evidently as often as *a* were a prime number, thus we may be able to enunciate succinctly, so that, whenever $4as \mp T$ were a prime number $= 2m+1$, then the formula $a^m - 1$ may admit the same divisor always; from which observed no further doubt will remain, why the numbers taken under the order Θ may not entertain a contrary property, as now thus it will be allowed to enunciate, so that, whenever the formula $4as \mp \Theta$ were a prime number $= 2m+1$, then no greater formula $a^m - 1$ may be divisible by that ; from which since $a^{2m} - 1$ shall always be divisible, it follows in this case the formula $a^m + 1$ always to become divisible by the prime number $2m+1$, and these two enunciations exhaust all the cases advanced above, for which the number *a* was prime ; but when *a* has factors, the matter is had otherwise, and it will be convenient to examine these cases in a particular way.

PROBLEM

30. *If the number a were composite, for example* $a = fg$, *to find the numbers of each kind designated by the letters T and* Θ.

SOLUTION

Therefore here all the prime divisors $2m+1$ are sought expressed by the formula $4fgs \mp T$, by which the formula $(fg)^m - 1$ shall be divisible ; that which can happen in two ways, either when these two formulas : $f^m - 1$ and $g^m - 1$ are divisible by $2m+1$, or also these two formulas: $f^m + 1$ and $g^m + 1$.
For in the first case, since there shall be

$$(fg)^m - 1 = g^m(f^m - 1) + g^m - 1$$

certainly this formula will be able to be divided by $2m+1$. Now for the prime numbers f and g with this outstanding property found above, we may represent thus, which for the sake of distinction :

$$4fgs \mp T^{(f)} \text{ and } 4gfs \mp T^{(g)};$$

which two formulas merge into one, if from the values of the letters given above $T^{(f)}$ and $T^{(g)}$ we may remove these, which are common to each. For these, if the letters T may be dealt with, certainly satisfy all the prime numbers of this form sought $4fgs \mp T$.
But in the latter case, where the formulas $f^m + 1$ and $g^m + 1$ have the divisor $2m+1$, because there is

$$(fg)^m - 1 = f^m(g^m + 1) - f^m - 1,$$

the same divisor of the formula will agree to this. But for this case above we have seen the form of the prime divisors to be

$$4fgs \mp \Theta^{(f)} \text{ and } 4gfs \mp \Theta^{(g)};$$

whereby if these may be removed from the values of the letter Θ for the numbers f and g, which by themselves are common, now these also will be required to be added to the values of the letter T ; and thus all the values of the letter T sought will be obtained, if both the numbers from the common formulas $T^{(f)}$ and $T^{(g)}$, as well as those also, which the formulas $\Theta^{(f)}$ and $\Theta^{(g)}$ have in common, may be taken together and may be extended as far as to the term $4fg = 4a$; which in the end we have continued now above the values of the letters beyond the first period. But from these found the remaining numbers of the form $4n+1$ hence will give the excluded values of the letter Θ, which

also thus are allowed to be deduced, so that from that both the common terms of the letters $T^{(f)}$ and $\Theta^{(g)}$, as well as from the common letters $T^{(g)}$ and $\Theta^{(f)}$ may be referred to.

EXAMPLE

31. Because this operation will be shown most easily by an example, let $a=15$ and thus $f=3$ and $g=5$, for which the values of the letters T and Θ for each number advanced from above are displayed. From which we will have therefore :

$$\text{For } f=3 \begin{cases} T^{(f)} = 1,\ 13,\ 25,\ 37,\ 49,\ 61. \\ \Theta^{(f)} = 5,\ 17,\ 29,\ 41,\ 53,\ 65. \end{cases}$$

$$\text{For } g=5 \begin{cases} T^{(g)} = 1,\ 9,\ 21,\ 29,\ 41,\ 49,\ 61,\ 69. \\ \Theta^{(g)} = 13,\ 17,\ 33,\ 37,\ 53,\ 57,\ 73,\ 77, \end{cases}$$

which values we have continued beyond the term $4a = 4fg = 60$.

Now the letters $T^{(f)}$ and $T^{(g)}$ have the same common terms : 1, 49, moreover the terms $\Theta^{(f)}$ and $\Theta^{(g)}$ have these common terms: 17, 53, which numbers taken together present the values of the letters T for this case. But for the letter Θ the first common terms may be taken from the letters $T^{(f)}$ and $\Theta^{(g)}$, which are 13, 37; then truly also the common numbers from the letters $T^{(g)}$ and $\Theta^{(f)}$, which are 29, 41. Consequently for the proposed case $a=15$ the values of the letters T and Θ for the first period to be continued as far as $4a=60$, will be :

$$T = \ 1,\ 17,\ 49,\ 53.$$
$$\Theta = 13,\ 29,\ 37,\ 41.$$

Here clearly all the numbers of the form $4n+1$ which occur, indeed are prime to 15 ; and being attended to lightly it is apparent just as many terms always appear in each order T and Θ.

SCHOLIUM

32. So that this latter observation may be understood better, thus an uncommon rule may be noted, which shows, how many numbers occur from unity to the given number N, where indeed it is apparent at once, if N itself were a prime number, then all the preceding numbers, of which the amount is $N-1$, likewise also for that to be prime; but if N were some composite number, it can be represented always in this general form

$$N = a^{\alpha} \cdot b^{\beta} \cdot c^{\gamma} \cdot d^{\delta} \ldots\ldots,,$$

where *a, b, c* etc. denote prime numbers; but then the amount of the primes numbers for *N* and which themselves will be smaller than *N* will be

$$(a-1)a^{\alpha-1}\cdot(b-1)b^{\beta-1}\cdot(c-1)c^{\gamma-1}.....$$

Now since in our case there shall be $N=60=2^2\cdot 3^1\cdot 5^1$, the smallest amount of numbers prime to *N*

$$=1.2.\ 2.\ 4=16,$$

which since all shall be odd and as many of the form $4n+1$ as of the form $4n-1$, only 8 will be present of our form $4n+1$, of which half refer to the letter *T,* the rest truly to the letter Θ. Therefore we may use this rule found for the numbers *T* and Θ for the more simple numbers *a* being established from two constant prime numbers :

1^{o}. Let $a=2\cdot 3;\ 4a=24$.

$T=1,\ 5$	$25,29$	$49,53$	$73,77.$
$\Theta=13,17$	$37,\ 41$	$61,\ 65$	$85,\ 89.$

2^{o}. Let $a=2\cdot 5\ ;\ 4a=40.$

$T=\ 1,\ 9,13,37$	$41,49,53,77.$
$\Theta=17,21,29,33$	$57,61,69,73.$

3^{o}. Let $a=2\cdot 7\ ;4a=56$.

$T=1,\ \ 5,\ 9,13,25,45$	$57,\ 61,\ 65,\ 69,\ 81,\ 101.$
$\Theta=17,29,33,37,41,53$	$73,\ 85,\ 89,\ 93,\ 97,\ 109.$

4^{o}. Let $a=2\cdot 11;4a=88$.

$T=1,\ \ 9,\ 13,\ \ 21,\ 25,\ 29,\ 49,\ 61,\ 81,\ 85.$
$\Theta=5,\ 17,\ 37,\ 41,\ 45,\ 53,\ 57,\ 65,\ 69,\ 73.$

5^{o}. Let $a=2\cdot 13;\ 4a=104$.

$T=\ \ 1,\ 5,\ \ 9,\ 17,\ 21,\ 25,\ 37,\ 45,\ 49,\ 81,\ 85,\ \ 93.$
$\Theta=29,\ 33,\ 41,\ 53,\ 57,\ 61,\ 69,\ 73,\ 77,\ 89,\ 97,\ 101.$

6^{o}. Let $a=3\cdot 5;\ 4a=60$.

$T =$ 1, 17, 49, 53.
$\Theta = 13,\ 29,\ 37,\ 41.$

7^{o}. Let $a = 3 \cdot 7;\ 4a = 84$.

$T =$ 1, 5, 17, 25, 37, 41.
$\Theta = 13,\ 29,\ 53,\ 61,\ 65,\ 73.$

PROBLEM

33. *If a were some composite number, to find the values of the letters T and Θ, which agree with that.*

SOLUTION

Initially it may be noted, if a were a square, for example ff, because for the two factors f and f both the letters T as well as Θ are equal to each other, clearly numbers of the form $4m+1$, in as much as they are prime to f, are required to be referred to the order T, thus so that the order Θ evidently may be left empty, which the nature of the matter evidently demands. For since there shall be $a = ff$, and thus $a^m = f^{2m}$, the formula $f^{2m} - 1$ is divisible always by the prime number $2m+1$, and thus the form $a^m + 1$ never allows a divisor. Then if there were $a = ffg$, since all the numbers for ff occur in the order T, truly none in Θ, it is evident for this case all the numbers in the same order enter T, which are found for the simple number g ; and neither besides truly from both does any besides enter Θ, truly these numbers must be omitted, which are not prime to ff. Finally if a were a product from more prime numbers, such as $a = fghk$; numbers are sought for the factors fg and hk being referred to the orders T and Θ, from which henceforth the values of these letters may be concluded thence for the number f, as in the preceding problem.

EXAMPLE

34. Let $a = 30 = 2 \cdot 3 \cdot 5$, and thus $4a = 120$; initially the letters T and Θ may be taken for the number $3 \cdot 5 = 15$, which may be continued just as far as to 120, which are :

$$\text{for } 3 \cdot 5 \begin{cases} T = 1,\ 17,\ 49,\ 53,\ 61,\ 77,\ 109,\ 113. \\ \Theta = 13,\ 29,\ 37,\ 41,\ 73,\ 89,\ 97,\ 101. \end{cases}$$

Since from these both forms may be prepared corresponding to the factor 2, and for each the common T are found

1, 17, 49, 113,

but the common terms of each of the letters Θ are

$$13,\ 29,\ 37,\ 101,$$

on account of which the orders sought T and Θ for the number $a = 30$ are:

$$T = \ 1,\ 13,\ 17,\ 29,\ 37, 49,\ 101,\ 113 \text{ etc.}$$
$$\Theta = 41,\ 53,\ 61,\ 73,\ 77,\ 89,\ \ 97,\ 109 \text{ etc.}$$

SCHOLIUM

35. Now we may gather together everything found thus far, and we may show for all the numbers *a,* with squares themselves excepted, as far as to the form 30 in the order of the prime numbers $2m+1$, by which either $a^m - 1$ or $a^m + 1$ shall be divisible:

a.	$2m+1$	$a^m \mp 1$
2.	$8s \mp 1,$	$2^m - 1.$
	$8s \mp 5,$	$2^m + 1.$
3.	$12s \mp 1,$	$3^m - 1.$
	$12s \mp 5,$	$3^m + 1.$
5.	$20s \mp 1,9.$	$5^m - 1.$
	$20s \mp 13,17,$	$5^m + 1.$
6.	$24s \mp 1,5,$	$6^m - 1.$
	$24s \mp 13,17,$	$6^m + 1.$
7.	$28s \mp 1,\ 9,25,$	$7^m - 1.$
	$28s \mp 5,13,17,$	$7^m + 1.$
8.	$32s \mp 1,\ 9,17,25,$	$8^m - 1.$
	$32s \mp 5,13,21,29,$	$8^m + 1.$
10.	$40s \mp 1,\ 9,13,37,$	$10^m - 1.$
	$40s \mp 17,21,29,33,$	$10^m + 1.$
11.	$44s \mp 1,\ \ 5,\ 9,\ 13,37,$	$11^m - 1.$
	$44s \mp 13,17,21,29,41,$	$11^m + 1.$
12.	$48s \mp 1,13,25,\ 37,$	$12^m - 1.$
	$48s \mp 5,17,29,41,$	$12^m + 1.$

13.	$52s \mp 1,\ 9,17,25,29,49,$ $52s \mp 5,21,33,37,41,45,$	$13^m - 1.$ $13^m + 1.$
14.	$56s \mp\ 1,\ 5,\ 9,13,25,45,$ $56s \mp 17,29,33,37,41,53,$	$14^m - 1.$ $14^m + 1.$
15.	$60s \mp\ 1,17,49,53,$ $60s \mp 13,29,37,41,$	$15^m - 1.$ $15^m + 1.$
17.	$68s \mp 1,\ 9,\ 13,21,25,33,49,53,$ $68s \mp 5,29,37,41,45,57,61,65,$	$17^m - 1.$ $17^m + 1.$
18.	$72s \mp 1,17,25,41,49,65,$ $72s \mp 5,13,29,37,53,61,$	$18^m - 1.$ $18^m + 1.$
19.	$76s \mp\ 1,\ 5,\ 9,17,25,45,49,61,73,$ $76s \mp 13,21,29,33,37,41,53,65,69,$	$19^m - 1.$ $19^m + 1.$
20.	$80s \mp\ 1,\ 9,21,29,41,49,61,69,$ $80s \mp 13,17,33,37,53,57,73,77,$	$20^m - 1.$ $20^m + 1.$
21.	$84s \mp\ 1,\ 5,17,25,37,41,$ $84s \mp 13,29,53,61,65,73,$	$21^m - 1.$ $21^m + 1.$
22.	$88s \mp 1,\ 9,\ 13,\ 21,25,29,49,61,81,85,$ $88s \mp 5,17,37,41,45,53,57,65,69,73,$	$22^m - 1.$ $22^m + 1.$
23.	$92s \mp 1,\ 9,\ 13,25,29,41,49,73,77,81,85,$ $92s \mp 5,17,21,33,37,45,53,\ 57,61,65,89,$	$23^m - 1.$ $23^m + 1.$
24.	$96s \mp\ 1,\ 5,25,29,49,53,73,77,$ $96s \mp 13,17,37,41,61,65,85,89,$	$24^m - 1.$ $24^m + 1.$
26.	$104s \mp\ 1,\ 5,\ 9,17,21,25,37,45,49,81,85,\ 93,$ $104s \mp 29,33,41,53,57,61,69,73,77,89,97,101,$	$26^m - 1.$ $26^m + 1.$
27.	$108s \mp 1,13,25,37,49,61,73,85,\ 97,$ $108s \mp 5,17,29,41,53,65,77,89,101,$	$27^m - 1.$ $27^m + 1.$
28.	$112s \mp 1,\ 9,25,29,37,53,57,65,81,85,93,109$ $112s \mp 5,13,17,33,41,45,61,69,73,89,97,101,$	$28^m - 1.$ $28^m + 1.$
29.	$116s \mp\ 1,\ 5,\ 9,13,25,33,45,49,53,57,65,\ 81,\ 93,109,$ $116s \mp 17,21,37,41,61,69,73,77,85,89,97,101,105,113.$	$29^m - 1.$ $29^m + 1.$
30.	$120s \mp\ 1,13,17,29,37,49,101,113,$ $120s \mp 41,53,61,73,77,89,\ \ 97,109,$	$30^m - 1.$ $30^m + 1.$

Therefore now everything, which were examined before, is allowed to be seen clear enough and nothing other may be considered to be present, so that these two conclusions deduced from observations maybe strengthened by rigorous demonstrations.

