# X.

# Fragmenta arithmetica ex Adversariis mathematicis (*) depromta.

## A. Divisores numerorum.

### a) *De numeris formae* mxx + nyy *eorumque divisoribus.*

**1.**

(*J. A. Euler.*)

Theorema. Si formula $mxx+nyy$ casu $x=a$ et $y=b$ praebeat numerum primum $\alpha$, tunc omnes numeri primi in formula $\alpha\pm 4mnp$ contenti simul erunt numeri formae $mxx+nyy$. Quin etiam omnes numeri primi in hac formula $aqq\pm 4mnp$ contenti simul erunt numeri formae $mxx+nyy$.

NB. Demonstratio adhuc desideratur. A. m. T. I. p. 13.

**2.**

(*Lexell.*)

Si formula $mxx+nyy$ divisibilis fuerit per numerum integrum $i$, infinitae aliae similes formulae per eundem divisibiles exhiberi possunt.

In genere enim haec formula $m(\alpha x\pm\beta i)^2+n(\alpha y\pm\gamma i)^2$ per $i$ erit divisibilis, quicunque numeri integri pro $\alpha$, $\beta$, $\gamma$ accipiantur; semper autem numeros $\alpha$, $\beta$, $\gamma$ ita accipere licebit, ut quadratorum radices ambae $\alpha x-\beta i$ et $\alpha y-\gamma i$ infra $\frac{1}{2}i$ deprimantur, quin etiam altera $\alpha x-\beta i$ ad unitatem revocari poterit, quum enim numeri $x$ et $i$ dentur pro fractione $\frac{i}{x}$, quaeratur in numeris minoribus fractio illi proxime aequalis $\frac{\alpha}{\beta}$, ita ut sit $\alpha x-\beta i=\pm 1$, quo casu invento sit altera radix $\alpha y-\gamma i=r$, atque hi duo valores $x=1$ et $y=r$ quasi principales spectentur, tum vero reliqui ordine in hac tabella exhibentur:

| $x$ | $y$ |
|---|---|
| 1 | $r$ |
| 2 | $2r\pm\delta i$ |
| 3 | $3r-\delta i$ |
| 4 | $4r-\delta i$ |
| 5 | $5r-\delta i$ |

Jam pulchra hic occurrit quaestio, quinam horum valorum pro $x$ et $y$ producturi sint minimam formulam $mxx+nyy$, quae cum minor sit quam $\frac{1}{4}(m+n)ii$, quotus certe minor erit quam $\frac{1}{4}i(m+n)$, ideoque erit vel 1, vel 2, vel 3 etc.

Exempli gratia, sit formula proposita $3xx+2yy$ et sumatur $x=7$, $y=2$, ac prodit numerus 155, cujus divisor sumatur $=i=31$, ut jam proxime fiat $\frac{i}{x}=\frac{31}{7}=\frac{\alpha}{\beta}=\frac{9}{2}$, sive $\alpha=9$ et $\beta=2$; tum enim fit

(*) Tomus I p. 1 ad 346, ab A. 1766 ad med. Apr. 1775; tomus II p. 1 ad 246, inde usque ad Junium 1779; tomus III p. 1 ad 184, inde usque ad mortem Euleri, 1783.

$\alpha x-\beta i=63-62=+1$, et altera radix $\alpha y-\gamma i=18-31=-13=r$,

unde fiat sequens tabula:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $x$ | 1, | 2, | 3, | 4, | 5, | 6, | 7 |
| $y$ | 13, | 5, | 8, | 10, | 3, | 15, | 2. |

Minima formula hinc nascens erit secunda: $3.2^2+2.5^2=62$, quod per 31 divisum dat quotum minimum 2.

A. m. T. I. p. 94. 95.

**3.**

Theorema. Si fuerit numerus primus formae $p=8n+5$, constat semper dari formam $aa+1$ per illum numerum $p$ divisibilem, tum vero nulla hujusmodi forma $xx\pm ayy$ unquam erit per $p$ divisibilis. Contra autem pro numeris primis formae $p=8n+1$ datur etiam forma $aa+1$ per $p$ divisibilis, tum vero dabuntur formulae $xx\pm ayy$ per $p$ divisibiles.

