II. Si p, q, r, s etc. fuerint primi inter se diversi, fueritque $a = b^{q-1}$ erit $(a^p - a) :: pq$. Porro $a = b^{(q-1)(r-1)}$ erit $(a^p - a) :: pqr$ et ita porro.

III. Si fuerit tam $(x^m - y^m) :: P$ quam $(x^n - y^n) :: P$, sitque $m > n$, erit quoque $(x^{m-n} - y^{m-n}) :: P$, si quidem x et y sint numeri inter se primi.

Demonstratio. Posterior formula ducta in x^{m-n} a priore subtrahatur, erit residuum

$$x^{m-n}y^n - y^m = y^n(x^{m-n} - y^{m-n}),$$

quod ergo etiam est divisibile per P, et quia y^n non est divisibile, necesse est ut $(x^{m-n} - y^{m-n}) :: P$.

IV. Si ut ante tam $(x^m - y^m) :: P$ quam $(x^n - y^n) :: P$ atque inter numeros m et n maximus communis divisor fuerit Δ, tum etiam $(x^\Delta - y^\Delta) :: P$.

Demonstratio. Ponatur $m = \mu\Delta$ et $n = \nu\Delta$, et quia Δ est maximus communis divisor, erunt μ et ν primi inter se. Dari igitur poterunt numeri α et β, ut sit $\alpha\mu - \beta\nu = 1$. Hinc igitur quoque erit $(x^{\alpha m} - y^{\alpha m}) :: P$ similique modo $(x^{\beta n} - y^{\beta n}) :: P$, unde per praecedens theorema erit $(x^{\alpha m - \beta n} - y^{\alpha m - \beta n}) :: P$. Est vero exponens $\alpha m - \beta n = \alpha\mu\Delta - \beta\nu\Delta = \Delta$, consequenter erit $(x^\Delta - y^\Delta) :: P$.

A. m. T. III. p. 174. 175.

B. Partitio numerorum in summas polygonalium.

32.

(Léonard Euler.)

Caractère général pour juger, si un nombre entier quelconque N *est somme de trois triangles, tous les nombres plus petits étant tels.*

Soit $N - A$ un nombre moindre quelconque qui soit égal à ces trois triangles: $\Delta p + \Delta q + \Delta r$; ensuite, prenant pour a et b des nombres quelconques et posant $A = ab$, s'il arrive que $p - q$, ou $p - r$, ou $q - r$ soit égal à $a - b$, alors le nombre proposé N sera somme de trois triangles, et un seul cas de a et b suffit pour cela.

(Lexell.)

Demonstration. Ayant posé $N - ab = \Delta p + \Delta q + \Delta r$, soit $p - q = a - b$, et pour cet effet mettons $p = x + a$ et $q = x + b$, de sorte que

$$N - ab = \Delta(x + a) + \Delta(x + b) + \Delta r.$$

Alors je dis qu'on aura

$$N = \Delta(x + a + b) + \Delta x + \Delta r;$$

car puisque

$$\Delta(x + a + b) = \frac{xx + 2(a + b)x + (a + b)^2 + x + a + b}{2},$$

on aura

$$N = \frac{1}{2}(xx + 2(a + b)x + (a + b)^2 + x + a + b) + \frac{xx + x}{2} + \Delta r.$$

Mais la première formule donne

$$N - ab = \frac{x^2 + 2ax + a^2 + x + a}{2} + \frac{x^2 + 2bx + b^2 + x + b}{2} + \Delta r$$

ce qui étant ôté de celle-là donne $ab = ab$, ce qu'il fallait démontrer.

Coroll. 1. Puisque $p - q = a - b$ et $p = x + a$ et $q = x + b$, on aura

$$x = p - a = q - b, \text{ donc } x + a + b = p + b = q + a;$$

par conséquent, dès qu'on aura

$$N - ab = \Delta p + \Delta(p - a + b) + \Delta r, \text{ il s'en suit } N = \Delta(p + b) + \Delta(p - a) + \Delta r.$$

Coroll. 2. Qu'on prenne $b = a$, et dès lors il arrive que $N - aa = \Delta p + \Delta p + \Delta r$, c'est à dire que si deux de ces triangles sont égaux entre eux, on en déduira

$$N = \Delta(p + a) + \Delta(p - a) + \Delta r.$$

Exemple. Prenons $N = 17$ et successivement $a = 1, 2, 3, 4$, etc. nous aurons

1. $a=1$ donc $17-1=10+3+3$ ou $17=10+6+1$
2. $a=2$, on aura $17-4=13=1+6+6$ donc $17=1+1+15$
3. $a=3$, on aura $17-9=8=6+1+1$ donc $17=6+10+1$
4. $a=4$, on aura $17-16=1=1+0+0$ donc $17=1+1+15$

Caractères semblables pour la résolution des nombres en quatre carrés.

Soit le nombre proposé $=N$ et un nombre plus petit quelconque $N-2ab$ qui soit $=pp+qq+rr+ss$. S'il arrive que $p-q=a-b$, ou bien $p=q+a-b$, $q=p-a+b$, alors on aura $N=(p+b)^2+(q-a)^2+rr+ss$; car celle-là

$$N=2ab+pp+pp-2p(a-b)+(a-b)^2+rr+ss$$

et celle-ci

$$N=\quad pp+pp+2pb-2ap+bb+aa+rr+ss$$

sont évidemment égales.

Coroll. Prenant $b=a$, si parmi les quatre carrés dont la somme donne $N-2aa$, deux se trouvent égaux entre eux, de sorte que $N-2aa=2pp+rr+ss$, alors on aura

$$N=(p+a)^2+(p-a)^2+rr+ss.$$

Exemples. Soit proposé le nombre $N=71$ et soit

1. $a=1$, on aura $71-2=69=4+4+36+25$ d'où l'on conclut $71=9+1+36+25$.
2. Prenant $a=2$, on aura $71-8=63=9+9+9+36$, et partant $71=36+9+1+25$.
3. Soit $a=3$ et puisque $71-18=53=49+4+0+0$, il s'en suit $71=49+4+9+9$.
4. Soit $a=4$; puisque $71-32=39=36+1+1+1$, il y aura $71=36+1+25+9$.
5. Soit $a=5$; puisque $71-50=21=4+4+4+9$, donc $71=9+4+49+9$.

A. m. T. I. p. 92. 93.

33.

(N. Fuss I.)

Problema. Si omnes numeri minores quam N sint resolubiles in tres numeros trigonales, ipsum numerum N etiam in tres trigonales resolvere.

Solutio. Sint x, y et z radices numerorum trigonalium, quorum summa aequetur numero N, ita ut sit

$$N=\frac{xx+x}{2}+\frac{yy+y}{2}+\frac{zz+z}{2}.$$

Jam consideretur numerus minor quicunque $N-p$, pro quo radices trigonalium sint a, b, c, ut sit

$$N-p=\frac{aa+a}{2}+\frac{bb+b}{2}+\frac{cc+c}{2}.$$

Sumamus autem hic esse $b=a+d$; tum vero statuatur $z=c$, ita ut esse debeat

$$\frac{xx+x}{2}+\frac{yy+y}{2}=\frac{aa+a}{2}+\frac{bb+b}{2}+p.$$

Fiat nunc $x=a-n$ et $y=b+n$ eritque

$$xx+x=aa-(2n-1)a+n(n-1) \text{ et } yy+y=bb+(2n+1)b+n(n+1),$$

quibus valoribus substitutis prodit

$$2p=2bn-2an+2nn, \text{ sive } p=(b-a)n+nn.$$

Cum igitur sit $b=a+d$ ideoque $b-a=d$, erit $p=dn+nn$. Hinc pro variis valoribus litterarum d et n littera p sequentes accipiet valores. Sit primo $n=1$ erit $p=d+1$

existente $n=2$ fiet $p=2d+4$

$n=3$ $\quad p=3d+9$

$n=4$ $\quad p=4d+16$

$n=5$ $\quad p=5d+25.$

Inde pro p sequentes oriuntur valores: $d = -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5$

$$\begin{array}{ll}
n = 1: & p = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6 \\
n = 2: & p = 2,\ 4,\ 6,\ 8,\ 10,\ 12,\ 14 \\
n = 3: & p = 3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24 \\
n = 4: & p = 8,\ 12,\ 16,\ 20,\ 24,\ 28,\ 32,\ 36 \\
\text{etc.} & \text{etc.}
\end{array}$$