For after some number *a,* whether prime or composite, the values of the letters *T* and Θ were found, the following two noteworthy theorems may be noteworthy:

I. *All the prime divisors of the form* $xx - ayy$ *may be expressed in one or other of these forms :* $4as + T$, *or* $4as - T$.

II. *All the prime divisors of this form :* $xx + ayy$ *may be expressed in one or other of these formulas:* $4as + T$ *or* $4as - \Theta$.

But it is apparent at once for the numbers *x* and *y* of this kind must be assumed, so that the two terms *xx* and *ayy* may have no common factors.

DE QUIBUSDAM EXIMIIS PROPRIETATIBUS CIRCA DIVISORES POTESTATUM OCCURRENTIBUS

Commentatio 557 indicis ENESTROEMIANI

Opuscula. analytica 1, 1783, p. 242-295

[Conventui exhibita. die 25. januarii 1773]

l. Constat omnes progressiones geometricas, veluti 1, a, a^2, a^3, a^4 etc., ita esse comparatas, ut, dum singuli termini per numerum quemcunque *N,* qui ad *a* sit primus, dividuntur, residua post certum intervallum iterum eodem ordine revertantur; et quia primum residuum est unitas, semper dabitur eiusmodi potestas a^n, quae per *N* divisa iterum relinquat unitatem; sequentes vero potestates a^{n+1}, a^{n+2}, a^{n+3} etc. eadem residua praebebunt, quae ex terminis a, a^2, a^3 etc. sunt nata. Deinde etiam demonstratum est, si *N* fuerit numerus primus, tum semper potestatem a^{N-1} iterum pro residuo unitatem exhibere. Saepenumero autem ista potestas a^{N-1} minima est, quae per *N* divisa unitatem relinquit; interdum vero etiam usu venit, ut minor potestas a^n idem praestet; tum autem semper *n* est pars aliquota exponentis $N-1$; atque hinc nascitur quaestio attentione nostra non indigna:

Quaenam pro quovis divisore N sit minima potestas a^n, ex qua residuum oriatur $=1$?

Atque hinc quaestio alia latius patens proponi potest:

Quaenam sit infima potestas a^n, quae per datum numerum N divisa datum relinquat residuum r?

Quae quaestio huc redit, ut exhibeatur minima formula $a^x - r$, quae per datum numerum *N* fuerit divisibilis. Quin etiam quaestio adhuc generalius proponi potest, ut *investigetur exponens x, quo haec formula* $fa^x + g$ *reddatur divisibilis per datum numerum N.*

2. Solutio huius Problematis imprimis requiritur ad numeros perfectos investigandos. Cum enim forma horum numerorum sit $2^{n-1}(2^n - 1)$, quoties $2^n - 1$ fuerit numerus primus, statim evidens est hoc evenire non posse, nisi ipse exponens *n* fuerit numerus

primus; quandoquidem huiusmodi forma $2^{\alpha\beta}-1$ semper habet divisores $2^{\alpha}-1$ et $2^{\beta}-1$. Neque vero vicissim sequitur, quoties *n* fuerit numerus primus, tum etiam formulam $2^{n}-1$ fore numerum primum. Plures enim casus iam sunt explorati, quibus hoc non evenit; veluti si fuerit $n=11,\ n=23;$ item $n=29,\ n=37$; ac praeterea sine dubio pluribus aliis casibus, quos omnes nondum explorare licuit. Alia autem via non patet ad hos casus investigandos praeter eam, qua olim sum usus, quae ita se habebat: Fingatur formulae $2^{n}-1$ divisor, si quem habet, esse numerus primus $2p+1$; et cum formula $2^{2p}-1$ semper divisorem habeat $2p+1$, sequitur hoc fieri non posse, nisi *n* fuerit pars aliquota ipsius 2*p,* sive 2*p* multiplum ipsius *n.* Sumto ergo $p=\lambda n$, fiet divisor $2\lambda n+1$; ex quo concluditur, si formula $2^{n}-1$ non sit numerus primus, eam alios divisores certe habere non posse, nisi qui in forma $2\lambda n+1$ contineantur; atque hoc principio olim sum usus in investigatione numerorum primorum. Simili modo cum olim assertionem FERMATII examinassem, qua asseverarat, formulam $2^{n}+1$ semper esse numerum primum, quoties exponens *n* fuerit ipse potestas binarii, quaestionem supra memoratam in subsidium vocare sum coactus, qua post plures calculos tandem inveni formulam $2^{32}+1$ divisorem habere 641; ex quo nunc quaestio formari potest: quaenam sit binarii potestas infima, quae unitate aucta fiat per 641 divisibilis ? Methodus quidem, qua olim sum usus, per calculos satis taediosos procedebat; nunc autem se mihi obtulit alia methodus multo simplicior et expeditior non solum hos memoratos casus circa potestates binarii resolvendi, sed quae adeo ad quaestionem illam generalissimam adplicari possit, qua scilicet quaeritur infima potestas a^{x}, ut formula $fa^{x}+g$ per datum numerum *N* fiat divisibilis. Hanc ergo novam methodum hic breviter sum expositurus; hunc autem in finem sequentia Lemmata sunt praemittenda:

LEMMA 1

3. Si numerus quicunque *A* per alium *N* divisus relinquat residuum *r,* tum etiam omnes hi numeri: $r\mp N,\ r\mp 2N,\ r\mp 3N$ et in genere $r\mp\lambda N$, aeque tanquam residua spectari possunt, quandoquidem hae ipsae formulae per *N* divisae relinquunt *r.*

LEMMA 2

4. Si numerus *A* per divisorem *N* divisus relinquat residuum *a,* numerus vero *B* per eundem divisus residuum *b,* tum productum *AB* per *N* divisum relinquet residuum *ab.* Hinc ergo potestates $A^{2},\ A^{3},\ A^{4}$ etc. dabunt residua $a^{2},\ a^{3}, a^{4}$ etc., quae pro lubitu, divisione per *N* facta, ad minimos valores reducere licet.

LEMMA 3

5. Si proposito divisore N potestas a^x residuum $\det = r$, potestas vero a^y residuum $= s$, tum potestas a^{x+y} residuum dabit $= rs$; unde etiam hae potestates a^{2x}, a^{3x}, a^{4x} etc. residua producent r^2, r^3, r^4 etc.

LEMMA 4

6. Si ut ante pro divisore N potestas a^x praebeat residuum r, potestas vero a^y residuum s, hinc etiam assignari poterit residuum respondens potestati a^{x-y}, quod quidem foret $= \frac{r}{s}$ per s dividi posset. Quia autem loco r sumere licet $r \mp \lambda N$, semper λ ita definiri poterit, ut haec forma $r \mp \lambda N$ per s dividi queat, ac tum quotus dabit ipsum residuum potestati a^{x-y} respondens.

LEMMA 5

7. Si pro divisore N potestas a^x relinquat r, fiatque $r \mp \lambda N = a^\alpha s$, ita ut $a^\alpha s$ tanquam residuum spectari possit, tum potestas $a^{x-\alpha}$ residuum relinquet s, quandoquidem dividendum et residuum semper per communem divisorem deprimere licet.

PROBLEMA GENERALE

8. *Proposita formula $fa^x + g$, invenire minimum exponentem x, quo haec formula per datum numerum N fiat divisibilis, siquidem id fuerit possibile.*

SOLUTIO

Quaestio ergo huc reducitur, ut forma fa^x per numerum datum N divisa relinquat residuum $= -g$. Quia nunc per Lemma primum pro residuo etiam haberi potest $-g \mp \lambda N$, facile λ ita assumere licebit, ut haec formula factorem obtineat a, vel adeo eius altiorem potestatem a^α. Sit igitur $-g \mp \lambda N = a^\alpha r$, atque per Lemma postremum quantitas $fa^{x-\alpha}$ per N divisa residuum relinquet $= r$. Iam simili modo fiat $r \mp \lambda N = a^\beta s$, et quantitas $fa^{x-\alpha-\beta}$ dabit residuum s, sicque ulterius progredi licebit, sumendo $s \mp \lambda N = a^\gamma t$; tum vero etiam $t \mp \lambda N = a^\delta u$; porro $u \mp \lambda N = a^\varepsilon v$ etc. ; quo pacto quantitas $a^{x-\alpha-\beta-\gamma-\varepsilon}$ per N divisa residuum relinquet $= v$; haeque operationes eousque

continuentur, donec perveniatur ad residuum $= f$; ita ut haec quantitas $fa^{x-\alpha-\beta-\gamma-\text{etc.}}$ residuum det $= f$; id quod semper continget, siquidem quaestio fuerit possibilis; atque hoc adeo antequam numeri ab exponente subtrahendi $\alpha+\beta+\gamma+\delta+\varepsilon+\text{etc.}$ superent numerum $N-1$, quia si exponentes ipsius *a* ultra hunc limitem continuentur, eadem residua recurrunt. Cum autem ad talem casum fuerit perventum, quo residuum est *f,* quia hoc evenit, si exponens ipsius *a* fuerit $=0$, hinc concludemus $x=\alpha+\beta+\gamma+\delta+\text{etc.}$ Omnes ergo has operationes ita succincte repraesentasse iuvabit:

$$\begin{aligned}
-g \mp \lambda N &= a^{\alpha} r \\
r \mp \lambda N &= a^{\beta} s \\
s \mp \lambda N &= a^{\gamma} t \\
t \mp \lambda N &= a^{\delta} u \\
&\cdots\cdots\cdots \\
z \mp \lambda N &= a^{\zeta} f
\end{aligned}$$

hincque deducitur conclusio $x=\alpha+\beta+\gamma+\delta+\cdots+\zeta$. Sin autem nunquam perveniatur ad tale residuum *f,* antequam summa $x=\alpha+\beta+\gamma+\delta+\cdots$ usque ad $N-1$ ascendat, Problema pro impossibili est habendum.

Quanquam hae operationes expedite instituuntur, tamen eas saepenumero haud mediocriter contrahere licebit, praecipue si perventum fuerit ad exiguum residuum, puta *t,* respondens formulae $fa^{x-\delta}$, ponendo $\delta=\alpha+\beta+\gamma$; tum enim eius quadratum t^2 respondebit formulae $f^2a^{2x-2\delta}$, quae per primam dividatur, ut formula $fa^{x-2\delta}$ respondeat residuo $\frac{t^2}{-g}$, quod si non fuerit numerus integer, loco t^2 scribendo $t^2 \mp \lambda N$ facile eo reducitur. Quin etiam cubus residui t^3 respondebit formulae $f^3a^{3x-3\delta}$, quae per quadratum primae divisa dabit formulae $fa^{x-3\delta}$ residuum $\frac{t^3}{g^2}$. Quin etiam binas formulas diversas *g* in se invicem ducere licebit, et per primam dividendo iterum ad novam huiusmodi formulam pervenietur. Imprimis autem hoc compendium maximum usum praestabit, ubi ad residua satis parva fuerit perventum; quorum potestates etiam superiores facile capiuntur, atque insuper fuerit primum residuum $-g$ numerus satis parvus vel adeo unitas.

COROLLARIUM

9. Quoniam has operationes clare descripsimus, eas adplicemus ad casus magis speciales. Ac primo quidem occurrit formula $2^x \mp 1$. Pro variis igitur divisoribus quaeramus exponentem *x,* ut potestas 2^x residuum relinquat ∓ 1. Sufficiet autem hoc

residuum $+1$ statuisse; si enim 2^x fuerit minima potestas residuum dans $=+1$, tum potestas $2^{\frac{1}{2}x}$ necessario dabit residuum $=-1$, siquidem x fuerit numerus par; sin autem x fuerit impar,
hic casus plane est impossibilis.

EXEMPLUM 1

10. Quaeratur minima potestas 2^x, quae per 23 divisa relinquat 1, sive ut 2^x-1 divisibilis fiat per 23. Hic igitur est $N=23,\ a=2$ et primum residuum $=1$; unde operationes nostrae sequenti modo procedent:

$$+1+23=+24=+\,2^3\cdot 3$$
$$+3-23=-20=-2^2\cdot 5$$
$$-5-23=-28=-2^2\cdot 7$$
$$-7+23=+16=+\,2^4\cdot 1.$$

Sic iam perventum est ad residuum optatum $+1$ ob $f=1$; sicque concludimus $x=11$. Cum ergo formula $2^{11}-1$ sit divisibilis per 23 et 11 numerus impar, nulla plane datur formula 2^x+1 per 23 divisibilis.