Demonstratio eo nititur fundamento, quod priori casu numerus $a$ semper sit non-residuum, in posteriori vero residuum; illud autem inde ostenditur, quod numerus residuorum sit $4n+2$, inter quos quilibet numerus utroque signo $+$ et $-$ occurrit, unde multitudo diversorum residuorum erit $2n+1$, scilicet impar; sin autem numerus ille $a$ inter residua esset, haec multitudo prodiret par, quod esset absurdum.

A. m. T. I. p. 114.

**4.**

(*N. Fuss I.*)

Theorema. Si formula $naa+bb$ divisibilis sit per numerum $p$, semper dari poterit formula $n+qq$ divisibilis per eundem numerum $p$, ita ut $q<\frac{1}{2}p$.

Demonstratio. Quaeratur primo formula generalis $nxx+yy$ per numerum $p$ divisibilis, quod fit sumendo $x=\alpha a-\beta p$ et $y=\alpha b-\gamma p$; tum enim ista formula erit $\alpha\alpha(naa+bb)-2p(na\alpha\beta+\alpha b\gamma)+pp(n\beta\beta+\gamma\gamma)$, quae ergo per $p$ est divisibilis. Jam semper numeros $\alpha$ et $\beta$ ita accipere licebit, ut fiat $\alpha a-\beta p=1$, ideoque $x=1$, quaerendo scilicet fractionem $\frac{\alpha}{\beta}$ proxime aequalem ipsi $\frac{p}{a}$. Cum igitur sit $y=\alpha b-\gamma p$, numerum semper ita accipere licebit, ut fiat $y$ non solum minus quam $p$, sed etiam minus quam $\frac{1}{2}p$.

Problema. Quando formula $naa+bb$ divisibilis est per numerum $p$, quotum ex divisione resultantem per formulam integram exprimere.

Solutio. Cum igitur detur numerus $q$, ut sit $n+qq$ divisibile per $p$, ponatur $\frac{n+qq}{p}=r$ sumaturque $b=qa+pd$ eritque $naa+bb=naa+qqaa+2pqad+ppdd$, quae ob $n=pr-qq$ abit in $p(raa+2qad+pdd)$, quae ergo per $p$ divisa dat $raa+2qad+pdd$. Quod autem poni possit $b=qa+pd$, sive ut $\frac{b-qa}{p}$ semper sit numerus integer, inde patet, quod etiam detur formula $n+qq$ per $p$ divisibilis, ideoque etiam $naa+aaqq$, quarum differentia $bb-aaqq$ per $p$ divisibilis erit, unde cum $p$ supponatur numerus primus, vel $b+aq$, vel $b-aq$ per $p$ divisibile, utrumvis perinde est. Quia ergo $\frac{b-qa}{p}$ integer sit $=d$, ideoque poni semper poterit $b=qa+pd$.

A. m. T. II. p. 209.

**5.**

Theorema. Omnis numerus primus formae $8n+1$ semper in forma $xx+2yy$ continetur.

Demonstratio. Sufficiet ostendisse semper exhiberi posse formam $A^2+2B^2$ per $8n+1$ divisibilem. Demonstratum autem est, hanc formam $a^{8n}-b^{8n}$ semper divisibilem esse per $8n+1$, quicunque numeri primi $a$ et $b$ accipiantur, scilicet primi ad $8n+1$. Ergo $a^{4n}-b^{4n}$, vel $a^{4n}+b^{4n}$ erit divisibilis. Facile autem demonstratur non omnes numeros $a^{4n}-b^{4n}$ divisibiles esse. Dantur ergo casus, quibus forma $a^{4n}+b^{4n}$ est divisibilis. Habebitur ergo summa duorum biquadratorum divisibilis $A^4+B^4$. Quare cum sit $a^4+b^4=(aa-bb)^2+2aabb$, propositum est demonstratum. — Ita cum 97 in forma $8n+1$ contineatur, reperitur $97=5^2+2.6^2$.

Theorema. Omnis numerus primus formae $8n+3$ simul in forma $xx+2yy$ continetur.

