10.

De aequatione $x^{2\lambda}+y^{2\lambda}=z^{2\lambda}$ per numeros integros resolvenda.

(Auctore, *E. E. Kummer*, Dr. phil., praeceptore gymnasii Ligunicensis.)

Quod clarissimus *Fermat* contendit: aequationem $x^{n+2}+y^{n+2}=z^{n+2}$ per numeros integros resolvi non posse, haud dubie ad elegantissima theoremata referendum est, quae de numerorum proprietatibus hactenus proposita sunt, cujus autem demonstratio gravissimis difficultatibus videtur laborare. Quamquam enim incrementa permagna nostris temporibus theoria numerorum accepit, tamen geometrae clarissimi, qui huic theoremati operam tribuerunt, paucos solummodo casus simpliciores demonstrationibus munire potuerunt. *Cl. Euler, Legendre* et *Lejeune Dirichlet* pro potestatibus tertiis, quartis, quintis et decimis quartis theorematis hujus demonstrationes invenerunt, quae in eo conveniunt, ut ex aequatione proposita alia ejusdem formae aequatio eliciatur, cujus numeri variabiles minores sint quam aequationis datae variabiles; artificia autem per quae ad hanc aequationem similem pervenerunt, pro potestatibus diversis maxime diversa sunt, neque ad alios casus applicationes patiuntur. Itaque res non multum profecit. In re tam difficili, nisi omni proventu carere volumus, a facilioribus incipiendum esse nobis necessarium videtur, itaque aequationem Fermatianam pro potestatum indicibus paribus, nobis tractandam proponimus. Hanc etiam disquisitionem faciliorem ad finem perducere nondum nobis contigit, attamen summas aliquas, quae hanc rem quodammodo promovere videntur cum geometris communicabimus.

Disquisitio nostra praesertim huic theoremati innititur:

Theorema 1. „Si n est numerus primus, atque a et b inter se primi, quantitates $a\pm b$ et $\frac{a^n\pm b^n}{a\pm b}$ non habet factorem communem, nisi numerum n, si vero $a^n\pm b^n$ habet factorem n, eundem etiam $a\pm b$ habere debet, et numerus factorum n in $a^n\pm b^n$ numerum factorum n in $a\pm b$ unitate superat."

Hujus theorematis veritas facile probatur ex aequatione identica

$$1.\quad \frac{a^n\pm b^n}{a\pm b} = (a\pm b)^{n-1}\mp n(a\pm b)^{n-3}ab+\frac{n(n-3}{1.2.}(a\pm b)^{n-5}a^2b^2\mp\ldots.$$
$$\ldots.(\mp 1)^h\frac{n(n-h-1)(n-h-2)\ldots.(n-2h+1)}{1.2.3\ldots.h}(a\pm b)^{n-2h-1}a^hb^h+\ldots(\mp 1)^{\frac{n-1}{2}}n(ab)^{\frac{n-1}{2}}.$$

Si enim $\frac{a^n\pm b^n}{a\pm b}$ et $a\pm b$ factorem communem habent, etiam $n(ab)^{\frac{n-1}{2}}$ (terminus solus ad dextram aequationis (1.), qui factorem $a\pm b$ non continet) per eundem factorem divisibilis esse debet, et quia ab et $a\pm b$ inter se primi sunt, maximus factor communis quem quantitates $\frac{a^n\pm b^n}{a\pm b}$ et $a\pm b$ habere possunt, erit numerus n. Ad alteram theorematis partem demonstrandam observo coefficientes omnes

$$\frac{n}{1},\quad \frac{n(n-3)}{1.2.},\quad \ldots.\quad \frac{n(n-h-1)(n-h-2)\ldots.(n-2h+1)}{1.2.3\ldots.h},\quad \ldots.$$

quia integri sunt, et numerus primus n e numeratore per denominatoris factores minores tolli nequit, per n esse divisibiles. Inde sequitur $a^n\pm b^n$ factorem n continere non posse, nisi simul $a\pm b$ per n est divisibilis, positisque $a^n\pm b^n = C.n^\varkappa$ et $a\pm b = c.n^\lambda$ ex aequatione (1.) sequitur $\lambda=\varkappa-1$, id quod demonstrandum erat.