EXEMPLUM 2

11. Proponatur divisor 41, per quem formula 2^x-1 reddi debeat divisibilis. Ergo ob $N=41,\ a=2,\ f=1$ et primum residuum $=1$, habebimus:

$$+1-41=-40=-2^3\cdot 5$$
$$-5+41=+36=+\,2^2\cdot 9$$
$$+9-41=-32=-2^5\cdot 1.$$

Hic iam subsistere possumus; cum enim potestas 2^{x-10} relinquat -1, eius quadratum 2^{2x-20} relinquet $+1$, et per primam formam dividendo prodit 2^{x-20} pro residuo $+1$ optato; sicque habemus $x=20$. Simul autem hinc patet potestati 2^{10} residuum convenire -1, ita ut formulae simplicissimae per 41 divisibiles sint $2^{10}+1$ et $2^{20}-1$.

EXEMPLUM 3

12. Pro divisore 73 quaeratur formula simplicissima $2^x \mp 1$ per eum divisibilis. Hic est $N = 73,\ a = 2$ et sumto primo residuo $= +1$ fiet

$$+1 - 73 = -72 = -2^3 \cdot 9$$
$$-9 + 73 = +64 = +2^6 \cdot 1,$$

ubi ergo iam subsistere licet, eritque $x = 9$, unde formula $2^9 - 1$ per 73 est divisibilis; et quia 9 est numerus impar, nulla plane datur formula $2^x + 1$ per eundem numerum *N* divisibilis.

EXEMPLUM 4

13. Proponatur divisor $N = 77$, et sumto prima residuo $= 1$, calculus ita se habebit:

$$+\ 1 - 77 = -\ 76 = -2^2 \cdot 19$$
$$-19 - 77 = -\ 96 = -2^5 \cdot\ 3$$
$$-\ 3 - 77 = -\ 80 = -2^4 \cdot 5$$
$$-\ 5 + 77 = +\ 72 = +2^3 \cdot 9$$
$$+\ 9 - 77 = -\ 68 = -2^2 \cdot 17$$
$$-17 + 77 = +\ 60 = +2^2 \cdot 15$$
$$+15 + 77 = +\ 92 = +2^2 \cdot 23$$
$$+23 + 77 = +100 = +2^2 \cdot 25$$
$$+25 - 77 = -\ 52 = -2^2 \cdot 13$$
$$-13 + 77 = +\ 64 = +2^6 \cdot\ \ 1,$$

unde $x = 30$; ita ut $2^{30} - 1$ sit simplicissima forma per 77 divisibilis. Hinc tamen non sequitur istam $2^{15} + 1$ divisibilem esse per 77, propterea quod 77 non est numerus primus; etsi enim $2^{30} - 1$ divisibile est per 77, neutiquam sequitur alterutrum eius factorum $2^{15} + 1$ sive $2^{15} - 1$ divisibilem esse debere, quemadmodum rite concludere liceret, si divisor esset numerus primus; hoc enim casu fieri potest, ut alter factor per 7, alter vero per 11 sit divisibilis; ac revera, cum $2^5 + 1$ per 11 sit divisibile, etiam $2^{15} + 1$ per 11 erit divisibile; at vero per 7 divisibilis est altera formula $2^{15} - 1$, quia factorem habet $2^3 - 1 = 7$.

EXEMPLUM 5

14. Sit divisor $N = 89$, et sumto iterum prima residuo $= 1$, faciemus:

$$+\ 1-89=-\ 88=-2^3\cdot 11$$
$$-11-89=-100=-2^2\cdot 25$$
$$-25+89=+\ 64=+2^6\cdot 1.$$

Hinc ergo $x=11$, sicque formula $2^{11}-1$ divisorem habet 89; nulla autem datur formula alterius speciei $2^{11}+1$.

EXEMPLUM 6

15. Sit divisor $N=105$, eritque:

$$+\ 1-105=-104=-\ 2^3\cdot 13$$
$$-13+105=+\ \ 92=+\ 2^2\cdot 23$$
$$+23+105=+128=+\ 2^7\cdot 1.$$

Summa exponentium $=12$; ergo $x=12$, et formula $2^{12}-1$ divisibilis erit per 105. At quia 105 non est numerus primus, non sequitur fore 2^6+1 per 105 divisibile. Tantum enim dividi potest per 5, dum altera formula 2^6-1 divisibilis est per $3\cdot 7$.

EXEMPLUM 7

16. Sit $N=\ 223$ et primum residuum $=1$, fiet:

	Summae exponentium
$+\ 1+223=+224=+2^5\cdot\ 7$	5
$+\ 7-223=-216=-2^3\cdot 27$	8
$-27+223=+196=+2^2\cdot 49$	10
$+49+223=+272=+2^4\cdot 17$	14
$+17+223=+240=+2^4\cdot 15$	18
$+15-223=-208=-2^4\cdot 13$	22
$-13-223=-236=-2^2\cdot 59$	24
$-59+223=+164=+2^2\cdot 41$	26
$+41+223=+264=+2^3\cdot 33$	29
$+33+223=+256=+\ 2^8\cdot 1$	37

Summa exponentium $=37$, ergo $x=37$, et formula $2^{37}-1$ divisibilis per 223.

Hinc quia 37 est numerus impar, certum est nullam dari formulam $2^x + 1$ per 223 divisibilem.

17. Quo nunc pateat, quomodo hae operationes possint sublevari, subsistamus iam in quinta, ubi residuum prodiit 15 et summa exponentium $= 18$; unde haec potestas 2^{x-18} residuum dat 15. Sumantur quadrata, et potestas 2^{2x-36} residuum dat 225 sive 2; haec iam per primam divisa praebet pro potestate 2^{x-18} residuum $2 = 2^1 \cdot 1$, ergo potestas 2^{x-37} praebet residuum 1, unde iam liquet esse $x = 37$.

EXEMPLUM 8

18. Sit $N = 641$ et primum residuum $= 1$, fiet:

	Summae exponentium
$+1-641 = -640 = -2^7 \cdot 5$	7
$-5+641 = +636 = +2^2 \cdot 159$	9
$+159+641 = +800 = +2^5 \cdot 25$	14
$+25-641 = -616 = -2^3 \cdot 77$	17
$-77+641 = +564 = +2^2 \cdot 141$	19
$+141-641 = -500 = -2^2 \cdot 125$	21
$-125+641 = +516 = +2^2 \cdot 129$	23
$+129-641 = -512 = -2^9 \cdot 1$	32

ubi iam subsistere possumus. Quia enim residuum est -1, si pro primo residuo sumsissemus -1, ut formula quaereretur $2^x + 1$ per 641 divisibilis, omnia sequentia residua signo contrario adfecta prodiissent et ultimum fuisset $+1$; unde rite concludimus esse $x = 32$, ita ut iam formula $2^{32} + 1$ sit divisibilis per 641. Evidens autem est pro minima formula huius formae $2^x - 1$ fore $x = 64$.

19. Hunc autem laborem mirifice contrahere licet. Statim enim post primam operationem subsistere possemus, quae pro potestate 2^{x-7} praebet residuum -5. Sumamus statim potestatem quartam, et pro 2^{4x-28} habebimus residuum 625, sive $-16 = -2^4 \cdot 1$, ita ut 2^{4x-32} conveniat residuum -1. Dividendo igitur per cubum primae, seu 2^{3x}, cuius residuum itidem est 1, etiam huius potestatis 2^{x-32} residuum erit -1, id quod ante
per ambages eruimus.

EXEMPLUM 9

20. Sit $N = 385 = 5 \cdot 7 \cdot 11$ et primum residuum $= 1$, erit:

	Summae exponentium
$+ \quad 1 - 385 = -384 = -2^7 \cdot 3$	7
$- \quad 3 - 385 = -388 \ -2^2 \cdot 97$	9
$- 97 + 385 = + 288 = +2^5 \cdot 9$	14
$+ \quad 9 - 385 = -376 = -2^3 \cdot 47$	17
$- 47 - 385 = -432 = -2^4 \cdot 27$	21
$- 27 - 385 = -412 = -2^2 \cdot 103$	23
$-103 - 385 = -488 = - \ 2^3 \cdot 61$	26
$- 61 + 385 = +324 = + \ 2^2 \cdot 81$	28
$+ 81 - 385 = -304 = -2^4 \cdot 19$	32
$- 19 - 385 = -404 = -2^2 \cdot 101$	34
$-101 + 385 = +284 = + \ 2^2 \cdot 71$	36
$+71 + 385 = +456 = + \ 2^3 \cdot 57$	39
$+57 - 385 = -328 = - \ 2^3 \cdot 41$	42
$-41 + 385 = +344 = + \ 2^3 \cdot 43$	45
$+43 + 385 = +428 = +2^2 \cdot 107$	47
$+107 + 385 = +492 = +2^2 \cdot 123$	49
$+123 + 385 = +508 = + \ 2^2 \cdot 127$	51
$+127 + 385 = +512 = + \ 2^9 \cdot 1$	60

ergo $x = 60$, ita ut formula $2^{60} - 1$ divisibilis sit per 385, quod etiam inde concludi potuisset, quod divisoris nostri factores sunt 5, 7, 11, quorum primus 5 est divisor formulae $2^2 + 1$, secundus 7 est formulae $2^3 - 1$, tertius 11 est formulae $2^5 + 1$; at formula per has tres divisibilis simplicior non datur quam $2^{60} - 1$.

21. Videamus nunc, quomodo hae operationes contrahi potuissent. Tertia operatione prodiit potestas 2^{x-14} residuum dans 9 ; unde eius quadratum 2^{2x-28} residuum praebet 81 ; cubus autem 2^{3x-42} praebet residuum 729, sive 344, sive -41 ; hinc quarta potestas 2^{4x-60} dabit residuum -369, sive $+16 = 2^4 \cdot 1$, ergo per 2^4 dividendo potestas 2^{4x-60}

dat residuum $+1$ et dividendo per 2^{3x}, cuius residuum etiam est $+1$, potestas 2^{x-60} residuum dabit $+1$, uti modo invenimus.

EXEMPLUM 10

Sit $N = 311$, fietque:

	Summae exponentium
$+ \quad 1 + 311 = +312 = +2^3 \cdot 39$	3
$+ \ 39 - 311 = -272 = -2^4 \cdot 17$	7
$- \ 17 - 311 = -328 = -2^3 \cdot 41$	10
$- \ 41 - 311 = -352 = -2^5 \cdot 11$	15
$- \ 11 + 311 = +300 = +2^2 \cdot 75$	17
$+ \ 75 - 311 = -236 = -2^2 \cdot 59$	19
$- \ 59 + 311 = +252 = +\ 2^2 \cdot 63$	21
$+ \ 63 - 311 = -\ 248 = -2^3 \cdot 31$	24
$- \ 31 + 311 = +280 = +2^3 \cdot 35$	27
$+ \ 35 - 311 = -276 = -2^2 \cdot 69$	29
$- \ 69 - 311 = -380 = -2^2 \cdot 95$	31
$- \ 95 + 311 = +216 = +2^3 \cdot 27$	34
$+ \ 27 - 311 = -284 = -2^2 \cdot 71$	36
$- \ 71 + 311 = +240 = +2^4 \cdot 15$	40
$+ \ 15 - 311 = -296 = -2^3 \cdot 37$	43
$- \ 37 - 311 = -348 = -2^2 \cdot 87$	45
$- \ 87 + 311 = +224 = +2^5 \cdot \ 7$	50
$+ \quad 7 - 311 = -304 = -2^4 \cdot 19$	54
$- \ 19 + 311 = +292 = +2^2 \cdot 73$	56
$+ \ 73 + 311 = +384 = +2^7 \cdot \ 3$	63
$+ \quad 3 - 311 = -308 = -2^2 \cdot 77$	65
$- \ 77 - 311 = -388 = -2^2 \cdot 97$	67
$- \ 97 - 311 = -408 = -2^3 \cdot 51$	70
$- \ 51 + 311 = +260 = +2^2 \cdot 65$	72
$+ \ 65 + 311 = +376 = +2^3 \cdot 47$	75
$+ \ 47 - 311 = -264 = -2^3 \cdot 33$	78
$- \ 33 - 311 = -344 = -2^3 \cdot 43$	81
$- \ 43 + 311 = +268 = +2^2 \cdot 67$	83
$+ \ 67 - 311 = -244 = -2^2 \cdot 61$	85

$$-61-311=-372=-2^2\cdot 93 \qquad 87$$
$$-93-311=-404=-2^2\cdot 101 \qquad 89$$
$$-101-311=-412=-2^2\cdot 103 \qquad 91$$
$$-103+311=+208=+2^4\cdot 13 \qquad 95$$
$$+13+311=+324=+2^2\cdot 81 \qquad 97$$
$$+81+311=+392=+2^3\cdot 49 \qquad 100$$
$$+49+311=+360=+2^3\cdot 45 \qquad 103$$
$$+45+311=+356=-2^2\cdot 89 \qquad 105$$
$$+89+311=+400=+2^4\cdot 25 \qquad 109$$
$$+25+311=+336=+2^4\cdot 21 \qquad 113$$
$$+21+311=+332=+2^2\cdot 83 \qquad 115$$
$$+83-311=-228=-2^2\cdot 57 \qquad 117$$
$$-57-311=-368=-2^4\cdot 23 \qquad 121$$
$$-23+311=+288=+2^5\cdot 9 \qquad 126$$
$$+9+311=+320=+2^6\cdot 5 \qquad 132$$
$$+5+311=+316=+2^2\cdot 79 \qquad 134$$
$$+79-311=-232=-2^3\cdot 29 \qquad 137$$
$$-29-311=-340=-2^2\cdot 85 \qquad 139$$
$$-85-311=-396=-2^2\cdot 99 \qquad 141$$
$$-99+311=+212=+2^2\cdot 53 \qquad 143$$
$$+53+311=+364=+2^2\cdot 91 \qquad 145$$
$$+91-311=-220=-2^2\cdot 55 \qquad 147$$
$$-55+311=+256=+2^8\cdot 1 \qquad 155$$

ergo $x=155$, sicque minima formula per 311 divisibilis est $2^{155}-1$. Si substitissemus in 25ta operatione, habuissemus 2^{x-75}, eiusque residuum 47 ; et sumtis quadratis 2^{2x-150}, sive per principalem dividendo, 2^{x-150} cum residuo 2209, sive $32=2^5\cdot 1$; unde potestas 2^{x-155} residuum optatum producit $+1$. Sin autem in operatione 17ma substitissemus, habuissemus 2^{x-50} cum residuo 7, sumtisque cubis 2^{3x-150} cum residuo 343, sive $32=2^5\cdot 1$; ita ut iam potestas 2^{3x-155}, sive etiam 2^{2x-155} residuum det $+1$; unde sequitur $x=155$, ut ante.