Demonstratio. Iterum sufficiet ostendisse, dari formam $A^2+2B^2$ per $8n+3$ divisibilem. Cum igitur haec forma $a^{8n+2}-b^{8n+2}$ semper sit divisibilis, quicunque numeri pro $a$ et $b$ accipiantur, erit vel $a.a^{4n}-b.b^{4n}$, vel $a.a^{4n}+b.b^{4n}$ divisibilis. Jam sumatur $a=cc$ et $b=2dd$ ut $a.a^{4n}$ fiat quadratum $A^2$ et $b.b^{4n}$ duplum quadratum, puta $2B^2$, sicque vel forma $A^2-2B^2$, vel $A^2+2B^2$ divisionem admittet per $8n+1$. At vero demonstratum est, formam $A^2-2B^2$ alios divisores non admittere, nisi vel formae $8n+1$, vel formae $8n-1$, unde sequitur alteram formam $A^2+2B^2$ divisibilem esse. Ita cum sit $107=8.13+3$, reperitur esse $107=3^2+2.7^2$, hocque semper unico modo, quod ita demonstratur:

Sit $P=aa+2bb$ simulque $P=cc+2dd$, numerus $P$ necessario est compositus. Cum enim sit

$$aa+2bb=cc+2dd, \quad \text{erit} \quad aa-cc=2(dd-bb),$$

unde sequitur $\frac{a+c}{b+d}=\frac{2(d-b)}{a-c}=\frac{p}{q}$. Erit ergo $a+c=\alpha p$ et $d+b=\alpha q$, $d-b=\beta p$ et $a-c=2\beta q$. Hinc $2a=\alpha p+2\beta q$ et $2b=\alpha q-\beta p$; quare cum $4P=4aa+2.4bb$ erit $4P=(\alpha\alpha+2\beta\beta)(pp+2qq)$, sicque $4P$ certe duos habet factores, quorum neuter unquam esse potest neque 1 neque 4; sequitur $P$ ad minimum duos habere factores:

| | |
|---|---|
| $3=1^2+2.1^2$ | $59=3^2+2.5^2$ |
| $11=3^2+2.1^2$ | $67=7^2+2.3^2$ |
| $19=1^2+2.3^2$ | $83=9^2+2.1^2$ |
| $43=5^2+2.3^2$ | $107=3^2+2.7^2$. |

Notandum hic, praeter casum primum, in omnibus reliquis alterum quadratum semper per 9 esse divisibile.

A. m. T. III. p. 180. 181.

## 6.

Theorema. Propositis numeris quibuscunque $a, b, c, d$, si numerus formae $abpp+cdqq$ multiplicetur per numerum formae $acrr+bdss$, tum productum semper continebitur in hac forma $bcxx+adyy$.

Demonstratio facile patet. Sumto enim $x=apr+dqs$ et $y=bps-cqr$, postrema forma $bcxx+adyy$ reperitur productum binarum praecedentium.

A. m. T. III. p. 182.

(*Golovin.*)

Theorema. Productum ex duabus hujusmodi formulis $aa+ab+bb$ et $cc+cd+dd$ semper ad similem formam $xx+xy+yy$ reduci potest. Est enim duplici modo

$$\text{vel} \quad x=ac+b(c+d) \quad \text{et} \quad y=ad-bc$$

$$\text{vel etiam} \quad x=ad+b(c+d) \quad \text{et} \quad y=ac-bd.$$

Ita si fuerit $a=3$ et $b=2$, tum vero $c=1$ et $d=5$, erit $aa+ab+bb=19$ et $cc+cd+dd=31$; prior igitur resolutio dat $x=15$ et $y=13$, hincque $xx+xy+yy=589$.

A. m. T. II. p. 204.

(*Lexell.*)

Theorema. Si formula $\alpha aa+2\beta ab+\gamma bb$ per aliam sui similem $\alpha pp+2\beta pq+\gamma qq$ multiplicetur, productum prodit hujus formae

$$xx+2\beta xy+\alpha\gamma yy \quad \text{eritque} \quad x=\alpha ap-\gamma bq \quad \text{et} \quad y=aq+bp+\frac{2\beta}{\alpha}bq.$$

Corollarium. Ita si fuerit $\alpha=1$, $2\beta=1$ et $\gamma=1$, erit $(aa+ab+bb)(pp+pq+qq)=xx+xy+yy$ existente $x=ap-bq$ et $y=aq+bp+bq$.