Quibus praeparatis ad aequationem propositam vertamur:

$$2.\quad x^{2\lambda}+y^{2\lambda}=z^{2\lambda}.$$

Salva quaestionis generalitate numeros x, y, z inter se primos accipimus, et λ numerum primum, si enim duo numerorum x, y, z factorem communem haberent, per eundem etiam tertius numerus divisibilis esset, atque hic factor omnium communis tolleretur, porro si λ esset numerus compositus e factoribus primis $\lambda=\alpha.\beta.\gamma.\ldots$, aequatione $x^{2\lambda}+y^{2\lambda}=z^{2\lambda}$ satisfieri non posset, nisi aequationes $x'^{2\alpha}+y'^{2\alpha}=z'^{2\alpha}$, $x''^{2\beta}+y''^{2\beta}=z''^{2\beta}$ etc. omnes simul per numeros integros solvi possent. Praeterea patet numerorum x, y, z unum parem ceteros impares esse et quia summa duorum quadratorum inter se primorum per altiorem potestatem ipsius 2 non est divisibilis, sequitur hunc numerum parem non esse z, sed alterum numerorum x et y. Hunc numerum parem nos ubique accipiemus esse y.

Jam theorema supra demonstratum ad aequationem propositam applicemus. Cui si forma datur:

$$3.\quad (z^2-y^2)\left(\frac{z^{2\lambda}-y^{2\lambda}}{z^2-y^2}\right) = x^{2\lambda}.$$

patet primo, si x factorem λ non continet, quia z^2-y^2 et $\frac{z^{2\lambda}-y^{2\lambda}}{z^2-y^2}$ inter se primi sunt, esse

$$4. \quad z^2-y^2=a^{2\lambda}$$

et quia $z+y$ et $z-y$ factorem communem non habent

$$5. \quad z+y=v^{2\lambda}, \quad z-y=\omega^{2\lambda}.$$

Si vero x per λ divisibilis est, maximaque potestas ipsius λ quae in x continetur est λ^{μ}, $x^{2\lambda}$, ideoque $z^{2\lambda}-y^{2\lambda}$ habent factorem $\lambda^{2\lambda\mu}$, itaque per theorema (1.) z^2-y^2 continebit factorem $\lambda^{2\lambda\mu-1}$, denique quia solo factore communi λ excepto z^2-y^2 et $\frac{z^{2\lambda}-y^{2\lambda}}{z^2-y^2}$ inter se primi sunt, esse debet

$$6. \quad z^2-y^2=\lambda^{2\lambda\mu-1}a^{2\lambda}$$

unde

$$7. \quad z\pm y=\lambda^{2\lambda\mu-1}v^{2\lambda}, \quad z\mp y=\omega^{2\lambda}.$$

Simili modo ex aequatione $z^{2\lambda}-x^{2\lambda}=y^{2\lambda}$, si y factorem λ non continet, sequitur

$$8. \quad z^2-x^2=b^{2\lambda}.$$

Per hypothesin est y numerus par, z et x impares, itaque si maxima potestas ipsius 2, quae in y continetur est 2^{ν}, $z^{2\lambda}$ habet factorem $2^{2\lambda\nu}$, eundem factorem habet z^2-x^2, inde quia maximus divisor communis numerorum $z+x$ et $z-x$ est 2, sequitur

$$9. \quad z\pm x=2.p^{2\lambda}, \quad z\mp x=2^{2\lambda\nu-1}.q^{2\lambda}.$$

Si vero y per λ divisibilis est, et maxima potestas ipsius λ quae in y continetur est λ^{μ}, per theorema (1.) erit

$$10. \quad z^2-x^2=\lambda^{2\lambda\mu-1}b^{2\lambda}.$$

Praeterea si accipimus maximam potestatem numeri 2 quae in y continetur esse 2^{ν}, quia etiam b eundem factorem 2^{ν} habere debet, erit

$$11. \quad \text{sive } z\pm x=2.p^{2\lambda} \quad \text{et } z\mp x=2^{2\lambda\nu-1}.\lambda^{2\lambda\mu-1}.q,$$
$$12. \quad \text{sive } z\pm x=2.\lambda^{2\lambda\mu-1}p^{2\lambda} \quad \text{et } z\pm x=2^{2\lambda\nu-1}.q^{2\lambda}.$$