Unde pro diversis valoribus ipsius p resolutio numeri N in tres trigonales succedet, si fuerit pro numeris minoribus

$$\begin{array}{llll}
 & & \text{tum erit} & \text{et} \\
N-1: & b = a & x = a-1 & y = b+1 \\
N-2 & \left\{\begin{array}{l} b = a+1 \\ b = a-1 \end{array}\right. & \begin{array}{l} x = a-1 \\ x = a-2 \end{array} & \begin{array}{l} y = b+1 \\ y = b+2 \end{array} \\
N-3 & \left\{\begin{array}{l} b = a+2 \\ b = a-2 \end{array}\right. & \begin{array}{l} x = a-1 \\ x = a-3 \end{array} & \begin{array}{l} y = b+1 \\ y = b+3 \end{array} \\
N-4 & \left\{\begin{array}{l} b = a+3 \\ b = a \\ b = a-3 \end{array}\right. & \begin{array}{l} x = a-1 \\ x = a-2 \\ x = a-4 \end{array} & \begin{array}{l} y = b+1 \\ y = b+2 \\ y = b+4 \end{array}
\end{array}$$

His positis ambarum x et y inventio succedet, si inter ternas radices a, b, c, primo pro numero $N-1$ fuerit $b = a$, sive si duae fuerint aequales. Secundo si pro numero $N-2$ fuerit vel $b = a+1$, vel $b = a-1$, hoc est si differentia fuerit inter binas $= 1$, tum vero duplex solutio locum habebit. Tertio si pro $N-3$ fuerit vel $b = a+2$, vel $b = a-2$, hoc est si binae radices binario discrepent. Quarto si pro numero $N-4$ fuerit vel $b = a+3$, vel $b = a$, vel $b = a-3$, hoc est si differentia inter binas radices fuerint vel $= 0$, vel $= 3$. Quinto si pro numero $N-5$ fuerit $b = a \pm 4$ h. e. si differentia inter binas radices fuerit $= \pm 4$. Sexto si pro numero $N-6$ fuerit vel $b = a \pm 5$, vel $b = a \pm 1$, hoc est si inter radices binas occurrat differentia vel 1, vel 5. Quamobrem si demonstrari posset, semper unum saltem horum casuum locum habere debere, tum demonstratum foret omnes numeros esse summas trium trigonalium. Quod cum de minoribus numeris certum per se sit, pro majoribus autem continuo plures casus examinandi occurrant, eo minus dubitari potest, quin resolutio semper sit locum habitura, idque plerumque pluribus modis, quo accedit, quod pro majoribus numeris fere omnes numeri $N-p$ pluribus modis in tres trigonales resolvi possint. Quod quo clarius pateat has resolutiones ab ipso initio numerorum secundum ternas radices contemplemur:

numeri	radices a, b, c	vel radices	vel radices
1	0, 0, 1		
2	0, 1, 1		
3	1, 1, 1	0, 0, 2	
4	0, 1, 2		
5	1, 1, 2		
6	0, 2, 2	0, 0, 3	
7	1, 2, 2	0, 1, 3	
8	1, 1, 3		
9	2, 2, 2	0, 2, 3	
10	0, 0, 4	1, 2, 3	
11	0, 1, 4		
12	0, 3, 3	1, 1, 4	2, 2, 3

Hinc ergo examinemus numerum $N = 13$ et habebimus

	a,	b,	c
pro $N-1 = 12$:	0,	3,	3
	1,	1,	4
	2,	2,	3
pro $N-2 = 11$:	0,	1,	4
pro $N-3 = 10$:	0,	0,	4
	1,	2,	3
pro $N-4 = 9$:	2,	2,	2
	0,	2,	3
pro $N-5 = 8$:	1,	1,	3
etc.		etc.	

Problema. Si omnes numeri minores quam N fuerint summae quatuor quadratorum, ipsum numerum N in quatuor quadrata resolvere.

Solutio. Sint pro numero quocunque minore $N-p$ quadratorum radices a, b, f, g, unde pro numero N statuantur radices x, y et f, g, ac ponatur $x=a+\alpha$ et $y=b+\beta$, eritque ab hoc $N-p$ subtracto

$$p=2a\alpha+\alpha\alpha+2b\beta+\beta\beta.$$

Jam sumatur $\alpha=-n$ et $\beta=+n$, ut fiat $p=2n(b-a)+2nn$; quare si fuerit $b=a+d$, habebitur $p=2(nd+nn)$, qui numerus duplo major est quam casu praecedente, pro numeris trigonalibus; unde eadem criteria locum habebunt, quae ante, si modo numerus p duplo major capiatur. Ita resolutio numeri $N-p$ succedet

si pro numero	$N-2$	fuerit $b=a$	tum erit	$x=a-1$,	$y=b+1$
	$N-4$	$b=a+1$		$x=a-1$,	$y=b+1$
	$N-6$	$b=a+2$		$x=a-1$,	$y=b+1$
	$N-8$	$b=a+3$		$x=a-1$,	$y=b+1$
		$b=a$		$x=a-2$,	$y=b+2$
	$N-10$	$b=a+4$		etc.	etc.
	etc.	etc.			

Hic ergo patet, pro hoc casu numerum criteriorum esse duplo majorem quam casu praecedente: Verum quia hic quatuor occurrunt radices, etiam hic multo probabilius est, inter quaternas radices occurrere duas, quarum differentia sit vel 0, vel 1, vel 2, vel 3, vel etc. Quin etiam plerique numeri pluribus modis in quatuor quadrata resolvi poterunt, unde hoc judicium aeque certum esse potest ac praecedens.

Problema. Si omnes numeri minores quam N fuerint resolubiles in quinque numeros pentagonales, ipsum numerum N in tales partes resolvere.

Solutio. Sint pro numero $N-p$ radices quinque pentagonalium a, b, f, g, h, unde pro ipso numero N statuantur quinque radices x, y, f, g, h, ac ponatur $x=a+\alpha$ et $y=b+\beta$, eritque

$$\frac{3xx-x}{2}-\left(\frac{3aa-a}{2}\right)=\frac{6a\alpha+3\alpha\alpha-\alpha}{2} \quad \text{et} \quad \frac{3yy-y}{2}-\left(\frac{3bb-a}{2}\right)=\frac{6b\beta+3\beta\beta-\beta}{2},$$

unde fiet
$$p=3a\alpha+\frac{3\alpha\alpha-\alpha}{2}+3b\beta+\frac{3\beta\beta-\beta}{2}.$$

Sumatur nunc $\alpha=-n$ et $\beta=+n$ eritque $p=3n(b-a)+3nn$; quare si fuerit $b=a+d$, fiet $p=3(nd+nn)$, ita ut hoc casu p sit triplo majus quam pro trigonalibus, unde eadem criteria locum habebunt, si modo ipso p valor triplo major tribuatur; hinc igitur resolutio semper succedet

si pro numero	$N-3$	fuerit	$b=a$
	$N-6$		$b=a+1$
	$N-9$		$b=a+2$
	$N-12$		$\begin{cases} b=a+3 \\ b=a \end{cases}$

ex quibus criteriis, si unicum tantum locum habuerit, resolutio numeri N certe succedit. Hic quidem triplo pauciora habentur criteria. Verum inter quinque radices reperientur binae, quarum differentia sit vel 0, vel 1, vel 2, vel 3, etc. Praeterea vero etiam plerique numeri multo pluribus modis in quinque pentagonales resolvi possunt.

Problema generale circa numeros polygonales quoscunque, quorum laterum numerus sit $=\pi$.