EXEMPLUM 11

23. Sit divisor $N = 233$, et sumto primo residuo $= 1$, faciemus:

	Summae exponentium
$+ \ 1 - 233 = -232 = -2^3 \cdot 29$	3
$-29 + 233 = +204 = +2^2 \cdot 51$	5
$+51 + 233 = +284 = +2^2 \cdot 71$	7
$+71 + 233 = +304 = +2^4 \cdot 19$	11
$+19 + 233 = +252 = +2^2 \cdot 63$	13
$+63 + 233 = +296 = +2^3 \cdot 37$	16
$+37 - 233 = -196 = -2^2 \cdot 49$	18
$-49 + 233 = +184 = +2^3 \cdot 23$	21
$+23 + 233 = +256 = +28 \cdot 1$	29

[ergo $x = 29$, sicque minima formula per 233 divisibilis est $2^{29} - 1$].

SCHOLION

24. Hac igitur methodo pro quolibet divisore N facile computatur formula simplicissima $2^x \pm 1$ per eum divisibilis. Haud igitur abs re visum est tabulam hic adiungere, in qua pro omnibus numeris primis usque ad 400 simplicissimae formulae exhibentur; divisores autem primos commode in quatuor ordines, secundum formas $8n+1,\ 8n-1,\ 8n+3$ et $8n-3$ distribui conveniet:

N $8n+1$	$2^x \pm 1$	N $8n-1$	$2^x \pm 1$
1	$2^0 - 1$	7	$2^3 - 1$
17	$2^4 + 1$	23	$2^{11} - 1$
41	$2^{10} + 1$	31	$2^5 - 1$
73	$2^9 - 1$	47	$2^{23} - 1$
89	$2^{11} - 1$	71	$2^{35} - 1$
97	$2^{24} + 1$	79	$2^{39} - 1$
113	$2^{14} + 1$	103	$2^{51} - 1$
137	$2^{34} + 1$	127	$2^7 - 1$
193	$2^{48} + 1$	151	$2^{15} - 1$
233	$2^{29} - 1$	167	$2^{83} - 1$

241	$2^{12}+1$	191	$2^{95}-1$
257	$2^{8}+1$	199	$2^{99}-1$
281	$2^{35}+1$	223	$2^{37}-1$
313	$2^{78}+1$	239	$2^{119}-1$
337	$2^{21}-1$	263	$2^{131}-1$
353	$2^{44}+1$	271	$2^{135}-1$
401	$2^{100}+1$	311	$2^{155}-1$
		359	$2^{179}-1$
		367	$2^{183}-1$
		383	$2^{191}-1$
		431	$2^{215}-1$

N	$2^{x}+1$	N	$2^{x}+1$
$8n+3$		$8n-3$	
3	$2^{1}+1$	5	$2^{2}+1$
11	$2^{5}+1$	13	$2^{6}+1$
19	$2^{9}+1$	29	$2^{14}+1$
43	$2^{7}+1$	37	$2^{18}+1$
59	$2^{29}+1$	53	$2^{26}+1$
67	$2^{33}+1$	61	$2^{30}+1$
83	$2^{41}+1$	101	$2^{50}+1$
107	$2^{53}+1$	109	$2^{18}+1$
131	$2^{65}+1$	149	$2^{74}+1$
139	$2^{69}+1$	157	$2^{26}+1$
163	$2^{81}+1$	173	$2^{86}+1$
179	$2^{89}+1$	181	$2^{90}+1$
211	$2^{105}+1$	197	$2^{98}+1$
227	$2^{113}+1$	229	$2^{38}+1$
251	$2^{25}+1$	269	$2^{134}+1$
283	$2^{47}+1$	277	$2^{46}+1$
307	$2^{51}+1$	293	$2^{146}+1$
331	$2^{10}+1$	317	$2^{158}+1$
347	$2^{173}+1$	349	$2^{174}+1$
371	$2^{185}+1$	373	$2^{186}+1$
379	$2^{189}+1$	389	$2^{194}+1$
		397	$2^{22}+1$

Hos casus probe perpendentes stabilire poterimus sequens Theorema, quod eo magis notatu dignum videtur, quod firma demonstratione etiamnum indiget.

THEOREMA I

25. *Si numerus primus* $2p+1$ *fuerit formae* $8n\mp 1$, *per eum semper divisibilis erit formula* 2^p-1 ; *sin autem habeat hanc formam :* $8n\mp 3$, *per eum divisibilis erit formula* 2^p+1.

Cum enim formula $2^{2p}-1$. semper divisibilis sit per numerum primum $2p+1$, necesse est, ut alterutra harum formularum: 2^p-1 vel 2^p+1 per eundem dividi queat; quod cum aeque valeat de omnibus aliis potestatibus $a^{2p}-1$, dummodo *a* ad $2p+1$ fuerit primus, prouti pro *a* alios atque alios valores assumamus, sequentia Theoremata vera deprehenduntur:

THEOREMA 2

26. *Si numerus primus* $2p+1$ *fuerit formae* $12n\pm 1$, *per eum semper divisibilis erit formula* 3^p-1. *Sin autem habeat formam* $12n\mp 5$, *per eum divisibilis erit formula* 3^p+1.

THEOREMA 3

27. *Sumto* $a=5$, *si* $2p+1$ *fuerit numerus primus, utrum per eum divisibilis sit sive formula* 5^p-1 *sive* 5^p+1 , *sequens tabella declarat :*

Si fuerit $2p+1$	divisibilis erit
$20n\mp 1$	5^p-1
$20n\mp 3$	5^p+1
$20n\mp 7$	5^p+1
$20n\mp 9$	5^p-1

THEOREMA 4

28. *Sumto a* = 6, *si fuerit* 2 *p* + 1 *numerus primus, utrum per eum divisibilis sit sive formula* 6^p-1 , *sive* 6^p+1, *sequens tabella declarat :*

Si fuerit $2p+1$	divisibilis erit
$24n\mp 1$	6^p-1

$24n \mp 3$	$6^p + 1$
$24n \mp 7$	$6^p + 1$
$24n \mp 9$	$6^p - 1$

THEOREMA 5

29. *Sumto* $a = 7$, *si fuerit* $2p+1$ *numerus primus, utrum per eum divisibilis sit sive formula* $7^p - 1$ *sive formula* $7^p + 1$, *ex sequenti tabella patet:*

Si fuerit $2p+1$	divisibilis erit
$28n \mp 1$	$7^p - 1$
$28n \mp 3$	$7^p + 1$
$28n \mp 7$	$7^p + 1$
$28n \mp 9$	$7^p - 1$
$28n \mp 11$	$7^p + 1$
$28n \mp 13$	$7^p + 1$

THEOREMA 6

30. *Sumto* $a = 8$, *si fuerit* $2p+1$ *numerus primus, utrum per eum divisibilis sit sive formula* $8^p - 1$, *sive* $8^p + 1$, *sequens tabella ostendit :*

Si fuerit $2p+1$	divisibilis erit
$32n \mp 1$	$8^p - 1$
$32n \mp 3$	$8^p + 1$
$32n \mp 5$	$8^p + 1$
$32n \mp 7$	$8^p - 1$
$32n \mp 9$	$8^p - 1$
$32n \mp 11$	$8^p + 1$
$32n \mp 13$	$8^p + 1$
$32n \mp 15$	$8^p - 1$

THEOREMA 7

31. *Sumto* $a = 10$, *si fuerit* $2p+1$ *numerus primus, utrum per eum divisibilis sit sive formula* $10^p - 1$, *sive* $10^p + 1$, *ex sequenti tabella perspicitur:*

Si fuerit $2p+1$	divisibilis erit
$40n \mp 1$	$10^p - 1$
$40n \mp 3$	$10^p - 1$
$40n \mp 7$	$10^p + 1$
$40n \mp 9$	$10^p - 1$
$40n \mp 11$	$10^p + 1$
$40n \mp 13$	$10^p - 1$
$40n \mp 17$	$10^p + 1$
$40n \mp 19$	$10^p + 1$

THEOREMA GENERALE

32. *Quicunque fuerit numerus a, si* $2p+1$ *denotet numerum primum et casu* $p = f$ *innotuerit, utrum formula* $a^f - 1$, *an* $a^f + 1$ *divisibilis sit per* $2f+1$, *tum generatim eiusdem generis formula sive* $a^p - 1$ *sive* $a^p + 1$ *divisibilis erit per* $2p+1$, *si fuerit* $2p+1 = 4af \mp (2f+1)$), *quicunque numerus pro n accipiatur, dummodo inde prodeat* $2p+1$ *numerus primus.*

COROLLARIUM 1

33. Ex praecedentibus Theorematibus satis liquet, casu $f = 0$ semper formulam av -1 divisibilem fore per $2p+1 = 4an \mp 1$, quoties scilicet hic numerus fuerit primus.

COROLLARIUM 2

34. Sin autem sit $f = 1$, prouti sive $a-1$, sive $a+1$ per 3 dividi potest, simili casu generatim sive formula $a^p - 1$ sive formula $a^p + 1$ per numerum primum $2p+1$ erit divisibilis, quoties $2p+1$ in hac forma: $4an \pm 3$ continetur.

SCHOLION

35. Theoremata autem particularia allata facile ulterius continuari possunt, si sequens Problema in subsidium vocetur, cuius quidem solutio firmissimis rationibus innititur.

PROBLEMA

36. *Quicunque fuerit numerus a, si* $2p+1$ *denotet numerum primum, quovis casu oblato investigare, utrum formula* a^p-1 *an altera* a^p+1 *divisibilis sit per* $2p+1$.

SOLUTIO

Quaerantur omnia residua, quae ex divisione quadratorum per numerum $2p+1$ resultant, quae sint 1, α, β, δ, δ etc. multitudine $= p$, numeri autem ab his diversi non residua adpellentur. Quo facto si numerus *a* inter residua reperiatur, tum semper formula a^p-1 erit divisibilis; sin autem numerus *a* inter non-residua occurrat, tum altera formula a^p+1 divisibilis erit.

Haec autem regula ita demonstratur: Si fuerit *a* residuum ex cuiusdam quadrati x^2 divisione per $2p+1$ natum, tum erit x^2-a per $2p+1$ divisibile; sive aequabitur cuipiam multiplo $m(2p+1)$, ita ut sit $a=x^2-m(2p+1)$. Hinc ergo fiet $a^p=(x^2-m(2p+1))^p$, quae potestas per $2p+1$ divisa idem residuum relinquet ac potestas $(x^2)^p$; verum haec potestas abit in x^{2p}, quae per $2p+1$ divisa certe unitatem relinquit. Ex quo sequitur etiam potestatem a^p unitatem relinquere, sive formulam a^p-1 esse divisibilem.

COROLLARIUM

37. Cum residua 1, α, β, δ, δ etc. minora esse soleant quam divisor $2p+1$, iis adhuc annumerari licet $1+(2p+1)$, $\alpha+(2p+1)$, $\beta+(2p+1)$ etc., quod observandum est, si numerus *a* maior fuerit divisore $2p+1$.

SCHOLION

38. Cum igitur in hoc negotio maximi sit momenti tam residua quam non-residua nosse, pro divisoribus primis minoribus sequentem tabulam hic adiiciamus; superfluum autem foret, non-residua adposuisse.

Divisor	Residua
3	1, 4, 7, 10, 13, 16, 19, 22, 25 etc.
5	1, 4, 6, 9, l1, 14, 16, 19, 21, 24 etc.
7	1, 2, 4, 8, 9, l1, 15, 16, 18, 22 etc.
1	1 1, 3, 4, 5, 9, 12, 14, 15, 16, 20, 23 etc.
13	1, 3, 4, 9, 10, 12, 14, 16, 17, 22, 23, 25, 27 etc.
17	1, 2, 4, 8, 9, 13, 15, 16, 18, 19, 21, 25, 26, 30 etc.
19	1, 4, 5, 6, 7, 9, 11, 16, 17, 20, 23, 24, 25, 26 etc.
23	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18, 24, 25, 26, 27 etc.
29	1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28 etc.

31	1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28 etc.
37	1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 etc.
	etc.

Ope huius tabulae sequentia Theoremata particularia facillime derivabimus.