Inde quatuor casus speciales erunt discernendi, primus quo neuter numerornm x et y per λ est divisibilis, secundus quo numerus impar x factorem λ habet, tertius et quartus casus, quibus numerus par y per λ divisibilis est. Pro singulis iis casibus est:

$$13. \begin{cases} \text{I. } z+y=v^{2\lambda}, & z-y=\omega^{2\lambda}, & z\pm x=2p^{2\lambda}, & z\mp x=2^{2\lambda\nu-1}q^{2\lambda}, \\ \text{II. } z\pm y=\lambda^{2\lambda\mu-1}.v^{2\lambda}, & z\mp y=\omega^{2\lambda}, & z\pm x=2p^{2\lambda}, & z\mp x=2^{2\lambda\nu-1}q^{2\lambda}, \\ \text{III. } z+y=v^{2\lambda}, & z-y=\omega^{2\lambda}, & z\pm x=2p^{2\lambda}, & z\mp x=2^{2\lambda\nu-1}.\lambda^{2\lambda\mu-1}.q^{2\lambda}, \\ \text{IV. } z+y=v^{2\lambda}, & z+y=\omega^{2\lambda}, & z\pm x=2.\lambda^{2\lambda\mu-1}.p^{2\lambda}, & z\mp x=2^{2\lambda\nu-1}.q^{2\lambda}, \end{cases}$$

ex quibus deducuntur formae numerorum x, y, z:

$$14.\quad \begin{cases} \text{I. } z=\dfrac{v^{2\lambda}+\omega^{2\lambda}}{2}, & y=\dfrac{v^{2\lambda}-\omega^{2\lambda}}{2}, \\ \quad z=p^{2\lambda}+2^{2\lambda n-2}.q^{2\lambda}, & \pm x=p^{2\lambda}-2^{2\lambda n-2}.q^{2\lambda}; \\ \text{II. } z=\dfrac{\lambda^{2\lambda\mu-1}.v^{2\lambda}+\omega^{2\lambda}}{2}, & \pm y=\dfrac{\lambda^{2\lambda\mu-1}v^{2\lambda}-\omega^{2\lambda}}{2}, \\ \quad z=p^{2\lambda}+2^{2\lambda\nu-2}q^{2\lambda}, & \pm x=p^{2\lambda}-2^{2\lambda\nu-2}q^{2\lambda}; \\ \text{III. } z=\dfrac{v^{2\lambda}+\omega^{2\lambda}}{2}, & y=\dfrac{v^{2\lambda}-\omega^{2\lambda}}{2}, \\ \quad z=p^{2\lambda}+2^{2\lambda n-2}.\lambda^{2\lambda\mu-1}.q^{2\lambda}, & \pm x=p^{2\lambda}-2^{2\lambda\nu-2}.\lambda^{2\nu\mu-1}.q^{2\lambda}; \\ \text{IV. } z=\dfrac{v^{2\lambda}+\omega^{2\lambda}}{2}, & y=\dfrac{v^{2\lambda}-\omega^{2\lambda}}{2}, \\ \quad z=\lambda^{2\lambda\mu-1}.p^{2\lambda}+2^{2\lambda\nu-2}.q^{2\lambda}, & \pm x=\lambda^{2\lambda\mu-1}.p^{2\lambda}-2^{2\lambda\nu-2}.q^{2\lambda}; \end{cases}$$

formisque binis ipsius z aequalibus positis est

$$15.\quad \begin{cases} \text{I. } v^{2\lambda}+\omega^{2\lambda} &= 2p^{2\lambda}+2^{2\lambda\nu-1}.q^{2\lambda}, \\ \text{II. } \lambda^{2\lambda\mu-1}.v^{2\lambda}+\omega^{2\lambda} &= 2p^{2\lambda}+2^{2\lambda\nu-1}.q^{2\lambda}, \\ \text{III. } v^{2\lambda}+\omega^{2\lambda} &= 2p^{2\lambda}+2^{2\lambda n-1}.\lambda^{2\lambda\mu-1}.q^{2\lambda}, \\ \text{IV. } v^{2\lambda}+\omega^{2\lambda} &= 2.\lambda^{2\lambda\mu-1}.p^{2\lambda}+2^{2\lambda\nu-1}.q^{2\lambda}. \end{cases}$$

In omnibus iis aequationibus numeri v, ω, p et q impares et inter se primi sunt, numeri v et ω factores ipsius x, et p et q factores numeri y.