*Nota Editorum.* Casum specialem, quo $\beta=0$, vide Comment. arithm. T. II, p. 201.

A. m. T. I. p. 26.

Theorema. Si formula $\alpha app + b\beta qq$ ducatur in formulam $abrr + \alpha\beta ss$, productum erit:

$$ab(\alpha apprr + \beta\beta qqss) + \alpha\beta(\alpha appss + bbqqrr) = \alpha b(apr \pm \beta qs)^2 + \alpha\beta(aps \pm bqr)^2,$$

hujus ergo producti forma est $\alpha bxx + \alpha\beta yy$ existente $x = apr \pm \beta qs$ et $y = aps \pm bqr$.

(Conf. pro casu $a = b = 1$ Comment. arithm. T. II, p. 201.)

Problema. Formulam $\alpha axx + b\beta yy$ in aliam ejusdem generis transformare.

Solutio. Ponatur $x = bmp + \beta nq$ et $y = anp - amq$ et prodibit

$$\alpha abbmmpp + \alpha a\beta\beta nnqq + b\beta aannpp + b\beta\alpha ammqq = \alpha bmm(abpp + \alpha\beta qq) + a\beta nn(\alpha\beta qq + abpp) = (\alpha bmm + a\beta nn)(abpp + \alpha\beta qq).$$

A. m. T. I. p. 130.

## 7.

(N. Fuss I.)

Theorema. Si numerus formae $xx + nyy$ divisibilis fuerit per numerum $pp + nqq$, quotus semper erit numerus ejusdem formae $A^2 + nB^2$.

Demonstratio. Cum numeri $x$ et $y$ ad $pp + nqq$ debeant esse primi, et $p$ et $q$ quoque sint primi inter se, quicunque fuerint numeri $x$ et $y$, semper per $p$ et $q$ ita repraesentari possunt, ut sit $x = \alpha p + \beta q$ et $y = \gamma p + \delta q$. Hoc modo formula $xx + nyy$ abit in hanc: $pp(\alpha\alpha + n\gamma\gamma) + qq(\beta\beta + n\delta\delta) + 2pq(\alpha\beta + n\gamma\delta)$, quae per $pp + nqq$ divisa praebeat quotum $\Delta$, ita ut sit

$$pp(\alpha\alpha + n\gamma\gamma) + qq(\beta\beta + n\delta\delta) + 2pq(\alpha\beta + n\gamma\delta) = \Delta pp + n\Delta qq.$$

Hinc igitur patet fore $\Delta = \alpha\alpha + n\gamma\gamma$, $n\Delta = \beta\beta + n\delta\delta$ et $\alpha\beta + n\gamma\delta = 0$, unde jam patet formam ipsius $\Delta$ esse $\alpha\alpha + n\gamma\gamma$. Tum etiam erit $n\Delta = \beta\beta + n\delta\delta$ et $\alpha\beta + n\gamma\delta = 0$. Ex ultima fit $\frac{\beta}{\delta} = \frac{-n\gamma}{\alpha}$. Ponatur ergo

$$\delta = \alpha f \text{ et } \beta = -n\gamma f, \quad \text{erit} \quad \beta\beta + n\delta\delta = nff(\alpha\alpha + n\gamma\gamma) = n\Delta, \quad \text{unde} \quad \Delta = ff(\alpha\alpha + n\gamma\gamma).$$

Cum igitur sit $\Delta = \alpha\alpha + n\gamma\gamma$, sequitur fore $f = \pm 1$. His valoribus fit

$$x = \alpha p \mp n\gamma q \quad \text{et} \quad y = \gamma p \pm \alpha q.$$

Hinc fit $$xx + nyy = pp(\alpha\alpha + n\gamma\gamma) + nqq(\alpha\alpha + n\gamma\gamma) = (pp + nqq)(\alpha\alpha + n\gamma\gamma),$$

sicque quotus, uti jam vidimus, $\Delta = \alpha\alpha + n\gamma\gamma$.

A. m. T. III. p. 184.

## 8.

Theoremata demonstranda. I. Si fuerit $4na + bb$ numerus primus, erit semper hujus formae $xx + ayy$.