THEOREMA 8

39. *Sumto* $a=11$, *si fuerit* $2p+1$ *numerus primus, utrum per eum divisibilis sit formula* 11^p-1, *sive* 11^p+1, *sequens tabella ostendit:*

Si fuerit $2p+1$	divisibilis erit
$44n\pm1$	11^p-1
$44n\pm3$	11^p+1
$44n\pm5$	11^p-1
$44n\pm7$	11^p-1
$44n\pm9$	11^p-1
$44n\pm13$	11^p+1
$44n\pm15$	11^p+1
$44n\pm17$	11^p+1
$44n\pm19$	11^p-1
$44n\pm21$	11^p+1

THEOREMA 9

40. *Sumto* $a=12$, *si fuerit* $2p+1$ *numerus primus, utrum per eum divisibilis sit sive forma* 12^p+1 *sive* 12^p-1, *ex sequenti tabella patet:*

Si fuerit $2p+1$	divisibilis erit
$48n\pm1$	12^p-1
$48n\pm5$	12^p+1
$48n\pm7$	12^p+1
$48n\pm11$	12^p-1
$48n\pm13$	12^p-1
$48n\pm17$	12^p+1

$48n \pm 19$	$12^p + 1$
$48n \pm 23$	$12^p - 1$

THEOREMA 10

41. *Sumto a successive* $= 13,\ 14,\ 15$, *si fuerit* $2p+1$ *numerus primus, utrum per eum divisibilis sit sive forma* $a^p + 1$ *sive* $a^p - 1$, *ex sequentibus tabellis patet :*

$a = 13$		$a = 14$		$a = 15$	
$2p+1$		$2p+1$		$2p+1$	
$52n \pm 1$	$13^p - 1$	$56n \pm 1$	$14^p - 1$	$60n \pm 1$	$15^p - 1$
$52n \pm 3$	$13^p - 1$	$56n \pm 3$	$14^p + 1$	$60n \pm 7$	$15^p - 1$
$52n \pm 5$	$13^p + 1$	$56n \pm 5$	$14^p - 1$	$60n \pm 11$	$15^p - 1$
$52n \pm 7$	$13^p + 1$	$56n \pm 9$	$14^p - 1$	$60n \pm 13$	$15^p + 1$
$52n \pm 9$	$13^p - 1$	$56n \pm 11$	$14^p + 1$	$60n \pm 17$	$15^p - 1$
$52n \pm 11$	$13^p + 1$	$56n \pm 13$	$14^p - 1$	$60n \pm 19$	$15^p + 1$
$52n \pm 15$	$13^p + 1$	$56n \pm 15$	$14^p + 1$	$60n \pm 23$	$15^p + 1$
$52n \pm 17$	$13^p - 1$	$56n \pm 17$	$14^p + 1$	$60n \pm 29$	$15^p + 1$
$52n \pm 19$	$13^p + 1$	$56n \pm 19$	$14^p + 1$		
$52n \pm 21$	$13^p + 1$	$56n \pm 23$	$14^p + 1$		
$52n \pm 23$	$13^p - 1$	$56n \pm 25$	$14^p - 1$		
$52n \pm 25$	$13^p - 1$	$56n \pm 27$	$14^p + 1$		

ADDITAMENTUM

Quae hactenus sunt tradita, plerumque adhuc firmis demonstrationibus destituuntur; omnia autem dubia maximam partem diluentur sequentibus propositionibus, quibus simul omnia ad multo maiorem evidentiae gradum evehentur.

THEOREMA 1

1. *Si formula* $4p+(2q+1)^2$ *fuerit numerus primus, per eumque omnia quadrata dividantur, inter residua occurret tam* $+p$ *quam* $-p$.

DEMONSTRATIO

In his residuis primo occurrunt omnia quadrata, quatenus sunt ipso divisore, quem littera *D* designemus, minora; praeterea vero ex quadratis maioribus, veluti Q^2, nascuntur residua Q^2-D vel $Q^2-\lambda D$. Quin etiam notum est ad residua referri posse omnes formulas $Q^2 \mp D$. Capiatur igitur $Q^2=(2q+1)^2$, et ob $D=4p+(2q+1)^2$ residuum prodit $-4p$; ergo etiam inter residua erit $-p$, quia generatim, si inter residua fuerit $\alpha^2\beta$, tum ibidem quoque semper β reperitur. Porro quoniam hic divisor $4p+(2q+1)^2$ in forma $4n+1$ continetur, iam demonstratum est singula residua utroque signo + et − adfecta reperiri; unde manifestum est nostro casu tam $+p$ quam $-p$ inter residua reperiri debere.

COROLLARIUM 1

2. Quia tam $+p$ quam $-p$ est residuum, dabuntur formulae tam $xx+pyy$ quam $xx-pyy$ per propositum divisorem *D* divisibiles.

COROLLARIUM 2

3. Cum autem hae formae: $xx+pyy$ et $xx-pyy$ alios non admittant divisores, nisi qui in certis formulis contineantur, necesse est, ut etiam numerus primus sub iisdem formulis comprehendatur.

COROLLARIUM 3

4. Quia, posito divisore $=2m+1$, numerus omnium residuorum tantum est $=m$, dum reliqui numeri omnes ad non-residua sint referendi, hinc sequitur etiam formulam p^m-1 divisibilem fore per $2m+1$, dummodo $2m+1$ fuerit numerus primus. Quia enim

omnes potestates ipsius *p* quoque sunt residua, horumque numerus tantum est *m,* necesse est, ut potestas p^m iterum ad unitatem, seu p^0 reducatur, hincque $p^m - 1$ dividi poterit per divisorem $2m+1$.

THEOREMA 2

5. *Si formula* $4p-(2q+1)^2$ *fuerit numerus primus, per eumque omma quadrata dividantur, in residuis semper occurret numerus p; at eius negativum* $-p$*, sive quod eodem redit* $D-p$*, denotante D divisorem, ad non-residua refertur.*

DEMONSTRATIO

Praeter ipsa quadrata, divisore minora, etiam inter residua occurret quadratum $(2q+1)^2$, divisore auctum, ideoque 4*p;* ergo etiam, ob rationem ante allegatam, occurret numerus *p.* Et quia hic divisor $4p-(2q+1)^2$ est numerus formae $4n-1$, ubi nullum residuum utroque signo + et − adfectum occurrit, sequitur $-p$ inter non-residua reperiri debere.

COROLLARIUM l

6. Quia ergo *p* certe est residuum, dabitur formula $xx-pyy$ per nostrum divisorem divisibilis, unde etiam divisor eiusmodi formam habebit, qualem divisores formulae $xx-pyy$ postulant.

COROLLARIUM 2

7. At quia $-p$ est non-residuum, nulla dabitur formula $x\,x+p\,y\,y$ per nostrum divisorem divisibilis, unde etiam divisor e formula generali, quae omnes divisores ipsius $xx+pyy$ complectitur, excluditur.

COROLLARIUM 3

8. Ob rationem ante allegatam, si divisor vocetur $2m+1$, formula p^m-1 per eum divisibilis esse debet; neque vero haec formula $(-p)^m-1$ erit divisibilis, id quod etiam per se est perspicuum. Cum enim divisor noster formam habeat $4n-1$, fiet $m=2n-1$, ideoque numerus impar, et $(-p)^m=-p^m$*;* quare cum p^m-1 sit divisibile, certe haec formula $-p^m-1$ sive p^m+1 non erit divisibilis.

THEOREMA 3

9. *Si* $4n+1$ *fuerit numerus primus, per eumque omnia quadrata dividantur, inter residua omnes occurrent numeri sive in hac forma generali:* $n-qq-q$ *sive in hac:* $qq+q-n$ *contenti.*

DEMONSTRATIO

Manifestum est divisorem nostrum $4n+1$ infinitis modis ad formam $4p+(2q+1)^2$ reduci posse. Posito enim $4n+1=4p+(2q+1)^2$ fiet $n=p+q^2+q$, ideoque $p=n-q^2-q$; unde sequitur, quicunque numerus pro q accipiatur, numerum $n-qq-q$ inter residua reperiri; deinde quia etiam $-p$ est residuum (§ 1), manifestum est etiam omnes numeros in hac forma $qq+q-n$ fore residua.

COROLLARIUM 1

10. Hoc ergo modo, dum pro q successive accipiuntur omnes numeri 0, 1, 2, 3, 4, 5 etc. infiniti, prodibunt numeri ad residua referendi, qui tamen omnes ad multitudinem $2n$ se reduci patientur, quandoquidem plura residua diversa non dantur quam $2n$.

COROLLARIUM 2

11. Necesse igitur est, ut omnes numeri, sive in forma $n-qq-q$ sive in forma $qq+q-n$ contenti, omnia plane praebeant residua, divisori $4n+1$ convenientia. Quin etiam ex aliquot huiusmodi residuis reliqua sponte nascuntur, cum tam potestates quoque singulorum, quam producta ex binis pluribusve pariter in residuis occurrere debeant; unde patet, si iam prodierint residua $\alpha\gamma$ et $\beta\gamma$, tum etiam residuum fore $\alpha\beta$. Quia enim productum $\alpha\beta\gamma^2$ est residuum, omisso quadrato γ^2 etiam $\alpha\beta$ erit residuum.

COROLLARIUM 3

12. Quodsi ergo compertum fuerit residuum $\alpha\beta$, ex alio autem casu residuum prodeat α, etiam alter factor β erit residuum.

SCHOLION

13. Cum huiusmodi combinationes binorum residuorum pluribus, immo infinitis modis institui queant, hinc iam maxime verisimile videtur, praeter ipsos numeros in formulis $n-qq-q$ et $qq+q-n$ contentos etiam omnes eorum factores primos in residuis occurrere, quae coniectura utrum fundamento certo innitatur necne, per sequentia

exempla exploremus. Hunc in finem exponamus numeros in formula $qq+q$ contentos, qui sunt

0, 2, 6, 12, 20, 30, 42, 56, 72, 90, 110, 132, 156,
182, 210, 240, 272, 306, 342, 380, 420 etc.,

et quemadmodum residua hinc nata littera *p* designamus, ita residua prima seu simplicia littera *r* indicemus, et quo facilius perspiciatur omnes factores numerorum *p* quoque esse residua, ipsos numeros *p* per suos factores primos repraesentemus:

1°. Sit $4n+1=5$; erit $n=1$.

$p=1,\ 1,\ 5,\ 11,\ 19,\ 29,\ 41,\ 5\cdot 11,\ 71$ etc.

$r=1,\ 5,\ 11,\ 19,\ 29,\ 41,\ 71$ etc.,

ubi patet numeri compositi *p,* qui est unicus $5\cdot 11$, ipsos factores quoque esse residua.

2°. Sit $4n+1=13; n=3$.

$p=3,\ 1,\ 3,\ 32,\ 17,\ 33,\ 3\cdot 13,\ 53,\ 3\cdot 23$ etc.

$r=1,\ 3,\ 13,\ 17,\ 23,\ 53$ etc.

3°. Sit $4n+1=17; n=4$.

$p=22,\ 2,\ 2,\ 23,\ 24\ ,\ 2\cdot 13,\ 2\cdot 19,\ 22\cdot 13,\ 22\cdot 17,\ 2\cdot 43$ etc.

$r=1,\ 2,\ 13,\ 17,\ 19,\ 43$ etc.

4°. Sit $4n+1=29$; $n=7$.

$p=7,\ 5,\ 1,\ 5,\ 13,\ 23,\ 5\cdot 7,\ 72\ ,\ 5\cdot 13,\ 83,\ 103$ etc.

$r=1,\ 5,\ 7,\ 13,\ 23,\ 83,\ 103$ etc.

5°. Sit $4n+1=37$; $n=9$.

$p=3^2,\ 7,\ 3,\ 3,\ 11,\ \left[3\cdot 7,\right]\ 3\cdot 11,\ 47,\ \left[3^2\cdot 7,\right]\ 3^4,\ 101$ etc.

$r=1,\ 3,\ 7,\ 11,\ 47,\ 101$ etc.

6°. Sit $4n+1=41; n=10$.

$p=2\cdot 5,\ 2^3,\ 2^2,\ 2,\ 2\cdot 5,\ 2^2\cdot 5,\ 2^5,\ 2\cdot 23,\ 2\cdot 31,\ 2^4\cdot 5,\ 2^2\cdot 5^2$ etc.

$r=1,\ 2,\ 5,\ 23,\ 31$ etc.,

ubi patet in numeris *p* nullos factores primos conspici, qui non simul sint residua.

7°. Sit $4n+1=53; n=13$

$p=13,\ 11,\ 7,\ 1,\ 7,\ 17,\ 29,\ 43,\ 59,\ 7\cdot 11,\ 97$ etc.

$r=1,7,\ 11,\ 13,\ 17,\ 29,\ 43,\ 59,\ 97$ etc.

8° Sit $n=61$; $n=15$.

$p=3\cdot 5,\ 13,\ 3^2,\ 3,\ 5,\ 3\cdot 5,\ 33,\ 41,\ 3\cdot 19,\ 3\cdot 52,\ 5\cdot 19$ etc.

$r=1,\ 3,\ 5,\ 13,\ 19,\ 41$ etc.

9°. Sit $4n+1=73; n=18$.

$p=2\cdot 3^2,\ 2^4,\ 2^2\cdot 3,\ 2\cdot 3,\ 2,\ 2^2\cdot 3,\ 2^3\cdot 3,\ 2\cdot 19,\ 2\cdot 3^3,\ 2^3\cdot 3^2,\ 2^2\cdot 2^3$ etc.

$r=1,\ 2,\ 3,\ 19,\ 23$ etc.

10°. Sit $4n+1=89; n=22$.

$p=2\cdot 11,\ 2^2\cdot 5,\ 2^4,\ 2\cdot 5,\ 2,\ 2^3,\ 2^2\cdot 5,\ 2\cdot 17,\ 2\cdot 5^2,\ 2^2\cdot 17,\ 2^3\cdot 11$ etc.

$r=1,\ 2,\ 5,\ 11,\ 17$ etc.

11°. Sit $4n+1=97; n=24$.

$p=2^3\cdot 3,\ 2\cdot 11,\ 2\cdot 32,\ 2^2\cdot 3,\ 2^2,\ 2\cdot 3,\ 2\cdot 3^2,\ 2^5,\ 2^4\cdot 3,\ 2\cdot 3\cdot 11,\ 2\cdot 43$ etc.

$r=1,\ 2,\ 3,\ 11,\ 43$ etc.