Ex aequatione proposita $x^{2\lambda}+y^{2\lambda}=z^{2\lambda}$, sequitur etiam $(z^{\lambda}+y^{\lambda})(z^{\lambda}-y^{\lambda})=x^{2\lambda}$, et quia factores $z^{\lambda}+y^{\lambda}$ et $z^{\lambda}-y^{\lambda}$ inter se primi sunt:

$$16.\quad z^{\lambda}+y^{\lambda}=A^{2\lambda},\qquad z^{\lambda}-y^{\lambda}=B^{2\lambda},$$

simili modo est $(z^{\lambda}\pm x^{\lambda})(z^{\lambda}\mp x^{\lambda})=y^{2\lambda}$, unde quia maximus factor communis numerorum $z^{\lambda}\pm x^{\lambda}$ et $z^{\lambda}\mp x^{\lambda}$ est 2, et per hypothesin maxima potestas ipsius 2, quam y continet est 2^{ν}, habetur

$$17.\quad z^{\lambda}\pm x^{\lambda}=2.C^{2\lambda},\qquad z^{\lambda}\mp x^{\lambda}=2^{2\lambda\nu-1}.D^{2\lambda}.$$

Signa ambigua $\pm$ et $\mp$ ita accipienda sunt, ut cum signis aequationum (13.), (14.) et (15.) conveniant, ubi enim in illis aequationibus signa superiora vel inferiora valent, eadem etiam in his valebunt.

Quum probabile sit omnes quatuor casus quos supra separavimus non pro omnibus numeris λ locum habituros esse, dijudicandum videtur: quinam casus ad certos numeros λ possint pertinere. Primum accipiamus numerum primum λ talem esse ut etiam $2\lambda+1$ sit numerus primus, id quod ex. gr. evenit pro numeris $\lambda=3, 5, 11, 23, 29, 41, 53, \ldots$ et pro aliis innumeris. Quo posito inquiramus an aequationum (13.) utraeque partes secundum modulum $2\lambda+1$ congruae esse possint. Quia per

cognitum theorema omnis potestas $2\lambda^{ta}$ unitati congrua est modulo $2\lambda+1$ (numero primo) nisi per $2\lambda+1$ est divisibilis, facile cognosci potest aequationum (15.) casus I. et III. consistere non posse, nisi q per $2\lambda+1$ divisibilis sit, sed casus II. et IV. nullomodo locum habere (casu $\lambda=3$ excepto). Praeterea demonstrari potest etiam primum casum rejiciendum esse, est enim identice

$$18. \quad \frac{z^{2\lambda}-x^{2\lambda}}{z^2-x^2} = (z^2-x^2)^{\lambda-1}+\lambda(z^2-x^2)^{\lambda-3}z^2x^2+\ldots+\lambda(zx)^{\lambda-1},$$

porro est $z^{2\lambda}-x^{2\lambda}=y^{2\lambda}$, et casu primo, de quo agitur, $z^2-x^2=2^{2\lambda\nu}.p^{2\lambda}.q^{2\lambda}$, ergo $\frac{z^{2\lambda}-x^{2\lambda}}{z^2-x^2}$ est potestas $2\lambda^{ta}$, quae sit $y'^{2\lambda}$. Cum supra inventum sit casu primo numerum q per $2\lambda+1$ divisibilem esse debere, etiam z^2-x^2 hunc factorem contineat necesse est; itaque ex aequatione (18.), terminis per z^2-x^2 sive per $2\lambda+1$ divisibilibus omissis, habemus congruentiam:

$$19. \quad y'^{2\lambda} \equiv \lambda(zx)^{\lambda-1} \pmod{2\lambda+1}.$$

Denique ex aequationibus $z=p^{2\lambda}+2^{2\lambda\nu-2}q^{2\lambda}$ et $\pm x=p^{2\lambda}-2^{2\lambda\nu-2}q^{2\lambda}$ sequitur $\pm x\equiv 1$ et $z\equiv 1$ modulo $2\lambda+1$, unde $(zx)^{\lambda-1}\equiv 1 \pmod{2\lambda+1}$; itaque congruentia 19. mutatur in

$$20. \quad y'^{2\lambda} \equiv \lambda \pmod{2\lambda+1},$$

quae congruentia nullomodo locum habere potest. Solus igitur remanet casus tertius, atque habemus