Si omnes numeri minores quam N *resolvi queant in π numeros polygonales, etiam ipsum numerum* N *in tales resolvere.*

Solutio. Sint pro numero quocunque minore, $N-p$, radices polygonalium a, b, f, g, h, i, k, etc. Tum vero pro ipso numero N radices x, y, f, g, h, i, k, etc. Sit autem in genere $x=a+\alpha$, $y=b+\beta$, et quia radicis x numerus polygonalis est

$$\frac{1}{2}(\pi-2)\,xx-\frac{1}{2}(\pi-4)\,x,$$

posito $x=a+\alpha$, iste numerus polygonalis erit

$$\frac{1}{2}(\pi-2)aa+(\pi-2)\,a\alpha+\frac{1}{2}(\pi-2)\,\alpha\alpha-\frac{1}{2}(\pi-4)\,a-\frac{1}{2}(\pi-4)\,\alpha,$$

unde si subtrahatur polygonalis ipsius a, remanet

$$(\pi-2)\,a\alpha+\frac{1}{2}(\pi-2)\,\alpha\alpha-\frac{1}{2}(\pi-4)\,\alpha;$$

hinc ergo si $N-p$ ab N subtrahatur, relinquetur

$$(\pi-2)\,a\alpha+\frac{1}{2}(\pi-2)\,\alpha\alpha-\frac{1}{2}(\pi-4)\,\alpha+(\pi-2)\,b\beta+\frac{1}{2}(\pi-2)\,\beta\beta-\frac{1}{2}(\pi-4)\,\beta.$$

Sumatur nunc $\alpha=-n$ et $\beta=+n$ fietque $p=n(\pi-2)(b-a)+(\pi-2)nn$; quamobrem si fuerit $b=a+d$, erit

$$p=n\,(\pi-2)\,d+(\pi-2)\,nn=(\pi-2)\,(nd+nn);$$

ideoque $\pi-2$ vicibus major quam pro numeris trigonalibus; quocirca criteria ita se habebunt:

Si pro numero	$N-(\pi-2)$, fuerit	$b=a$
	$N-2\,(\pi-2)$,	$b=a+1$
	$N-3\,(\pi-2)$,	$b=a+2$
	$N-4\,(\pi-2)$,	$\begin{cases} b=a+3 \\ b=a \end{cases}$
	etc.	etc.

Nisi ergo omnia haec criteria fallant, numerus N certe in π numeros polygonales resolvi potest. Pro theoremate igitur Fermatii demonstrando requiritur, ut demonstretur, fieri omnino non posse, ut omnia plane haec criteria simul fallant.

Scholion. Quemadmodum haec criteria deducta sunt ex consideratione binarum radicum x et y, cum binis datis a et b collatarum, ita etiam simpliciora criteria exhiberi possunt, si unica radix x cum a comparetur, manente $y=b$. Tum igitur erit

$$p=(\pi-2)\,a\alpha+\frac{1}{2}(\pi-2)\,\alpha\alpha-\frac{1}{2}(\pi-4)\,\alpha;$$

quare si capiamus $a=0$, fiet

$$p=\frac{1}{2}(\pi-2)\,\alpha\alpha-\frac{1}{2}(\pi-4)\,\alpha.$$

Quod si ergo pro numero unico $N-p$ occurrat unica radix $=0$, resolutio etiam certe succedet. Quocirca dispiciendum erit, num pro aliquo horum numerorum ipso N minorum:

$$N-1,\quad N-\pi,\quad N-(3\pi-3),\quad N-(6\pi-8),\quad N-(10\pi-15)\ \text{etc.}$$

inter ejus radices una occurrat $=0$. Quod si semel tantum evenerit, numerus N certe resolutionem admittet. Sin autem hoc criterium unquam succedat, tum demum superiora criteria examinari poterunt.

Scholion. Talia criteria possunt etiam derivari ex comparatione ternarum radicum x, y, z, ponendo $x=a+\alpha$, $y=b+\beta$ et $z=c+\gamma$, tum enim erit

$$p=(\pi-2)\,(a\alpha+b\beta+c\gamma)+\frac{1}{2}(\pi-2)\,(\alpha\alpha+\beta\beta+\gamma\gamma)-\frac{1}{2}(\pi-4)\,(\alpha+\beta+\gamma),$$

unde si sumatur $\alpha+\beta+\gamma=0$ simulque fuerit $a\alpha+b\beta+c\gamma=0$, obtinebitur

$$p=\frac{1}{2}(\pi-2)\,(\alpha\alpha+\beta\beta+\gamma\gamma).$$

Cum autem sit $\gamma = -\alpha - \beta$, erit $a\alpha + b\beta - c\alpha - c\beta = 0$, unde fit

$$c = \frac{a\alpha + b\beta}{\alpha + \beta}; \text{ tum igitur erit } p = (\pi - 2)(\alpha\alpha + \alpha\beta + \beta\beta);$$

quam ob rem, si pro numero $N-p$ inter ejus radices, quarum numerus est π, tres reperiantur a, b, c, ita comparatae, ut sit $c = \frac{a\alpha + b\beta}{\alpha + \beta}$, tum resolutio certe succedet. Sumatur ex. gr. $\alpha = n$ et $\beta = n$, eritque $c = \frac{a+b}{2}$, sive $a + b = 2c$, vel $a = 2c - b$, ex qua conditione sequitur, numeros b, c, a esse in progressione arithmetica, quia hinc fiet $c - b = a - c$. Quare si pro numero $N - p = N - 3nn(\pi - 2)$ inter ejus radices ternae sint in progressione arithmetica, numerus N semper erit resolubilis. Similique modo multitudo criteriorum pro lubitu augeri poterit, quorum si unicum successerit, resolutio numeri N locum habebit. Totum ergo negotium huc est reductum, ut demonstretur, nunquam fieri posse, ut omnia ista criteria simul fallant. In quo negotio imprimis erit perpendendum: in omnibus numeris minoribus $N-p$ omnes plane combinationes radicum 0, 1, 2, 3, 4, 5, etc., quarum quidem numeri polygonales simul sumti numerum N non superant, occurrere; unde demonstrandum erit: fieri non posse, ut in omnibus his combinationibus omnia nostra criteria simul fallant. Tum vero etiam hoc erit perpendendum, in numeris minoribus pro N assumtis resolutionem semper locum habere, ita, ut demonstratio tantum pro majoribus numeris sit suscipienda; ubi non solum numerus criteriorum major evadet, sed etiam numerus omnium combinationum. Quodsi enim nostra criteria unquam fallerent, id maxime metuendum foret in numeris minoribus.

Aliud tentamen in theorema Fermatianum inquirendi.

Sit series numerorum polygonalium 0, 1, A, B, C, D, etc., ac posito numero laterum $= n+2$, erit

$A = n+2$, $B = 3n+3$, $C = 6n+4$, $D = 10n+5$, $E = 15n+6$, $F = 21n+7$, $G = 28n+8$, etc.

et in genere pro radice x numerus polygonalis

$$= \frac{1}{2} nxx - \frac{1}{2}(n-2)x.$$

Quibus positis videamus, quot numeris hujus seriei opus sit ad singulos numeros producendos. Ac primo quidem ab 1 usque ad A quilibet numerus N, minor quam A, componitur ex N unitatibus, unde pro numeris ab 1 ad A ad summum opus est A. Nunc ad intervallum ab A ad B progrediamur, et quia $A+1$ constat ex duobus, $A+2$ ex tribus, $A+3$ ex quatuor, usque ad $A+n+1$ qui est primus qui postulat $n+2$ partes, praecedentes vero omnes ex paucioribus constant; est vero $A+n+1 = 2n+3$, unde videtur sequentem numerum $2n+4$ requirere $n+3$, quia autem est $2n+4 = 2A$, hic numerus tantum duos postulat; sequens igitur $2n+5$ postulat 3, $2n+6$ postulat 4, $2n+7$ postulat 5 etc. et $2A+n$ postulat $n+2$. Est vero $2A+n = 3n+4$; at vero hic numerus est $B+1$, ideoque tantum postulat duos; unde patet usque ad B unicum esse numerum scilicet $2n+3$, qui $n+2$ partes postulat, omnes reliqui pauciores. Nunc a B ad C progrediamur, ac manifestum est, hinc omnes numeros minores quam $B+2n+3$ ad summum requirere $n+2$, numerus autem $B+2n+3 = 5n+6$ videtur $n+3$ partes requirere; est vero $5n+6 = 3A+2n = 4A+n-2$, ubi $4A$ constat quatuor partibus et $n-2$ ex $n-2$ partibus, unde ipse numerus $4A+n-2$ constat ex $n+2$. Verum hic excipiendus est casus, ubi $n<2$, quia $n<2$ foret negativum: hoc autem casu numerus noster $B+2n+3$ fiet $= C-n+2$; unde casu $n=1$ erit $C+1$, ideoque duabus tantum constat partibus. Casu autem $n=2$ fit $5n+6 = C$, ideoque ipse est numerus polygonalis; reliquis vero casibus, ubi $n>2$, iste numerus $5n+6$ secundus est, qui $n+2$ partes postulat, dum minores omnes praeter $2n+3$ paucioribus constant. Sequens autem numerus $5n+7 = 2A+B$, ideoque tribus tantum constat partibus. Hunc sequens, $5n+8$, constabit quatuor, ac tandem $5n+7+n-1$ constabit ex $n+2$; est vero $5n+7+n-1 = C+2$, ideoque constat tantum tribus. Nunc a C ad D progrediamur usque, ubi primum occurrit $C+2n+3$, qui dubius videri potest. Est vero