12°. Sit $4n+1=101; n=25$.

$p=5^2,\ 23,\ 19,\ 13,\ 5,\ 5,\ 17,\ 31,\ 47,\ 5\cdot 13,\ 5\cdot 17$ etc.

$r=1,\ 5,\ 13,\ 17,\ 19,\ 23,\ 31,\ 47$ etc.

13°. Sit $4n+1=109; n=27$.

$p=33,\ 5^2,\ 3\cdot 7,\ 3\cdot 5,\ 7,\ 3,\ 3\cdot 5,\ 29^2,\ 32\cdot 5,\ 32\cdot 7,\ 83$ etc.

$r=1,\ 3,\ 5,\ 7,\ 29^3,\ 83$ etc.

14°. Sit $4n+1=113; n=28$.

$p=\ 2^2\cdot 7,\ 2\cdot 13,\ 2\cdot 11,\ 2^4,\ 2^3,\ 2,\ 2\cdot 7,\ 2^2\cdot 7,\ 2^2\cdot 11,\ 2\cdot 31,\ 2\cdot 41$ etc.

$r=1,\ 2,\ 7,\ 11,\ 13,\ 31,\ 41$ etc.

15°, Sit $4n+1=137; n=34$.

$p=2\cdot 17,\ 2^5,\ 2^2\cdot 7,\ 2\cdot 11,\ 2\cdot 7,\ 2^2,\ 2^3,\ 2\cdot 11,\ 2\cdot 19,\ 23\cdot 7,\ 22\cdot 19$ etc.

$r=1,\ 2,\ 7,\ 11,\ 17,\ 19$ etc.

16°. Sit $4n+1=149; n=37$.

$p=\ 37,\ 5\cdot 7,\ 31,\ 52,\ 17,\ 7,\ 5,\ 19,\ 5\cdot 7,\ 53,\ 73$ etc.

$r=\ 1,\ 5,\ 7,\ 17,\ 19,\ 31,\ 37,\ 53,\ 73$ etc.

17°. Sit $4n+1=157; n=39$.

$p=3\cdot 13,\ 37,\ 3\cdot 11,\ 33,\ 19,\ 32,\ 3,\ 17,\ 3\cdot 11,\ 3\cdot 17,\ 71$ etc.

$r=1,\ 3,\ 11,\ 13,\ 17,\ 19,\ 37,\ 71$ etc.

18°. Sit $4n+1=173; n=43$.

$p=\ 43,\ 41,\ 37,\ 31,\ 23,\ 13,\ 1,\ 13,\ 29,\ 47,\ 67$ etc.

$r=1,\ 13,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 67$ etc.

19°. Sit $4n+1=181; n=45$.

$p=3^2\cdot 5,\ 43,\ 3\cdot 13,\ 3\cdot 11,\ 52,\ 3\cdot 5,\ 3,\ 11,\ 33,\ 32\cdot 5,\ 5\cdot 13$ etc.

$r=1,\ 3,\ 5,\ 11,\ 13,\ 43$ etc.

20°. Sit $4n+1=193; n=48$.

$p = 2^4 \cdot 3,\ 2 \cdot 23,\ 2 \cdot 3 \cdot 7,\ 2^2 \cdot 3^2,\ 2^2 \cdot 7,\ 2 \cdot 3^2,\ 2 \cdot 3,\ 2^3,\ 2^3 \cdot 3,\ 2 \cdot 3 \cdot 7,\ 2 \cdot 31$ etc.

$r = 1,\ 2,\ 3,\ 7,\ 23,\ 31$ etc.

23. Sit $4n+1 = 197; n = 49$.

$p = 7^2,\ 47,\ 43,\ 37,\ 29,\ 19,\ 7,\ 7,\ 23,\ 41,\ 61$ etc.

$r = 1,\ 7,\ 19,\ 23,\ 29,\ 37,\ 41,\ 43,\ 47,\ 61$ etc.

SCHOLION

14. Ex his omnibus exemplis manifesto liquet nullos numeros primos sub littera *p* tamquam factores occurrere, qui non simul ipsi sint residua; quae veritas certe omnem attentionem eo magis meretur, quod ex sola inductione est conclusa, neque etiamnunc firma demonstratione corroborata; quia tamen in omnibus allatis exemplis tam luculenter se offert, neutiquam desperandum videtur. Qui autem hanc investigationem suscipere voluerit, probe perpendat hanc egregiam proprietatem tum tantum locum habere, quando $4n+1$ est numerus primus; si enim non est primus, plurimi occurrunt casus, quibus hoc secus evenit. Huius generis exemplum est, quo $n = 11$;
tum enim prodit $p = 11,\ 3^2,\ 5,\ 1,\ 3^2,\ 19,\ 31,\ 3^2 \cdot 5,\ 61,\ 79,\ 3^2 \cdot 11$ etc., unde
de numero 3 nihil plane concludere licet, an ad residua pertineat necne?
Quod autem casibus, quibus $4n+1$ est numerus primus, semper succedat, ratio fortasse in eo est quaerenda, quod pro divisore $2n + 1$ numerus residuorum semper est *n,* dum contra, si $2n+1$ non est primus, numerus residuorum multo est minor; id quod in caussa esse videtur, quod in allato exemplo circa numerum 3 nihil decidatur. Quicquid autem sit, nullum plane dubium superesse videtur, quominus sequens stabiliatur

CONCLUSIO

15. Quoties numerus $4n+1$ fuerit primus, per eumque omnia quadrata dividantur, non solum omnes numeri in hac formula: $n - qq - q$, sive etiam hac: $qq + q - n$ contenti, inter residua occurrunt ipsi, sed etiam omnes plane factores primi, ex quibus illi sint compositi.

THEOREMA 4

16. *Si* $4n-1$ *fuerit numerus primus et per eum omnia quadrata dividantur, inter residua omnes occurrent numeri in hac formula* $n + qq + q$ *contenti.*

DEMONSTRATIO

Hic etiam clarum est numerum $4n-1$ infinitis modis sub hac forma $4p-(2q+1)^2$ repraesentari posse; posito enim $4n-1 = 4p-(2q+1)^2$,

fiet $n = p - q^2 - q$, sive $p = n + q^2 + q$. Cum ergo $4p - (2q+1)^2$ sit numerus primus, ante demonstratum est numerum *p* inter residua reperiri; quocirca etiam omnes numeri in hac formula contenti $n + qq + q$ inter residua reperientur.

COROLLARIUM 1

17. Si ergo pro *q* omnes numeri 0, 1, 2, 3, 4 etc. substituantur, infiniti huiusmodi oriuntur numeri, quos tamen omnes ad multitudinem *2n* - 1 deprimere licet, siquidem isti numeri $n + qq + q$ per divisorem $4n - 1$ dividantur.

COROLLARIUM 2

18. Necesse ergo est hoc modo omnia plane prodire residua, quandoquidem etiam tam potestates, quam producta singulorum istorum numerorum inter residua reperiuntur; unde ut ante sequitur, si iam habeantur duo residua α et $\alpha\beta$, tum etiam β fore residuum; quin etiam si $\alpha\gamma\gamma$ fuerit residuum, ipsum α quoque erit residuum.

SCHOLION

19. Cum eiusmodi bina residua infinitis modis combinari possint, maxime verisimilis est suspicio praeter ipsos numeros in forma $n + qq + q$ contentos etiam omnes eorum factores primos in residuis occurrere; quae coniectura utrum, pariter ut ante, certo fundamento nitatur necne, per sequentia exempla exploremus. Iam supra autem exposuimus numeros in formula $qq + q$ contentos, unde pro quolibet numero primo residua simplicia, pariter ut ante, littera *r* indicemus.

1°. Sit $4n - 1 = 3$; erit $n = 1$.
$p = 1,\ 3,\ 7,\ 13,\ 3\cdot 7,\ 31,\ 43,\ 3\cdot 19,\ 73,\ 7\cdot 13,\ 3\cdot 37$ etc.
$r = 1,\ 3,\ 7,\ 13,\ 19,\ 31,\ 37,\ 43,\ 73$ etc.

2°. Sit $4n - 1 = 7$; erit $n = 2$.
$p = 2,\ 2^2,\ 2^3,\ 2\cdot 7,\ 2\cdot 11,\ 2^5,\ 2^2\cdot 11,\ 2\cdot 29,\ 2\cdot 37,\ 2^2\cdot 23,\ 2^4\cdot 7$ etc.
$r = 1,\ 2,\ 7,\ 11,\ 23,\ 29,\ 37$ etc.

3°. Sit $4n - 1 = 11$; erit $n = 3$.
$p = 3,\ 5,\ 3^2,\ 3\cdot 5,\ 23,\ 3\cdot 11,\ 3^2\cdot 5,\ 59,\ 3\cdot 5^2,\ 3\cdot 31,\ 113$ etc.
$r = 1,\ 3,\ 5,\ 11,\ 23,\ 31,\ 59,\ 113$ etc.

4°. Sit $4n - 1 = 19$; erit $n = 5$.
$p = 5,\ 7,\ 11,\ 17,\ 5^2,\ 5\cdot 7,\ 47,\ 61,\ 7\cdot 11,\ 5\cdot 19,\ 5\cdot 23$ etc.
$r = 1,\ 5,\ 7,\ 11,\ 17,\ 19,\ 23,\ 47,\ 61$ etc.

5°. Sit $4n - 1 = 23$; $n = 6$.

$p = 2\cdot 3,\ 2^3,\ 2^2\cdot 3,\ 2\cdot 3^2,\ 2\cdot 13,\ 2^2\cdot 3^2,\ 2^4\cdot 3,\ 2\cdot 31,\ 2\cdot 3\cdot 13,\ 2^5\cdot 3,\ 2^2\cdot 29$ etc.

$r = 1,\ 2,\ 3,\ 13,\ 29,\ 31$ etc.

6°. Sit $4n-1 = 31$; erit $n = 8$.

$p = 2^3,\ 2\cdot 5,\ 2\cdot 7,\ 2^2\cdot 5,\ 2^2\cdot 7,\ 2\cdot 19,\ 2\cdot 5^2,\ 2^6,\ 2^4\cdot 5,\ 2\cdot 7^2,\ 2\cdot 59$ etc.

$r = 1,\ 2,\ 5,\ 7,\ 19,\ 59$ etc.

7°. Sit $4n-1 = 43$; erit $n = 11$.

$p = 11,\ 13,\ 17,\ 23,\ 31,\ 41,\ 53,\ 67,\ 83,\ 101,\ 11^2$etc.

$r = 1,\ 11,\ 13,\ 17,\ 23,\ 31,\ 41,\ 53,\ 67,\ 83,\ 101$ etc.

8°. Sit $4n-1 = 47$; $n = 12$.

$p = 2^2\cdot 3, 2\cdot 7, 2\cdot 3^2, 2^3\cdot 3, 2^5, 2\cdot 3\cdot 7, 2\cdot 3^3,\ 2^2\cdot 17,\ 2^2\cdot 3\cdot 7,\ 2\cdot 3\cdot 17, 2\cdot 61$etc.

$r = 1,\ 2,\ 3,\ 7,\ 17,\ 61$ etc.

9°. Sit $4n-1 = 59$; $n = 15$.

$p = 3\cdot 5,\ 17,\ 3\cdot 7,\ 3^3,\ 5\cdot 7,\ 3^2\cdot 5,\ 3\cdot 19,\ 71,\ 3\cdot 29$ etc.

$r = 1,\ 3,\ 5,\ 7,\ 17,\ 19,\ 29,\ 71$ etc.

10°. Sit $4n-1 = 67$; $n = 17$.

$p = 17,\ 19,\ 23,\ 29,\ 37,\ 47,\ 59,\ 73,\ 89,\ 107,\ 127$ etc.

$r = 1,\ 17,\ 19,\ 23,\ 29,\ 37,\ 47,\ 59,\ 73,\ 89,\ 107,\ 127$ etc.

11°. Sit $4n-1 = 71$; $n = 18$.

$p = 2\cdot 3^2,\ 2^2\cdot 5,\ 2^3\cdot 3,\ 2\cdot 3\cdot 5,\ 2\cdot 19,\ 2^4\cdot 3,\ 2^2\cdot 3\cdot 5,\ 2\cdot 37,\ 2\cdot 3^2\cdot 5,\ 2^2\cdot 3^3, 2^7,\ 2\cdot 3\cdot 5^2$etc.

$r = 1,\ 2,\ 3,\ 5,\ 19,\ 37$ etc.

12°. Sit $4n-1 = 79$; $n = 20$.

$p = 2^2\cdot 5,\ 2\cdot 11,\ 2\cdot 13,\ 2^5,\ 2^3\cdot 5,\ 2\cdot 5^2,\ 2\cdot 31,\ 2^2\cdot 19,\ 2^2\cdot 23,\ 2\cdot 5\cdot 11$ etc.

$r = 1,\ 2,\ 5,\ 11,\ 13,\ 19,\ 23,\ 31$ etc.

13°. Sit $4n-1 = 83$; $n = 21$.

$p = 3\cdot 7,\ 23,\ 3^3,\ 3\cdot 11,\ 41,\ 3\cdot 17,\ 3^2\cdot 7,\ 7\cdot 11,\ 3\cdot 31,\ 3\cdot 37$ etc.

$r = 1,\ 3,\ 7,\ 11,\ 17,\ 23,\ 31,\ 37,\ 41$ etc.

14°. Sit $4n-1 = 103$; $n = 26$.

$p = 2\cdot 13,\ 2^2\cdot 7,\ 2^5, 2\cdot 19, 2\cdot 23,\ 2^3\cdot 7,\ 2^2\cdot 17,\ 2\cdot 41,\ 2\cdot 7^2,\ 2^2\cdot 29$ etc.

$r = 1,\ 2,\ 7,\ 13,\ 17,\ 19,\ 23,\ 29,\ 41$ etc.