Theorema 2. „Si praeter λ etiam $2\lambda+1$ est numerus primus, aequatio $x^{2\lambda}+y^{2\lambda}=z^{2\lambda}$ per numeros integros solvi nequit, nisi y, qui est numerus par, simul per λ et per $2\lambda+1$ divisibilis est, et numerorum x, y, z formae sunt: $z=\frac{v^{2\lambda}+\omega^{2\lambda}}{2}$, $y=\frac{v^{2\lambda}-\omega^{2\lambda}}{2}$, $z=p^{2\lambda}+2^{2\lambda\nu-2}.\lambda^{2\lambda\mu-1}.q^{2\lambda}$, $\pm x=p^{2\lambda}-2^{2\lambda\nu-2}\lambda^{2\lambda\mu-1}.q^{2\lambda}$."

Consideramus etiam residua, quae aequationes (15.) dant modulo 8. Quum numerorum imparium p, q, v, ω quadrata sive potestates pares unitati congrua sint modulo 8, ex aequationibus illis habemus congruentias: pro casu secundo: $1+\lambda\equiv 2 \pmod{8}$, et pro quarto casu: $1+1\equiv 2\lambda \pmod{8}$, unde elucet casum secundum non posse locum habere nisi λ habeat formam $8n+1$, neque casum quartum nisi sit $\lambda=4n+1$. Generalius autem demonstrari potest.

Theorema 3. „Casus primus, secundus et quartus non possunt locum habere nisi λ habet formam $8n+1$, pro ceteris formis numeri λ, $8n+3$, $8n+5$ et $8n+7$ solus casus tertius locum habere potest."

Hoc theorema demonstratur ex aequatione identica

$$21. \quad \frac{z \mp x^\lambda}{z \mp x} = (z \mp x)^{\lambda-1} \pm \lambda (z \mp x)^{\lambda-3} xz + \ldots + \lambda (\pm xz)^{\frac{\lambda-1}{2}}$$

est enim pro casibus I., II. et IV. $z^\lambda \mp x^\lambda = 2^{2\lambda\nu-2} D^{2\lambda}$ et $z \mp x = 2^{2\lambda\nu-1} q^{2\lambda}$, ergo

$$22. \quad \frac{z^\lambda \mp x^\lambda}{z \mp x} = E^{2\lambda}$$

inde, terminis per 8 divisibilibus omissis, aequatio (21.) mutatur in congruentiam

$$23. \quad E^{2\lambda} \equiv \lambda (\pm xz)^{\frac{\lambda-1}{2}} \pmod 8$$

porro e formis numerorum $\mp x$ et z, ad (14.) notatis sequitur esse ubique $\pm xz \equiv 1 \pmod 8$, itaque congruentia (23.) mutatur in

$$24. \quad 1 \equiv \lambda \pmod 8$$

quae congruentia continet theorema pronunciatum.

Revertimur ad aequationes (17.) quae in hanc formam redigi possunt:

$$25. \quad z^\lambda - C^{2\lambda} = 2^{2\lambda\nu-2} . D^{2\lambda}, \quad C^{2\lambda} \mp x^\lambda = 2^{2\lambda\nu-2} D^{2\lambda}.$$

Casibus I., II., et IV. $z \mp x$ factorem λ non continet, pro iis igitur casibus neque $z^\lambda \mp x$, neque D factorem λ potest continere, itaque per theorema primum ex aequationibus (25.) sequuntur:

$$26. \quad z - C^2 = 2^{2\lambda\nu-2} r^{2\lambda}, \quad C^2 \mp x = 2^{2\lambda\nu-2} . s^{2\lambda},$$

ex iisque additis:

$$27. \quad z \mp x = 2^{2\lambda\nu-2} (r^{2\lambda} + s^{2\lambda}),$$

et quia pro casibus I. II. et IV. est $z \mp x = 2^{2\lambda\nu-2} q^{2\lambda}$, habemus

$$28. \quad r^{2\lambda} + s^{2\lambda} = 2 . q^{2\lambda}.$$

Pro casu tertio $z \mp x$ continet factorem $\lambda^{2\lambda\mu-1}$, ergo $z^\lambda \mp x^\lambda$ factorem habebit $\lambda^{2\lambda\mu}$, et D factorem λ^μ, inde per theorema primum ex aequationibus (25.) pro hoc tertio casu deducuntur