$$C+2n+3 = 8n+7 = 2B+2n+1 = 2B+A+n-1,$$

quarum partium numerus est $n+2$, qui ergo est tertius numerus $n+2$ partes postulans. Quia deinde ab $2n+3$ usque ad $5n+6$ omnes numeri postulant partes pauciores quam $n+2$, numerus sequens dubius erit $C+5n+6=11n+10$, qui autem jam superat D et ad sequens intervallum pertinet. Simili modo progredientes a D versus E, ubi primum numerum dubium reperimus $D+2n+3=12n+8=2C$, qui ergo duabus tantum constat partibus, unde ulterius progredi licet, usque ad $2C+n$, qui constabit ex $n+2$. Sequens est

$$2C+n+1=13n+9,$$

qui videtur $n+3$ partes requirere: est vero $13n+9=D+B+1$, qui ergo in tres partes resolvitur. Hinc progrediemur usque ad $14n+9=2C+2n+1=2C+A+n-1$, sicque partium numerus reducitur ad $n+2$; sequens vero numerus $14n+10=D+4n+5=D+B+A$ sicque tribus constat partibus, unde progredi licet usque ad $14n+10+n-1=15n+9$ quod jam superat . . . .

A. m. T. I. p. 336—340.

34.

(*Lexell.*)

Demonstratio sequens, ardua Viro Celeb. la Grange *debetur:*

Si fuerit $Aa=pp+qq+rr+ss$, ubi sumere licet $pp+qq$, ut cum a communem non habeat divisorem. Ponatur $pp+qq=t$ et $rr+ss=u$, ut sit $Aa=t+u$, et per t multiplicando $Aat=tt+tu$. Cum nunc sit $tu=(pp+qq)(rr+ss)$, erit summa duorum quadratorum; ergo ponatur $=xx+yy$, eritque $x=pr\pm qs$ et $y=ps\mp qr$, ita ut sit $Aat=tt+xx+yy$. Jam quaerantur numeri α, β, γ, δ, ut fiat

$$x=t\alpha+a\gamma \quad \text{et} \quad y=t\beta+a\delta,$$

quod cum infinitis modis fieri possit, casu simplicissimo α et β capere licebit minores quam $\frac{1}{2}a$, eritque

$$Aat=tt(1+\alpha\alpha+\beta\beta)+2at(\alpha\gamma+\beta\delta)+aa(\gamma\gamma+\delta\delta).$$

Debet ergo primum membrum $1+\alpha\alpha+\beta\beta$ factorem habere a, quia autem t ad a est primus, necesse est, ut $1+\alpha\alpha+\beta\beta$ divisibile sit per a; ponatur ergo $1+\alpha\alpha+\beta\beta=aa'$, ita ut nunc habeamus

$$At=a'tt+2t(\alpha\gamma+\beta\delta)+a(\gamma\gamma+\delta\delta),$$

quae per a' multiplicata fit $\quad Aa't=a'a'tt+2a't(\alpha\gamma+\beta\delta)+aa'(\gamma\gamma+\delta\delta),$

formula per t divisibilis. In ultimo membro loco aa' restituatur $1+\alpha\alpha+\beta\beta$, ut habeamus

$$Aa't=a'a'tt+2a't(\alpha\gamma+\beta\delta)+(\alpha\alpha+\beta\beta)(\gamma\gamma+\delta\delta)+\gamma\gamma+\delta\delta,$$

cujus formulae ad dextram tria priora membra manifesto reducuntur ad

$$(a't+\alpha\gamma+\beta\delta)^2+(\beta\gamma-\alpha\delta)^2$$

ita ut nunc habeamus $\quad Aa't=(a't+\alpha\gamma+\beta\delta)^2+(\beta\gamma-\alpha\delta)^2+\gamma\gamma+\delta\delta.$

Supra autem vidimus $\gamma\gamma+\delta\delta$ per t esse divisibile, unde etiam summam duorum priorum quadratorum

$$(a't+\alpha\gamma+\beta\delta)^2+(\beta\gamma-\alpha\delta)^2$$

per t divisibilem esse oportet, ita ut uterque quotus fiat summa duorum quadratorum, quare si faciamus

$$\frac{(a't+\alpha\gamma+\beta\delta)^2+(\beta\gamma-\alpha\delta)^2}{t}=p'p'+q'q' \quad \text{et} \quad \frac{\gamma\gamma+\delta\delta}{t}=r'r'+s's'$$

habebimus $Aa'=p'p'+q'q'+r'r'+s's'$ scilicet summae quatuor quadratorum. Hic vero imprimis notandum est fore $a'<a$. Cum enim sit $a'=\frac{1+\alpha\alpha+\beta\beta}{a}$, ac ut vidimus

$$\alpha<\frac{1}{2}a \quad \text{et} \quad \beta<\frac{1}{2}a, \quad \text{erit} \quad 1+\alpha\alpha+\beta\beta<1+\frac{1}{2}aa,$$

unde sequitur fore $a'<\frac{1}{2}a+\frac{1}{a}$, ideoque certe minor quam a, vel $a'<\frac{1}{2}a+1$. Consequenter si productum

Ad fuerit summa quatuor quadratorum, etiam hoc minus productum Aa' erit talis summa, hocque modo continuo ad minora hujusmodi producta Aa'', Aa''' etc. progredi licet, sicque tandem necessario pervenietur ad productum $A.1$, ideoque A summa quatuor quadratorum. Quae est demonstratio insignis illius et demonstratu difficillimi theorematis, quod si quispiam numerus A fuerit divisor summae quatuor quadratorum, quae quidem inter se factorem non habeant communem, tum ipsum numerum A fore quoque summam quatuor quadratorum, seu, quod eodem redit, summam quatuor quadratorum alios non admittere divisores nisi qui ipsi sint summae quatuor quadratorum.

(*Krafft.*)

Ejusdem theorematis demonstratio mea (scil. Euleri).

Lemma I. Si N et n fuerint numeri inter se primi, tum quicunque numerus A ita potest repraesentari, ut sit $A = Nx + ny$, et quia hoc infinitis modis fieri potest, dabitur casus, quo $x < \frac{1}{2}n$. Sit enim

$$A = Nf + ng, \quad \text{erit etiam} \quad A = N(f - \lambda n) + n(g + \lambda N),$$

unde, quantumvis magnus fuerit numerus f, ita accipere licebit λ, ut fiat $f - \lambda n < n$; tum vero si f etiamnunc fuerit $> \frac{1}{2}n$, tum $f - n$ certe minus erit, quam $\frac{1}{2}n$: hic enim ipsi numeri spectantur, et perinde est, sive sint positivi, sive negativi.

Lemma II. Productum ex binis numeris, quorum uterque est summa quatuor quadratorum, in quatuor quadrata resolvere.