SCHOLION

20. Ex his exemplis iterum abunde patet omnes plane numeros primos in numeris p contentos ipsos quoque esse residua. Evidens autem est, ut primum hoc de minoribus numeris fuerit certum, de maioribus nullum amplius dubium relinqui; at vero in numeros p binarius non ingreditur, nisi iam fuerit in ipso numero primo n; ternarius autem, nisi in duobus primis insit, ex tota serie p excluditur. Eodem modo patet quinarium, nisi in tribus

primis insit, quoque excludi; septenarius autem penitus excluditur, nisi in quatuor primis iam occurrat, et sic de reliquis. Unde patet in continuatione ulteriori istius seriei nullos numeros primos minores ingredi posse, qui non iam ante fuerint ingressi; quae observatio fortasse ad demonstrationem deducere posset. Verum hic iterum probe notetur hanc insignem proprietatem tantum locum habere, quoties $4n-1$ fuerit numerus primus; si enim esset compositus, tum utique eiusmodi numeri primi occurrere possunt, de quibus neutiquam liquet, utrum in ordinem *r* sint referendi. Veluti si fuerit $n=30=2\cdot3\cdot5$, tum numeri prop ita se habebunt:

$$p=2\cdot3\cdot5,\ 2^5,\ 2^2\cdot3^2,\ 2\cdot3\cdot7,\ 2\cdot5^2,\ 2^2\cdot3\cdot5,\ 2^3\cdot3^2,\ 2\cdot43,\ 2\cdot3\cdot17,\ 23\cdot3\cdot5,$$
$$2^2\cdot5\cdot7,\ 2\cdot34 \text{ etc.}$$

Hic quidem statim adparet binarium ad residua esse referendum; quo sublato iudicium redit ad sequentes numeros:

$$3\cdot5,\ 3^2,\ 3\cdot7,\ 5^2,\ 43,\ 3\cdot17,\ 5\cdot7,\ 3^4\text{etc.}$$

Hinc autem nullo modo concludi potest sive 3 sive 5 sive 7 in residuis reperiri; et fieri posset, ut singuli essent non-residua, quandoquidem producta ex binis non-residuis producunt residua; verum etiam hinc numerus $4n-1=119$ non est primus. De primis autem certa videtur haec

CONCLUSIO

21. Quoties numerus $4n-1$ fuerit primus, per eumque dividantur omnia quadrata, non solum omnes numeri in forma $n+qq+q$ contenti inter residua occurrunt ipsi, sed etiam omnes plane factores primi, ex quibus illi sunt compositi.

THEOREMA GENERALE

22. *Denotante T numerum quemcunque in hac formula* $(2q+1)^2-4at$ *contentum, si fuerit vel* $4as+T$ *vel* $4as-T$ *numerus primus, per eumque quadrata dividantur, tum in residuis semper reperietur numerus a.*

DEMONSTRATIO

Cum enim sit $T=(2q+1)^2-4at$, numerus ille primus erit vel $4as-4at+(2q+1)^2$, vel $4as+4at-(2q+1)^2$. Illo casu habebimus $p=a(s-t)$, hoc vero $p=a(s+t)$, sicque in utroque casu *p* factorem habet *a,* qui ergo per praecedentes conclusiones in residuis ex quadratis ortis occurret.

COROLLARIUM I

23. Hoc ergo modo numeri T ex quadratis $(2q+1)^2$ formati infra 4a deprimi poterunt; sicque multitudo horum valorum ad numerum determinatum reducetur, etiamsi numeri $(2q+1)^2$ in infinitum progrediantur. Inventis autem omnibus ipsius T valoribus ipso $4a$ minoribus, si illis continuo addantur multipla ipsius 4a, hos valores in infinitum continuare licebit.

COROLLARIUM 2

24. Quia numerus a inter residua quadratorum occurrit, semper dabitur formula $xx - ayy$ per numerum illum primum divisibilis, sive is sit $4as + T$ sive $4as - T$; ac si iste numerus primus vocetur $2m+1$, tum formula $a^m - 1$ divisorem habebit $2m+1$.

SCHOLION

25. Quot autem valores diversos littera T infra 4a sortiatur, id pendet ab indole numeri a, sive is fuerit primus sive compositus; atque hoc discrimen probe est notandum, cum ulterior evolutio harum formularum pro casibus, quibus a est numerus compositus, commode expediri nequeat, nisi casus, quibus a est numerus primus, ante fuerint explorati.

THEOREMA 5

26. *Si a fuerit numerus primus, puta $2\alpha+1$, tum numerus valorum litterae T ipso* 4a *minorum erit $= \alpha$, et totidem numeri formae $4n+1$ inde excludentur.*

DEMONSTRATIO

Omnes valores diversi litterae T ipso 4a minores colliguntur ex quadratis imparibus minoribus quam $a^2 = (2\alpha+1)^2$, quae ergo sunt 1, 9, 25, 49, ... $(2\alpha-1)^2$, quorum numerus utique est α. Perspicuum autem est ex quadratis maioribus quam a eosdem prorsus valores ipsius T resultare, qui ex minoribus prodierunt. Sit enim quadratum quodvis maius $(a+\beta)^2$, hocque comparetur cum quadrato minore $(a-\beta)^2$, et quia eorum differentia $4a\beta$ divisibilis est per 4a, utrinque idem residuum oriatur necesse est. Facile autem porro intelligitur ex omnibus quadratis ipso a^2 minoribus diversa residua nasci debere. Quia iam T denotat numeros formae $4n+1$, videamus, quot huiusmodi numeri ab unitate usque ad $4a = 8\alpha + 4$ occurrant. Facile autem patet eorum numerum fore $= 2\alpha+1$, inter quos occurrit unus per a divisibilis; quo excluso multitudo reliquorum est $= 2\alpha$; quare cum multitudo valorum idoneorum ipsius T sit $= \alpha$, evidens est totidem numeros formae $4n+1$ inde excludi.

COROLLARIUM 1

27. Quia omnes valores litterae T in forma $4n+1$ continentur, si omnes numeri huius formae ab unitate usque ad 4a scribantur, eorum semissis tantum praebet veros valores litterae *T,* reliqui vero omnes inde excluduntur. Utamur autem littera Θ ad huiusmodi numeros exclusos denotandos.

COROLLARIUM 2

28. Cum ergo omnes numeri formae $4n+1$, qui sunt: 1, 5, 9, 13, 17, 21, 25, 29, 33 etc., pro quovis casu numeri a sive ad ordinem terminorum $T=(2q+1)^2-4at$, sive ad ordinem exclusorum Θ referantur, operae pretium erit ambos istos ordines pro minoribus saltem ipsius a valoribus, qui quidem sint primi, exhibere; atque utile erit non solum primam periodum horum numerorum ipso *4a* minorum, sed etiam sequentes periodos, addendo continuo 4*a,* ob oculos exponere:

1°. Sit $a=2$; erit $4a=8$.

$$\begin{array}{l|l|l|l|l|l} T=1 & 9 & 17 & 25 & 33 & \\ \Theta=5 & 13 & 21 & 29 & 37 & \end{array} \text{etc.}$$

2°. Sit $a=3$; erit $4a=12$.

$$\begin{array}{l|l|l|l|l|l} T=1 & 13 & 25 & 49 & 61 & \\ \Theta=5 & 17 & 29 & 53 & 65 & \end{array} \text{etc.}$$

Quia hic a erat 3, quadrata per 3 divisibilia excludi debebant.

3°. Sit $a=5$; erit $4a=20$.

$$\begin{array}{l|l|l|l|l|l} T=1,9 & 21,29 & 41,49 & 61,69 & 81,89 & \\ \Theta=13,17 & 33,37 & 53,57 & 73,77 & 93,97 & \end{array} \text{etc.}$$

Hic scilicet ex ordine Θ exclusimus numerum 5, utpote ipsi a aequalem.

4°. Sit $a=7$; erit $4a=28$.

$$\begin{array}{l|l|l|l|l} T=1,9,25 & 29,37,53 & 57,65,81 & & \\ \Theta=5,13,17 & 33,41,45 & 61,69,73 & & \end{array} \text{etc.}$$

Hic in ordine Θ omisimus numerum 21, utpote per $a=7$ divisibilem.

5°. Sit $a=11; 4a=44$.

$$\begin{array}{l|l|l} T=1, \quad 5,\ 9,25,37 & 45,49,53,69,81 & 89,\ 93,\ 97,113,125 \\ \Theta=13,17,21,29,41 & 57,61,65,73,85 & 101,105,109,117,129 \end{array} \text{ etc.}$$

6°. Sit $a=13;\ 4a=52$.

$$\begin{array}{l|l} T=\ 1,9,17,25,29,49 & 53,61,69,77,81,101 \\ \Theta=5,21,33,37,41,45 & 57,73,85,89,93,\ 97 \end{array} \text{ etc.}$$

7°. Sit $a=17;\ 4a=68$.

$$\begin{array}{l} T=1,\ \ 9,13,21,25,33,49,53 \\ \Theta=5,29,37,41,45,57,61,65 \end{array} \text{ etc.}$$

8°. Sit $a=19\ ;\ 4a=76$.

$$\begin{array}{l|l} T=\ 1,\ 5,\ 9,17,25,45,49,61,73 & 77,81,\ \ 85,\ 93,101,\ 121,125,137,149 \\ \Theta=13,21,29,33,37,41,53,65,69 & 89,97,105,109,113,117,129,141,\ 145 \end{array} \text{ etc.}.$$

9°. Sit $a=23;\ 4a=92$.

$$\begin{array}{l} T=1,\ 9,\ 13,\ 25,\ 29,\ 41,\ 49,\ 73,\ 77,\ 81,\ 85 \\ \Theta=5,17,21,\ 33,\ 37,45,\ \ 53,\ 57,\ 61,\ 65,\ 89 \end{array} \text{ etc.}$$

10°. Sit $a=29;\ 4a=116$.

$$\begin{array}{l} T=\ 1,\ 5,\ \ 9,\ \ 13,\ 25,\ 33,\ 45,\ 49,\ 53,\ 57,\ 65,\ \ 81,\ \ \ 93,\ 109 \\ \Theta=17,\ 21,\ 37,\ 41,\ 61,\ 69,\ 73,\ 77,\ 85,\ 89,\ 97,\ 101,\ 105,\ 113 \end{array} \text{ etc.}$$

SCHOLION

29. Hinc ergo pro istis numeris primis *a* innotescunt tam valores litterae *T,* quam litterae Θ, quos ita intelligere decet, ut, quoties formula $4as+T$ vel $4as-T$ fuerit numerus primus, puta $2m+1$, tum semper exhiberi possit formula $xx-ayy$ per $2m+1$ divisibilis; tum vero etiam semper formula a^m-1 eundem habebit divisorem $2m+1$, ita ut iam plura Theoremata supra allata, scilicet quoties *a* fuerit numerus primus, ita succincte possimus enuntiare, ut, quoties fuerit $4as\mp T$ numerus primus $=2m+1$, tum semper formula a^m-1 eundem admittat divisorem; quo observato nullum amplius dubium supererit, quin numeri sub ordine Θ comprehensi contraria gaudeant proprietate, quam iam ita enuntiare licebit, ut, quoties formula

$4as \mp \Theta$ fuerit numerus primus $= 2m+1$, tum non amplius formula $a^m - 1$ per eum sit divisibilis; unde cum formula $a^{2m} - 1$ semper sit divisibilis, sequitur hoc casu semper formulam $a^m + 1$ per numerum primum $2m+1$ fore divisibilem. Atque haec duo enuntiata omnes casus supra allatos exhauriunt, quibus numerus *a* erat primus; quando autem *a* habet factores, res secus se habet, hosque casus peculiari modo tractari conveniet.

PROBLEMA

30. *Si numerus a fuerit compositus, puta* $a = fg$, *invenire numeros utriusque indolis per litteras* T *et* Θ *designatos.*

SOLUTIO

Hic igitur quaeruntur omnes divisores primi $2m+1$ sub formula $4fgs \mp T$ contenti, per quos formula $(fg)^m - 1$ sit divisibilis; id quod duplici modo fieri potest, vel quando hae duae formulae: $f^m - 1$ et $g^m - 1$ per $2m+1$ sunt divisibiles, vel etiam hae duae formulae: $f^m + 1$ et $g^m + 1$.
Priore enim casu, cum sit

$$(fg)^m - 1 = g^m(f^m - 1) + g^m - 1$$

utique haec formula per $2m+1$ dividi poterit. Iam pro numeris primis *f* et *g* divisores primi hoc praestantes supra sunt inventi, quos distinctionis gratia ita repraesentemus:

$$4fgs \mp T^{(f)} \text{ et } 4gfs \mp T^{(g)};$$

quae duae formulae in unam coalescent, si ex valoribus supra datis litterarum $T^{(f)}$ et $T^{(g)}$ eos excerpamus, qui utrique sunt communes. Hi enim si littera T comprehendantur, utique omnes numeri primi huius formae $4fgs \mp T$ quaesito satisfacient. Posteriore autem casu, quo formulae $f^m + 1$ et $g^m + 1$ divisorem habent $2m+1$, quia est

$$(fg)^m - 1 = f^m(g^m + 1) - f^m - 1,$$

huic formulae idem divisor conveniet. Pro hoc autem casu supra vidimus formam divisorum primorum esse

$$4fgs \mp \Theta^{(f)} \text{ et } 4gfs \mp \Theta^{(g)};$$

quare si ex valoribus litterae Θ pro numeris *f* et *g* ii, qui ipsis sunt communes, excerpantur, eos nunc etiam valoribus litterae *T* accenseri oportet; sicque omnes valores quaesiti litterae *T* obtinebuntur, si tam numeri formulis

$T^{(f)}$ et $T^{(g)}$ communes, quam etiam ii, quos formulae $\Theta^{(f)}$ et $\Theta^{(g)}$ communes habent, coniungantur atque usque ad terminum $4fg = 4a$ producantur; quem in finem iam supra valores harum litterarum ultra primam periodum continuavimus. His autem inventis reliqui numeri formae $4n+1$ hinc exclusi valores dabunt litterae Θ quos etiam ita colligere licet, ut eo referantur tam termini litteris $T^{(f)}$ et $\Theta^{(g)}$, quam litteris $T^{(g)}$ et $\Theta^{(f)}$ communes.