$$29. \quad z - C^2 = 2^{2\lambda\nu-2} . \lambda^{2\lambda\mu-1} . r^{2\lambda}, \quad C^{2\lambda} \mp x = 2^{2\lambda\nu-2} . \lambda^{2\lambda\mu-1} . s^{2\lambda},$$

quibus additis:

$$30. \quad z \mp x = 2^{2\lambda\nu-2} . \lambda^{2\lambda\mu-2} . (r^{2\lambda} + s^{2\lambda})$$

et quia pro casu tertio invenimus $z \mp x = 2^{2\lambda\nu-1} . \lambda^{2\lambda\mu-1} . q^{2\lambda}$ est

$$31. \quad r^{2\lambda} + s^{2\lambda} = 2 . q^{2k}.$$

Numeri r, s, et q aequationum (28.) et (31.) factores sunt numeri D, ideoque etiam numeri D, ideoque etiam numeri y, eaeque aequationes continent theorema insigne:

Theorema 4. „Si aequatio $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ per numeros integros solvi potest, semper inveniri possunt numeri tres, r, s et q, numeri y, ejusmodi ut satisfaciant aequationi $r^{2\lambda} + s^{2\lambda} = 2 . q^{2\lambda}$."

De numeris r, s, et q pauca adjicienda esse videntur. Per numeros x, y et z determinantur hoc modo:

casu I., II. et IV.

$$32.\quad z-\left(\frac{z^\lambda \pm x^\lambda}{2}\right)^{\frac{1}{\lambda}} = 2^{2\lambda\nu-2}.r^{2\lambda},$$

$$33.\quad \left(\frac{z^\lambda \pm x^\lambda}{2}\right)^{\frac{1}{\lambda}} \mp x = 2^{2\lambda\nu-2}.s^{2\lambda},$$

$$34.\quad z \mp x = 2^{2\lambda\nu-1}.q^{2\lambda},$$

casu III.

$$35.\quad z-\left(\frac{z^\lambda \pm x^\lambda}{2}\right)^{\frac{1}{\lambda}} = 2^{2\lambda\nu-2}.\lambda^{2\lambda\mu-1}.r^{2\nu},$$

$$36.\quad \left(\frac{z^\lambda \pm x^\lambda}{2}\right)^{\frac{1}{\lambda}} \pm x = 2^{2\lambda\nu-2}.\lambda^{2\lambda\mu-1}.s^{2\lambda},$$

$$37.\quad z \mp x = 2^{2\lambda\nu-1}.\lambda^{2\lambda\mu-1}.q^{2\lambda}.$$

Fieri potest ut numeri r, s, et q, quos hae aequationes praebent, factores communes habeant, qui vero, cum omnium trium communes esse debeant, ex aequatione $r^{2\lambda}+s^{2\lambda}=2.q^{2\lambda}$ tolli poterunt. Praeterae contendo, iis factoribus communibus sublatis, numerorum r et s factores omnes formam $2\lambda n+1$ habere. Notum est enim formae $z^\lambda \mp x^\lambda$ factores omnes, qui non sunt factores ipsius $z \mp x$, hanc formam habere, unde sequitur omnes etiam factores ipsius D, qui non sint factores ipsius $z \mp x$, sive ipsius q, eandem formam habere. Quum vero numeri r et s factores sint numeri D, e quibus per hyp. factores cum q communes sublati sunt, sequitur omnes eorum factores formam $2\lambda n+1$ habere. Si certum aliquem factorem primum numeri r accipimus esse $2\lambda m+1$, ex aequatione $r^{2\lambda}+s^{2\lambda}=2q^{2\lambda}$ habemus congruentiam

$$38.\quad s^{2\lambda} \equiv 2.q^{2\lambda} \pmod{2\lambda m+1}$$

unde

$$39.\quad s^{2\lambda m} \equiv 2^m.q^{2\lambda m} \pmod{2\lambda m+1}$$

et quia per hyp. numerus $2\lambda m+1$ est primus, esse debet

$$s^{2\lambda m} \equiv 1 \quad \text{et} \quad q^{2\lambda m} \equiv 1 \quad \text{modulo } 2\lambda m+1,$$

itaque

$$40.\quad 2^m \equiv 1 \pmod{2\lambda m+1}$$

huic igitur congruentiae omnes factores primi numeri r satisfacere debent, et apertum est hoc idem de factoribus primis numeri s valere.

Lignicii Oct. 1835.