Sit hujusmodi productum $(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2)$,

ac sumatur

$$A = + a\alpha + b\beta + c\gamma + d\delta, \quad B = + a\beta - b\alpha - c\delta + d\gamma$$
$$C = + a\gamma + b\delta - c\alpha - d\beta, \quad D = + a\delta - b\gamma + c\beta - d\alpha,$$

quorum quadrata si invicem addantur, omnia duplicia producta ex binis se mutuo tollent, et quodvis quadratum latinarum literarum multiplicatur per omnia quadrata litterarum graecarum, atque hinc manifesto fiet

$$(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = A^2 + B^2 + C^2 + D^2.$$

Theorema. Si numerus primus N fuerit divisor summae quatuor quadratorum $P^2 + Q^2 + R^2 + S^2$, tum ille ipse numerus N erit summa quatuor quadratorum.

Demonstratio. Quantumvis magni fuerint numeri P, Q, R, S, eos semper deprimere licebit infra $\frac{1}{2}N$; nam si loco P scribatur $P - \lambda N$, summa illa etiamnunc erit per N divisibilis, quod etiam de reliquis Q, R et S valet, sicque singulae radices infra N deprimentur; ac si P adhuc majus fuerit quam $\frac{1}{2}N$, ejus loco scribatur $N - P$, quod certo erit minus quam $\frac{1}{2}N$. Sit ergo $p^2 + q^2 + r^2 + s^2$ ista quatuor quadratorum summa per N divisibilis, ita, ut singulae radices minores sint quam $\frac{1}{2}N$, ac denotet n quotum resultantem, ut sit

$$Nn = p^2 + q^2 + r^2 + s^2$$

et haec summa minor erit quam N^2, sicque certo erit $n < N$. Jam sequenti modo istae quatuor radices exhibeantur secundum lemma I:

$$p = Na + n\alpha, \quad q = Nb + n\beta, \quad r = Nc + n\gamma, \quad s = Nd + n\delta,$$

ubi litteras a, b, c, d ita assumere licebit, ut sint minores quam $\frac{1}{2}n$, sive hoc fiat negative, sive positive. His jam valoribus substitutis habebimus

$$Nn = N^2(a^2 + b^2 + c^2 + d^2) + 2Nn(a\alpha + b\beta + c\gamma + d\delta) + n^2(\alpha^2 + \beta^2 + \gamma^2 + \delta^2),$$

ubi notetur esse, per lemma II, $a\alpha + b\beta + c\gamma + d\delta = A$. Duo posteriora membra sponte sunt divisibilia per n; ergo necesse est, ut etiam primum per n sit divisibile. At N^2 dividi nequit per n, ergo necesse est, ut $a^2 + b^2 + c^2 + d^2$ sit per n divisibile. Ponatur ergo

$a^2+b^2+c^2+d^2=nn'$, et quia $a<\frac{1}{2}n$, $b<\frac{1}{2}n$, $c<\frac{1}{2}n$, $d<\frac{1}{2}n$, erit summa $a^2+b^2+c^2+d^2<n^2$, ideoque $nn'<n^2$, ergo $n'<n$, nisi forte sit $n=1$. Divisa ergo per n illa aequatione, prodit

$$N=N^2n'+2NA+n(\alpha^2+\beta^2+\gamma^2+\delta^2);$$

quae per n' multiplicetur, ut habeamus

$$Nn'=N^2n'^2+2Nn'A+nn'(\alpha^2+\beta^2+\gamma^2+\delta^2);$$

quia autem $nn'=a^2+b^2+c^2+d^2$, ultimum illud membrum abit in

$$(a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2)=A^2+B^2+C^2+D^2$$

per lemma II; consequenter

$$Nn'=N^2n'^2+2Nn'A+A^2+B^2+C^2+D^2=(Nn'+A)^2+B^2+C^2+D^2.$$

Sicque formula Nn' etiam erit summa quatuor quadratorum, existente $n'<n$. Eodem modo pervenire licebit ad formas ulteriores Nn'', Nn''' etc. ita, ut sit $n''<n'$, $n'''<n''$ etc. sicque tandem perveniri necesse est ad formam $N.1$, quae ergo etiam est summa quatuor quadratorum. Q. E. D.

Hinc etiam sequens Theorema facilius demonstrari potest, quam hactenus est factum:

Summa duorum quadratorum inter se primorum alios non admittit divisores, nisi qui ipsi sint summae duorum quadratorum.

Lemma. Productum ex duabus summis duorum quadratorum ipsum in duo quadrata resolvere.

Sit productum $(a^2+b^2)(\alpha^2+\beta^2)$, et sumtis $A=a\alpha+b\beta$ et $B=a\beta-b\alpha$, erit

$$(a^2+b^2)(\alpha^2+\beta^2)=A^2+B^2.$$

Si nunc N fuerit divisor formae p^2+q^2, posito quoto $=n$, habetur $Nn=p^2+q^2$. Nunc igitur p et q ita exhibeantur, ut sit $p=Na+n\alpha$ et $q=Nb+n\beta$, ita, ut a et b sint minores quam $\frac{1}{2}n$; hincque $a^2+b^2<\frac{1}{2}n^2$, quo substituto fit

$$Nn=N^2(a^2+b^2)+2Nn(a\alpha+b\beta)+n^2(\alpha^2+\beta^2),$$

quae cum per n divisibilis esse debeat, statuatur $a^2+b^2=nn'$, et diviso per n erit

$$N=N^2n'+2NA+n(\alpha^2+\beta^2).$$

Multiplicetur per n', erit

$$Nn'=N^2n'^2+2Nn'A+nn'(\alpha^2+\beta^2)$$

at $nn'(\alpha^2+\beta^2)=A^2+B^2$, ergo

$$Nn'=N^2n'^2+2Nn'A+A^2+B^2=(Nn'+A)^2+B^2,$$

sicque Nn' est etiam summa duorum quadratorum, ubi $n'<\frac{1}{2}n$. Hocque modo ulterius progrediendo, mox pervenietur ad $N.1$. Consequenter N certo erit summa duorum quadratorum.

Alia demonstratio simplicior ejusdem theorematis.

Si numerus quicunque N fuerit divisor summae quatuor quadratorum $P^2+Q^2+R^2+S^2$, quae singula seorsim per eum non sint divisibilia, ille ipse numerus quoque erit summa quatuor quadratorum.

Demonstratio. I. Illa quadrata semper ad alia reduci possunt minora quam $\frac{1}{4}N^2$. Ponatur enim

$$P=\mathfrak{A}N\mp p,\quad Q=\mathfrak{B}N\mp q,\quad R=\mathfrak{C}N\mp r,\quad S=\mathfrak{D}N\mp s,$$

ubi literae $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ ita assumi possunt, ut numeri p, q, r, s infra semissem numeri N deprimantur, quibus substitutis evidens est, formulam $p^2+q^2+r^2+s^2$, quae utique minor erit quam N^2, divisibilem fore per N et quotum fore minorem quam N.

II. Sit ergo iste quotus $=n$, ut sit $Nn=p^2+q^2+r^2+s^2$, et ratione hujus numeri n radices istorum quadratorum ita exhiberi poterunt

$$p=a+\alpha n,\quad q=b+\beta n,\quad r=c+\gamma n\quad\text{et}\quad s=d+\delta n,$$

si pro a, b, c et d etiam valores negativi admittantur, hos numeros itidem infra $\frac{1}{2}n$ deprimere licebit, ut sit $a^2+b^2+c^2+d^2<n^2$.

III. His autem valoribus substitutis fiet

$$Nn=a^2+b^2+c^2+d^2+2n(a\alpha+b\beta+c\gamma+d\delta)+n^2(\alpha^2+\beta^2+\gamma^2+\delta^2),$$

quae formula per lemma praemissum abit in hanc

$$Nn=a^2+b^2+c^2+d^2+2nA+n^2(\alpha^2+\beta^2+\gamma^2+\delta^2),$$

quae cum sit divisibilis per n et bina posteriora membra jam in se sint per n divisibilia, necesse est, ut etiam pars prima $a^2+b^2+c^2+d^2$ factorem habeat n. Quare ponatur $a^2+b^2+c^2+d^2=nn'$ et dividendo per n habebimus

$$N=n'+2A+n(\alpha^2+\beta^2+\gamma^2+\delta^2).$$

IV. Multiplicemus nunc in n', et in postremo membro loco nn' substituamus valorem $a^2+b^2+c^2+d^2$, ut prodeat

$$Nn'=n'^2+2n'A+(a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2).$$

Jam per lemma praemissum hoc postremum membrum transformatur in $A^2+B^2+C^2+D^2$, ita, ut nunc habeamus

$$Nn'=n'^2+2n'A+A^2+B^2+C^2+D^2,$$

sive $\quad Nn'=(n'+A)^2+B^2+C^2+D^2=$ summae quatuor quadratorum.