EXEMPLUM

31. Quia haec operatio facillime exemplo illustrabitur, sit $a = 15$ ideoque $f = 3$ et $g = 5$, pro quo utroque numero ex supra allatis depromantur valores litterarum T et Θ. Inde igitur habebimus:

$$\text{Pro } f = 3 \begin{cases} T^{(f)} = 1,\ 13,\ 25,\ 37,\ 49,\ 61. \\ \Theta^{(f)} = 5,\ 17,\ 29,\ 41,\ 53,\ 65. \end{cases}$$

$$\text{Pro } g = 5 \begin{cases} T^{(g)} = 1,\ 9,\ 21,\ 29,\ 41,\ 49,\ 61,\ 69. \\ \Theta^{(g)} = 13,\ 17,\ 33,\ 37,\ 53,\ 57,\ 73,\ 77, \end{cases}$$

quos valores ultra terminum $4a = 4fg = 60$ continuavimus.

Iam litterae $T^{(f)}$ et $T^{(g)}$ sequentes habent terminos communes: 1, 49, litterae autem $\Theta^{(f)}$ et $\Theta^{(g)}$ communes habent istos terminos: 17, 53, qui numeri coniunctim praebent valores litterae T pro isto casu. At pro littera Θ capiantur primo termini communes ex litteris $T^{(f)}$ et $\Theta^{(g)}$, qui sunt 13, 37; tum vero etiam numeri litteris $T^{(g)}$ et $\Theta^{(f)}$ communes, qui sunt 29, 41. Consequenter pro casu proposito $a = 15$ valores litterarum T et Θ per primam periodum, usque ad $4a = 60$ continuati, erunt:

$$T = 1,\ 17,\ 49,\ 53.$$
$$\Theta = 13,\ 29,\ 37,\ 41.$$

Hic scilicet occurrunt omnes numeri formae $4n+1$, qui quidem ad 15 sunt primi; et leviter attendenti patet totidem semper terminos in utrumque ordinem T et Θ ingredi.

SCHOLION

32. Quo haec postrema observatio melius intelligatur, regula haud adeo communis notetur, quae ostendit, quot ab unitate usque ad datum numerum N occurrant numeri ad ipsum primi, ubi quidem statim patet, si N fuerit ipse numerus primus, tum omnes praecedentes, quorum multitudo est $N-1$, simul quoque ad eum esse primos; sin autem N fuerit numerus utcunque compositus, semper repraesentari poterit hac forma generali

$$N = a^{\alpha} \cdot b^{\beta} \cdot c^{\gamma} \cdot d^{\delta} ....., ,$$

ubi *a, b, c* etc. denotant numeros primos; tum autem multitudo numerorum ad *N* primorum ipso que minorum erit

$$(a-1)a^{\alpha-1} \cdot (b-1)b^{\beta-1} \cdot (c-1)c^{\gamma-1} .....$$

Cum nunc nostro casu sit $N = 60 = 2^2 \cdot 3^1 \cdot 5^1$, erit multitudo numerorum ad *N* primorum ipsoque mimorum

$$= 1.2.\ 2.\ 4 = 16,$$

qui cum omnes sint impares et tam formae $4n+1$ quam formae $4n-1$, nostrae formae $4n+1$ tantum aderunt numeri 8, quorum semissis ad litteram *T,* reliqui vero ad litteram Θ referuntur. Utamur ergo hac regula inventa ad numeros *T* et Θ pro simplicioribus numeris *a* ex binis factoribus primis constantibus evolvendos:

1°. Sit $a = 2{\cdot}3;\ 4a = 24$.

$T = 1,\ 5$	$25, 29$	$49, 53$	$73, 77.$
$\Theta = 13, 17$	$37,\ 41$	$61,\ 65$	$85,\ 89.$

2°. Sit $a = 2 \cdot 5\ ;\ 4a = 40.$

$T =\ 1,\ 9, 13, 37$	$41, 49, 53, 77.$
$\Theta = 17, 21, 29, 33$	$57, 61, 69, 73.$

3°. Sit $a = 2 \cdot 7\ ; 4a = 56$.

$T = 1,\ \ 5,\ 9, 13, 25, 45$	$57,\ 61,\ 65,\ 69,\ 81,\ 101.$
$\Theta = 17, 29, 33, 37, 41, 53$	$73,\ 85,\ 89,\ 93,\ 97,\ 109.$

4°. Sit $a = 2 \cdot 11; 4a = 88$.

$T = 1,\ \ 9,\ 13,\ \ 21,\ 25,\ 29,\ 49,\ 61,\ 81,\ 85.$
$\Theta = 5,\ 17,\ 37,\ 41,\ 45,\ 53,\ 57,\ 65,\ 69,\ 73.$

5°. Sit $a = 2 \cdot 13;\ 4a = 104$.

$T =\ \ 1,\ 5,\ \ 9,\ 17,\ 21,\ 25,\ 37,\ 45,\ 49,\ 81,\ 85,\ \ 93.$
$\Theta = 29,\ 33,\ 41,\ 53,\ 57,\ 61,\ 69,\ 73,\ 77,\ 89,\ 97,\ 101.$

6°. Sit $a = 3{\cdot}5;\ 4a = 60$.

$T = 1, 17, 49, 53.$
$\Theta = 13, 29, 37, 41.$

7^{o}. Sit $a = 3 \cdot 7;\ 4a = 84$.

$T = 1, 5, 17, 25, 37, 41.$
$\Theta = 13, 29, 53, 61, 65, 73.$

PROBLEMA

33. *Si a fuerit numerus utcunque compositus, invenire valores litterarum T et Θ, qui illi conveniunt.*

SOLUTIO

Primo notetur, si *a* fuerit quadratum, puta *ff,* quia pro binis factoribus *f* et *f* tam litterae *T* quam Θ inter se conveniunt, omnes plane numeri formae $4m+1$, quatenus scilicet ad *f* sunt primi, ad ordinem *T* sunt referendi, ita ut ordo Θ plane vacuus relinquatur, id quod natura rei manifesto postulat. Cum enim sit $a = ff$, ideoque $a^m = f^{2m}$, semper formula $f^{2m} - 1$ divisibilis est per numerum primum $2m+1$, sicque forma a^{m+1} nunquam hunc divisorem admittit. Deinde si fuerit $a = ffg$, quoniam pro *ff* in ordine *T* omnes numeri occurrunt, in Θ vero nulli, manifestum est pro hoc casu in ordinem *T* eosdem numeros ingredi, qui pro simplici numero *g* sunt inventi; neque vero ex ambobus Θ ullus praeterea accedet, omitti vero debent ii numeri, qui ad *ff* non sunt primi. Denique si *a* fuerit productum ex pluribus numeris primis, veluti $a = fghk$; quaerantur pro factoribus *fg* et *hk* numeri ad ordines *T* et *e* referendi, ex quibus deinceps valores harum litterarum pro ipso numero *f* perinde concludentur, uti in Problemate praecedente.

EXEMPLUM

34. Sit $a = 30 = 2 \cdot 3 \cdot 5$, ideoque $4a = 120$; sumantur primo litterae *T* et Θ pro numero $3 \cdot 5 = 15$, qui autem usque ad 120 continuentur, qui sunt:

$$\text{pro } 3 \cdot 5 \begin{cases} T = 1, 17, 49, 53, 61, 77, 109, 113. \\ \Theta = 13, 29, 37, 41, 73, 89, 97, 101. \end{cases}$$

Cum his comparentur ambae formae factori 2 respondentes, atque termini communes utrique *T* reperiuntur

1, 17, 49, 113,

termini autem communes utriusque litterae Θ sunt

13, 29, 37, 101,

quocirca ordines quaesiti T et Θ pro numero $a = 30$ erunt:

$T =$ 1, 13, 17, 29, 37, 49, 101, 113 etc.

$\Theta =$ 41, 53, 61, 73, 77, 89, 97, 109 etc.

SCHOLION

35. Colligamus iam omnia hactenus inventa, ac pro omnibus numeris *a,* exceptis ipsis quadratis, usque ad 30 formas numerorum primorum $2m+1$ ordine exhibeamus, per quos vel $a^m - 1$ vel $a^m + 1$ fit divisibilis:

a.	$2m+1$	$a^m \mp 1$
2.	$8s \mp 1,$	$2^m - 1.$
	$8s \mp 5,$	$2^m + 1.$
3.	$12s \mp 1,$	$3^m - 1.$
	$12s \mp 5,$	$3^m + 1.$
5.	$20s \mp 1,9.$	$5^m - 1.$
	$20s \mp 13,17,$	$5^m + 1.$
6.	$24s \mp 1,5,$	$6^m - 1.$
	$24s \mp 13,17,$	$6^m + 1.$
7.	$28s \mp 1, 9,25,$	$7^m - 1.$
	$28s \mp 5,13,17,$	$7^m + 1.$
8.	$32s \mp 1, 9,17,25,$	$8^m - 1.$
	$32s \mp 5,13,21,29,$	$8^m + 1.$
10.	$40s \mp 1, 9,13,37,$	$10^m - 1.$
	$40s \mp 17,21,29,33,$	$10^m + 1.$
11.	$44s \mp 1, 5, 9, 13,37,$	$11^m - 1.$
	$44s \mp 13,17,21,29,41,$	$11^m + 1.$
12.	$48s \mp 1,13,25, 37,$	$12^m - 1.$
	$48s \mp 5,17,29,41,$	$12^m + 1.$
13.	$52s \mp 1, 9,17,25,29,49,$	$13^m - 1.$
	$52s \mp 5,21,33,37,41,45,$	$13^m + 1.$
14.	$56s \mp 1, 5, 9,13,25,45,$	$14^m - 1.$
	$56s \mp 17,29,33,37,41,53,$	$14^m + 1.$

15.	$60s \mp 1,17,49,53,$ $60s \mp 13,29,37,41,$	$15^m - 1.$ $15^m + 1.$
17.	$68s \mp 1, 9, 13,21,25,33,49,53,$ $68s \mp 5,29,37,41,45,57,61,65,$	$17^m - 1.$ $17^m + 1.$
18.	$72s \mp 1,17,25,41,49,65,$ $72s \mp 5,13,29,37,53,61,$	$18^m - 1.$ $18^m + 1.$
19.	$76s \mp 1, 5, 9,17,25,45,49,61,73,$ $76s \mp 13,21,29,33,37,41,53,65,69,$	$19^m - 1.$ $19^m + 1.$
20.	$80s \mp 1, 9,21,29,41,49,61,69,$ $80s \mp 13,17,33,37,53,57,73,77,$	$20^m - 1.$ $20^m + 1.$
21.	$84s \mp 1, 5,17,25,37,41,$ $84s \mp 13,29,53,61,65,73,$	$21^m - 1.$ $21^m + 1.$
22.	$88s \mp 1, 9, 13, 21,25,29,49,61,81,85,$ $88s \mp 5,17,37,41,45,53,57,65,69,73,$	$22^m - 1.$ $22^m + 1.$
23.	$92s \mp 1, 9, 13,25,29,41,49,73,77,81,85,$ $92s \mp 5,17,21,33,37,45,53, 57,61,65,89,$	$23^m - 1.$ $23^m + 1.$
24.	$96s \mp 1, 5,25,29,49,53,73,77,$ $96s \mp 13,17,37,41,61,65,85,89,$	$24^m - 1.$ $24^m + 1.$
26.	$104s \mp 1, 5, 9,17,21,25,37,45,49,81,85, 93,$ $104s \mp 29,33,41,53,57,61,69,73,77,89,97,101,$	$26^m - 1.$ $26^m + 1.$
27.	$108s \mp 1,13,25,37,49,61,73,85, 97,$ $108s \mp 5,17,29,41,53,65,77,89,101,$	$27^m - 1.$ $27^m + 1.$
28.	$112s \mp 1, 9,25,29,37,53,57,65,81,85,93,109$ $112s \mp 5,13,17,33,41,45,61,69,73,89,97,101,$	$28^m - 1.$ $28^m + 1.$
29.	$116s \mp 1, 5, 9,13,25,33,45,49,53,57,65, 81, 93,109,$ $116s \mp 17,21,37,41,61,69,73,77,85,89,97,101,105,113.$	$29^m - 1.$ $29^m + 1.$
30.	$120s \mp 1,13,17,29,37,49,101,113,$ $120s \mp 41,53,61,73,77,89, 97,109,$	$30^m - 1.$ $30^m + 1.$

Nunc igitur omnia, quae ante fuerant tradita, satis clare perspicere licet atque in hoc genere nihil aliud superesse videtur, quam ut binae illae conclusiones ex observationibus deductae firmis demonstrationibus muniantur.

Postquam pro quovis numero *a,* sive primo, sive composito, valores litterarum

T et Θ fuerint inventi, sequentia duo Theoremata notari merentur:

I. *Omnes divisores primi formae* $xx - ayy$ *in alterutra harum formarum :*
$4as + T$, *vel* $4as - T$ *continentur.*
II. *Omnes divisores primi huius formae :* $xx + ayy$ *in alterutra harum formularum:* $4as + T$ *vel* $4as - \Theta$ *continentur.*

Sponte autem patet pro x et y eiusmodi numeros sumi debere, ut bina membra xx et ayy nullum habeant divisorem communem.