V. Cum autem sit $nn'=a^2+b^2+c^2+d^2<n^2$, utique erit $n'<n$. Quemadmodum igitur ex forma Nn, quae erat summa quatuor quadratorum, pervenimus ad hanc minorem Nn', etiam aequalem summae quatuor quadratorum; ita ulterius pervenire licebit ad formulas Nn'', Nn''' etc. itidem quatuor quadratis aequales, ita, ut numeri n', n'', n''', etc. continuo diminuantur. Tandem ergo haec diminutio usque ad unitatem deducetur; ita, ut tum futurum sit $N.1$, hoc est ipse numerus propositus N aequalis summae quatuor quadratorum. Q. E. D.

Corollarium 1. Haec adeo demonstratio locum habet, etiamsi N non fuerit numerus primus; dummodo ergo numerus quicunque N fuerit factor vel divisor summae cujuspiam quatuor quadratorum, tum certe is ipse numerus quoque erit summa quatuor quadratorum.

Corollarium 2. Quodsi ergo demonstrari posset, proposito quocunque numero N, semper exhiberi posse summam quatuor quadratorum per eum divisibilem, tum utique completa haberetur demonstratio theorematis illius Fermatiani, quod omnis numerus sit summa quatuor quadratorum, vel etiam pauciorum.

Theorema. Proposito quocunque numero primo N, semper exhiberi possunt quatuor quadrata, singula minora quam $\frac{1}{4}N^2$, quorum summa per illum numerum sit divisibilis.

Demonstratio. I. Ratione numeri propositi N omnes plane numeri in aliqua sequentium formularum erunt contenti $\quad \lambda N,\ \lambda N+1,\ \lambda N+2,\ \lambda N+3,\ \lambda N+4,\ldots\lambda N+(N-1),$

quarum numerus est $=N$. Singulae autem hae formae non omnes continent numeros quadratos; dantur scilicet inter illas ejusmodi formulae, quae numeros quadratos involvunt, reliquae vero quadrata prorsus excludunt. Seposita enim prima forma λN, quae ipsa multipla numeri N continet, reliquarum primae $\lambda N+1$ et ultimae $\lambda N+N-1$, vel $(\lambda+1)N-1$ quadrata in eadem formula continebuntur, nempe $\lambda N+1$. Eodem modo quadrata secundae et penultimae formulae continentur in formula $\lambda N+4$. Simili modo quadrata tertiae et antepenultimae continebuntur in formula $\lambda N+9$, quarum formularum multitudo est $\frac{1}{2}(N-1)$, quae scilicet in se complectuntur quadrata. Reliquae formulae omnes ab his diversae quadrata penitus excludunt, quarum numerus itidem est $\frac{1}{2}(N-1)$.

II. Sint formulae illae quadrata admittentes: $\lambda N+a$, $\lambda N+b$, $\lambda N+c$, $\lambda N+d$, etc., quarum numerus est $\frac{1}{2}(N-1)$ et modo vidimus, inter hos numeros a, b, c, d, etc. reperiri quadratos 1, 4, 9, 16, etc. quamdiu scilicet sunt minores, quam N. Majorum enim residua ex divisione per N relicta sumuntur. Formulae autem quadrata penitus excludentes sint: $\lambda N+\alpha$, $\lambda N+\beta$, $\lambda N+\gamma$, $\lambda N+\delta$, etc., quorum numerus itidem est $\frac{1}{2}(N-1)$.

III. Facile autem demonstrari potest, binas formulas prioris classis in se multiplicatas etiamnunc ad priorem classem pertinere, scilicet cum prior classis contineat formas a, b, c, d, etiam continebit producta ex binis vel quotcunque horum numerorum. Scilicet producta ex binis numeris prioris classis etiam in priore classe occurrent, cujusmodi sunt aa, bb, cc, etc. Tum vero productum ex numero prioris classis in numerum posterioris classis cadet in classem posteriorem. Denique productum ex binis numeris posterioris classis etiam cadet in classem priorem.

IV. Jam si in prima classe occurreret formula $\lambda N - a$, sive quod eodem redit, $\lambda N + N - a$, darentur quadrata formae $\lambda N + a$ et $\lambda N - a$, quorum ergo summa foret per N divisibilis. Quare si quis neget, dari summam quatuor quadratorum per N divisibilem, multo magis negare debebit, dari adeo summam duorum quadratorum divisibilem.

V. Quo igitur nostrum theorema demonstremus, sumamus tantisper, non dari summam quatuor vel pauciorum quadratorum, quae non esset divisibilis per numerum propositum N, atque ostendemus hinc maxima absurda esse secutura.

VI. Ista igitur opinione quasi adoptata, quia numerus $-a$ vel $N-a$ in priore classe non occurrit, certe occurret in posteriore classe inter numeros α, β, γ, δ; ergo inter numeros α, β, γ, δ occurrent numeri $-a$, $-b$, $-c$, $-d$, ideoque etiam negativa quadrata -1, -4, -9, -16.

VII. Eodem modo ostendi potest, numerum $-a-b$ certe non in priori classe contineri; si enim ibi contineretur, darentur tres numeri quadrati formarum $\lambda N + a$, $\lambda N + b$ et $\lambda N - a - b$, quorum summa esset per N divisibilis; quod cum hypothesi repugnet, hic numerus $-a-b$ in posteriori classe reperiatur necesse est.

VIII. Quia autem in posteriori classe reperitur -1, productum ex -1 in $-a-b$, id est $+a+b$ in prima classe continetur; sicque in priori classe jam occurrerent numeri 1, 2, 4, 5, 8, 9, 10, 13; eorundem autem negativa occurrent in classe posteriori.

IX. Cum ergo formulae $\lambda N + 1$ et $\lambda N + 2$ sint prioris classis, ibidem non continebitur formula $\lambda N - 3$, quia alioquin haberemus tria quadrata harum formularum, quorum summa foret per N divisibilis. Quia ergo -3 non in priori classe continetur, continebitur in posteriori; ejus vero productum in -1, hoc est $+3$, continebitur in priori.

X. Sit autem generalius f numerus quicunque primae classis, atque dico, in priori classe formulam $\lambda N - f - 1$ non contineri, quia darentur tria quadrata, scilicet $\lambda N + 1$, $\lambda N + f$, et $\lambda N - 1 - f$, quorum summa foret divisibilis per N; unde numerus $-f-1$ in classe posteriori reperiatur necesse est; ejus vero negativum $+f+1$ in priorem classem cadet.

XI. Admissa ergo illa hypothesi, si formula quaecunque $\lambda N + f$ in prima classe contineatur, ibidem quoque occurret formula $\lambda N + f + 1$; quocirca in prima classe occurrerent omnes istae formulae:

$$\lambda N + 1, \quad \lambda N + 2, \quad \lambda N + 3, \quad \lambda N + 4, \quad \text{etc.}$$

hoc est omnes plane formulae forent prioris classis, simul vero in classem posteriorem ingrederentur omnes istae formulae:

$$\lambda N - 1, \quad \lambda N - 2, \quad \lambda N - 3, \quad \lambda N - 4, \quad \text{etc.}$$

hoc est omnes plane formulae tam in priore quam in posteriore classe occurrerent. Quare cum ante sit ostensum, in priore classe tantum occurrere $\frac{1}{2}(N-1)$ formulas et totidem in posteriore, absurdum est manifestum quod inde ortum est, quod falso supposuimus, non dari summam trium quadratorum per N divisibilem; quamobrem verum erit, dari summas trium quadratorum per N divisibiles. Multo magis ergo dantur summae quatuor quadratorum per N divisibiles. Q. E. D.

Corollarium. Cum ergo, proposito numero primo quocunque N, dentur summae non solum quatuor sed etiam trium quadratorum per illum divisibiles, ipse ille numerus N erit quoque summa quatuor quadratorum, vel et pauciorum, et cum producta ex binis vel pluribus numeris, quorum singuli sunt summae quatuor quadratorum, sint etiam summae quatuor quadratorum, jam rigorosissime demonstratum est, omnes plane numeros esse summas quatuor quadratorum.

Observatio singularis. Cum productum ex binis numeris, quorum uterque est summa duorum quadratorum, etiam sit summa duorum quadratorum, tum vero etiam productum ex duobus numeris, quorum uterque est summa quatuor quadratorum, quoque sit summa quatuor quadratorum. Hinc concludendum videtur, idem etiam de summis trium quadratorum valere, quod autem longe secus se habet, neque etiam eo modo, quo in lemmate superiore sumus usi, talis forma $(a^2+b^2+c^2)(\alpha^2+\beta^2+\gamma^2)$ ad tria quadrata revocari potest. Fieri enim saepe potest, ut productum ex binis summis trium quadratorum non in pauciora quam quatuor quadrata resolvi possit, veluti $3=1+1+1$ et $21=1+4+16$; horum tamen productum 63 nullo modo in pauciora quam quatuor quadrata potest resolvi, quandoquidem est numerus formae $8n-1$ sive $8n+7$.

A. m. T. I. p. 177—186.

35.

(*N. Fuss I.*)

Theorema. Nulli numeri in sequentibus formulis contenti in duos numeros trigonales resolvi possunt:

I. $9n+$ 5, 8

II. $49n+$ 5, 19, 26, 33, 40, 47

III. $81n+47$, 74

IV. $121n+$ 8, 19, 41, 52, 63, 74, 85, 96, 107, 118

V. $361n+14$, 33, 52, 71, 109, 128, 147, 166, 185, 204, 223, 242, 261, 280, 299, 318, 337, 356.

Specimen Demonstrationis pro formula $49n+19$:

Sit $49n+19=\frac{aa+a}{2}+\frac{bb+b}{2}$, erit multiplicando per 8

$$392n+152=4aa+4a+4bb+4b,$$

ergo $392n+154=(2a+1)^2+(2b+1)^2$, ideoque summa duorum quadratorum. At numerus $392n+154$ factorem habet 7, ideoque duorum quadratorum summa esse nequit.

Problema. Numeros in hac forma contentos $xx+7$ in quatuor quadrata resolvere.

Solutio. Formula $xx+7$ transformatur in has:

$$(x-1)^2+2x+6,\quad \text{vel}\quad (x-2)^2+4x+3,\quad \text{vel}\quad (x-3)^2+6x-2,\quad \text{vel}\quad (x-4)^2+8x-9,$$

vel in genere

$$(x-n)^2+2nx-nn+7,$$

unde si $2nx-nn+7$ in tria vel pauciora quadrata resolvi potest, quaesito satisfiet. Plerumque statim una harum formularum priorum negotium conficit. Verum dantur etiam casus, quibus longe progredi oportet. Veluti si x fuerit 75, usque ad $n=11$ progredi oportet, tum enim fiet

$$75^2+7=64^2+1650-121+7=64^2+1536.$$

Est vero $1536=16\,.\,96=16^2.6$, at $6=4+1+1$,

unde quatuor quadrata erunt $64^2+16^2+32^2+16^2$.

Aliud exemplum multo notabilius est, quo $x=181$; tum enim formulae supra datae frustra tentantur, donec perveniatur ad $n=53$, tum autem fiet

$$181^2+7=128^2+19186-2802=128^2+16384=128^2+128^2.$$

Sicque hic numerus ad duo quadrata est reductus, neque ullo alio modo vel in tria, vel in plura adhuc quadrata resolvi potest.

Hac occasione sequens theorema omnem attentionem meretur.

Theorema. Omnis potestas binarii 2^n semper est numerus in hac formula contentus: $xx+7yy$.

DEMONSTRATIO. Sumto enim $x=\frac{1}{2}$ et $y=\frac{1}{2}$ prodit $xx+7yy=2$. Notum autem est omnes pote-states formulae $xx+7yy$ in eadem formula contineri, quandoquidem est

$$(aa+7bb)(cc+7dd)=(ac\pm 7bd)^2+7(ad\mp bc)^2.$$

Hinc igitur per factores imaginarios erit

$$2=\frac{1+7}{4}=\frac{1+\sqrt{-7}}{2}\cdot\frac{1-\sqrt{-7}}{2}, \text{ erit ergo } 2^n=\left(\frac{1+\sqrt{-7}}{2}\right)^n\cdot\left(\frac{1-\sqrt{-7}}{2}\right)^n.$$

Binomii autem $\frac{1+\sqrt{-7}}{2}$ potestates sequenti modo progrediuntur

$$\frac{-3+\sqrt{-7}}{2}=\left(\frac{1+\sqrt{-7}}{2}\right)^2$$

$$\frac{-5-\sqrt{-7}}{2}=\left(\frac{1+\sqrt{-7}}{2}\right)^3$$

$$\frac{1-3\sqrt{-7}}{2}=\left(\frac{1+\sqrt{-7}}{2}\right)^4$$

etc. etc.

Harum formularum ambae partes seriem recurrentem constituunt, cujus scala relationis est $1, -2$, unde si ex. gr. ponatur $\frac{1+\sqrt{-7}}{2}=A$, et quia omnes hae formulae per 2 dividuntur, istae formulae sequenti modo continuantur:

$$\begin{array}{ll}
2A=1+\sqrt{-7} & 2A^8=-31-3\sqrt{-7}\\
2A^2=-3+\sqrt{-7} & 2A^9=-5-17\sqrt{-7}\\
2A^3=-5-\sqrt{-7} & 2A^{10}=57-11\sqrt{-7}\\
2A^4=1-3\sqrt{-7} & 2A^{11}=67+23\sqrt{-7}\\
2A^5=11-\sqrt{-7} & 2A^{12}=-47+45\sqrt{-7}\\
2A^6=9+5\sqrt{-7} & 2A^{13}=-181-\sqrt{-7}\\
2A^7=-13+7\sqrt{-7} & \text{etc.}
\end{array}$$

Cum igitur sit

$$\left(\frac{1+\sqrt{-7}}{2}\right)^{13}=\frac{-181-\sqrt{-7}}{2}, \text{ erit } \left(\frac{1-\sqrt{-7}}{2}\right)^{13}=\frac{-181+\sqrt{-7}}{2}, \text{ indeque } 2^{13}=\frac{181^2+7}{4},$$

$$\text{ergo}\quad 2^{15}=181^2+7.$$

Ratio autem scalae relationis in hoc sita est, quod si ponatur

$$z=\frac{1+\sqrt{-7}}{2},\quad \text{fit}\quad z-\frac{1}{2}=\frac{\sqrt{-7}}{2}$$

et sumtis quadratis erit $zz=z-2$, unde nascitur scala relationis $1, -2$. In superiori progressione, ubi omnes termini in forma $a+b\sqrt{-7}$ continentur, ii casus maxime sunt notatu digni, quibus b est vel $+1$, vel -1, quibus casibus pars rationalis fit maxima. Hincque sequens problema omnino peculiarem postulat solutionem.

PROBLEMA. Cum sit uti vidimus $\left(\frac{1+\sqrt{-7}}{2}\right)^n=\frac{a+b\sqrt{-7}}{2}$, investigare eos exponentes n, pro quibus fiat $b=\pm 1$, id quod fieri observavimus casibus $n=1, 2, 3, 5, 13$. Quaerantur igitur casus sequentes.

SOLUTIO. Cum esse debeat $b=\pm 1$, reducatur formula $\frac{1+\sqrt{-7}}{2}$ ad hanc formam $p(\cos\varphi+\sqrt{-1}.\sin\varphi)$ eritque

$p\cos\varphi=\frac{1}{2}$ et $p\sin\varphi=\frac{1}{2}\sqrt{7}$, unde fit $\operatorname{tang}\varphi=\sqrt{7}$, hincque $\sin\varphi=\sqrt{\frac{7}{8}}$ et $\cos\varphi=\sqrt{\frac{1}{8}}$, sicque erit $p=\sqrt{2}$.

Invento igitur angulo φ, ut sit $\operatorname{tang}\varphi=\sqrt{7}$ erit primo

$$\frac{1+\sqrt{-7}}{2}=\sqrt{2}(\cos\varphi+\sqrt{-1}.\sin\varphi) \text{ ideoque } \left(\frac{1+\sqrt{-7}}{2}\right)^n=2^{\frac{n}{2}}(\cos n\varphi+\sqrt{-1}.\sin n\varphi).$$

Quaestio igitur huc redit, ut membrum imaginarium fiat quam minimum, id quod evenit, quando angulus $n\varphi$ quam minime differt ab π, vel 2π, vel etc. vel $i\pi$. Quod si ergo statuamus $n\varphi = i\pi$ erit $\frac{n}{i} = \frac{\pi}{\varphi}$, quamobrem quaerantur fractiones proxime aequales ipsi $\frac{\pi}{\varphi}$, earumque numeratores dabunt valores pro n. Cum igitur sit

$$\tang\varphi = \sqrt{7} \quad \text{erit} \quad l.\tang\varphi = 0{,}4225490, \quad \text{unde} \quad \varphi = 69^0\ 17'\ 43'' = 249463''.$$

At vero
$$\pi = 180^0 = 648000'', \quad \text{unde} \quad \frac{\pi}{\varphi} = \frac{648000}{249463} = \frac{n}{i}.$$

Evolvatur ergo haec fractio per continuam divisionem, eruntque quotientes 2, 1, 1, 2, 16, 7. Ex his quotis formentur sequentes fractiones

$$\frac{1}{0},\quad \frac{2}{1},\quad \frac{3}{1},\quad \frac{5}{2},\quad \frac{13}{5},\quad \frac{213}{82},$$

ex quarum numeratoribus statim patet, quaesito satisfieri casibus 1, 2, 3, 5, 13, unde tuto affirmare licet idem evenire casu $n = 213$. Consideremus casum $n = 13$, eritque

$$13\varphi = 900^0\ 50'\ 19'' = 180^0\ 50'\ 19''.$$

Nunc vero est
$$l2^{\frac{13}{2}} = 1{,}9566950,$$

unde fiet

$$\begin{array}{rlrl} l2^{\frac{13}{2}} &= 1{,}9566950 & l2^{\frac{13}{2}} &= 1{,}9566950 \\ l\cos 13\varphi &= 9{,}9999534 & l\sin 13\varphi &= 8{,}1654040 \\ \hline & 1{,}9566484 & & 0{,}1220990 \end{array}$$

$$2^{\frac{13}{2}}\cos 13\varphi = -90{,}5 = -\frac{181}{2}, \qquad 2^{\frac{13}{2}}\sin 13\varphi = -1{,}32 = -\frac{1}{2}\sqrt{7},$$

eritque
$$2^{\frac{13}{2}}\sin 13\varphi\sqrt{-1} = -\frac{1}{2}\sqrt{-7}, \quad \text{unde patet esse} \quad \left(\frac{1+\sqrt{-7}}{2}\right)^{13} = \frac{-181-\sqrt{-7}}{2}.$$

Cum sit $181^2 + 7 = 2\,(2^7)^2$, erit $181^2 = 2\Box - 7$. Consideretur formula $2xx - 7yy$ reddaturque quadratum: Ponatur $x = 2y + z$ eritque $yy + 8yz + 2zz$, cujus radix statuatur

$$y + \frac{p}{q}z, \quad \text{eritque} \quad 8y + 2z = \frac{2p}{q}y + \frac{pp}{qq}z, \quad \text{unde fit} \quad \frac{y}{z} = \frac{pp - 2qq}{8qq - 2pq}.$$

Statuatur ergo $y = pp - 2qq$ et $z = 8qq - 2pq$, eritque radix illa quadrata $8pq - pp - 2qq$, in qua ergo forma contineri debet 181, quod fit si $q = 5$ et $p - 4q = 13$, ideoque $p = 33$, vel $p = 7$, ergo $y = -1$ et $z = 130$ et $x = 128$. Eritque ergo $181^2 = 2.128^2 - 7$, uti habuimus $181^2 + 7 = 2\,(2^7)^2$.

A. m. T. II. p. 110—113.

36.

(*J. A. Euler.*)

Hujus seriei: 1^2, 3^2, 6^2, 10^2, 15^2, etc. ad minimum duodecim termini conjungi debent, ut omnes numeri prodeant. At seriei

$$1^n,\quad 2^n,\quad 3^n,\quad 4^n,\quad 5^n,\quad 6^n,\quad \text{etc.}$$

ad minimum tot termini jungi debent quot indicat haec formula

$$\frac{3^n}{2^n} + 2^n - 2 = T,$$

ubi pro $\frac{3^n}{2^n}$ numerus integer proxime minor capi debet

$$\begin{array}{llllllllll} \text{si} & n = 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, \\ \text{fit} & T = 1, & 4, & 9, & 19, & 37, & 73, & 143, & 279. \end{array}$$

Pro numeris figuratis litera T ita se habet:

*

	T		T		T
1. 2. 3. 4. 5. 6	1	1. 3. 5. 7. 9	2	1. $1+a$. $1+2a$. $1+3a$	a
1. 3. 6. 10. 15. 21	3	1. 4. 9. 16. 25	4	1. $2+a$. $3+3a$. $4+6a$	$a+2$
1. 4. 10. 20. 35. 56	5	1. 5. 14. 30. 55	6	1. $3+a$. $6+4a$. $10+10a$	$a+4$
1. 5. 15. 35. 70	7	1. 6. 20. 50. 105	8	1. $4+a$. $10+5a$. $20+15a$	$a+6$
				1. $5+a$. $15+6a$. $35+21a$	$a+8$

(*Krafft.*)

Omnes illae superiores series numerorum figuratorum sequenti forma generali comprehendi possunt

$$1; \quad \frac{n+a}{1}; \quad \frac{(n+1)(n+2a)}{1.2}; \quad \frac{(n+1)(n+2)(n+3a)}{1.2.3}; \quad \frac{(n+1)(n+2)(n+3)(n+4a)}{1.2.3.4} \quad \text{etc.}$$

pro qua superior littera T fit $=a+2n-2$.

A. m. T. I. p. 234. 235.

C. Analysis Diophantea.

a) *Quaestiones ad resolutionem unius aequationis ducentes.*

37.

(*J. A. Euler.*)

Problema. Si fuerit $x^3=m$, et proposita sit formula $axx+bx+c$, invenire multiplicatorem $pxx+qx+r$, ut productum

$$(axx+bx+c)(pxx+qx+r)$$

fiat numerus absolutus non amplius involvens x, posito scilicet $x^3=m$.

Solutio. Productum ergo erit

$$\begin{aligned} &mapx+(aq+bp)m+(ar+bq+cp)xx \\ &+(br+cq)x+cr. \end{aligned}$$

Debet ergo poni $br+cq+map=0$ et $ar+bq+cp=0$, tum enim productum erit

$$m(aq+bp)+cr.$$

Fit autem

$$p=\frac{-br-cq}{ma}=\frac{-ar-bq}{c},$$

unde fit $bcr+ccq=maar+mabq$; hinc $mabq-ccq=bcr-maar$,

$$\text{consequenter} \qquad \frac{q}{r}=\frac{bc-maa}{mab-cc}.$$

Capiatur ergo $q=bc-maa$, $r=mab-cc$, erit $p=ac-bb$, ita ut multiplicator quaesitus sit

$$(ac-bb)xx+(bc-maa)x+mab-cc;$$

ac tum productum erit

$$3mabc-m^2a^3-mb^3-c^3.$$

A. m. T. I. p. 50. 51.

38.

Problema. Invenire numeros x et y, ut fiat $xy(xx-yy)=\alpha nn$, existente α numero primo: ubi hi casus sunt notandi:

I. Si $\alpha=7$, sumatur $x=16$ et $y=9$, tum enim fit $xy(xx-yy)=7.16.9.25$.

II. Si $\alpha=13$, sumatur $x=325$ et $y=36$, erit $xy(xx-yy)=13.25.36.361.289$.