II. Si fuerit $4na - bb$ numerus primus, erit semper hujus formae $ayy - xx$.

A. m. T. II. p. 154.

## 9.

Theorema. Si numerus $mnff + gg$ divisorem habeat primum $p = \frac{maa + nbb}{\Delta}$, tum etiam quotus $q$, ex hac divisione ortus, erit quoque ejusdem formae scilicet $q = \frac{mcc + ndd}{\Delta}$.

Explicatio. Quaerantur primo duo numeri $\lambda$ et $\mu$, ut sit $\lambda a - \mu p = \pm 1$; deinde ut formula $mnff + gg$ divisorem admittat $p$, alteram litteram $f$ pro lubitu accipere licet, tum vero altera $g$ ita esse debet comparata, ut sit $g = n\lambda bf - \nu p$, quibus notatis cum sit $mnff + gg = pq$ existente $q = \frac{mcc + ndd}{\Delta}$, litterae $c$ et $d$ sequenti modo determinantur

$$c = n\mu bf - \nu a \quad \text{et} \quad d = m\mu af + \nu b - \lambda\Delta f.$$

A. m. T. II. p. 244.

## b) *De divisoribus numerorum formae* $fa^n + gb^n$.

### 10.

(*Lexell.*)

Problema. Si formula $fa^n + gb^n$ divisorem habeat $d$, invenire infinitas alias similes formas $fx^n + gy^n$ per eundem numerum $d$ divisibiles.

Solutio. Capiatur $x = ma \pm \mu d$, et $y = mb \pm \nu d$, et quaesito satisfiet; si enim $\mu$ et $\nu = 0$, res est manifesta; sin autem multipla ipsius $d$ accedant, omnes termini post primos ex evolutione nati, per se sunt divisibiles per $d$.

Problema. Invenire omnes divisores primos formulae $x^4 + y^4$. Cum haec formula sit factor hujus $x^8 - y^8$, demonstratum est, omnes ejus divisores contineri in forma $8n + 1$, quod etiam hoc modo ostenditur: Cum formae $a^2 + b^2$ omnes divisores sint formae $4n + 1$, ponamus formulae $aa + bb$ divisorem primum esse $4n + 1 = d$; tum ergo etiam omnes formulae $xx + yy$ per eundem numerum erunt divisibiles sumendo $x^2 = ma \pm \mu d$, $y^2 = mb \pm \nu d$.

Pro nostro ergo casu hi ambo numeri debent esse quadrati. Pro priore sumto $\mu = 0$, hoc fiet si $m = app$, ut fiat $x = ap$. Superest ergo, ut et haec forma $y^2 = abpp \pm \nu d$ fiat quadratum, idque sive positivum sive negativum. Ponatur ergo $abpp \pm \nu d = \pm qq$ et res huc redit, ut $abpp \pm qq$ divisibile fiat per $d$, et quia statui potest $a^2 + b^2 = d$, quaeritur ergo quibus casibus formula $abpp \pm qq$ divisibilis fieri possit per $d$. Varios ergo casus evolvamus:

I. Sit $d = 5$, erit $a = 2$ et $b = 1$, unde formula $2pp \pm qq$ divisorem habere deberet 5, id quod fieri nequit, neque vero 5 continetur in forma $8n + 1$, atque hinc vicissim concludere possumus, neque $2pp + qq$, nec $2pp - qq$ unquam divisibile esse per 5.

II. Sit $d = 13$, erit $a = 2$ et $b = 3$, et nunc quaeritur an formula $6pp \pm qq$ divisibilis esse possit per 13, id quod negari debet, quia 13 non est formae $8n + 1$.

III. Sit $d = 17$, erit $a = 1$ et $b = 4$, nunc quaeritur an $4pp \pm qq$ divisibilis esse possit per 17, quod utique affirmandum, verum est etiam $17 = 8n + 1$.

IV. Sit $d = 29$ erit $a = 2$ et $b = 5$, et quaeritur an $10pp \pm qq$ divisibilis esse possit per 29, quod quia 29 non est $8n + 1$, negari debet.

Corollarium 1. Hic ergo distingui oportet duos casus, prouti existente $b$ numero impari, numerus $a$ fuerit vel impariter par, vel pariter par. Priori casu divisor $d$ non erit formae $8n + 1$, sed formae $8n + 5$, ideoque hic casus est excludendus. Sit igitur

$$a = 4\alpha \pm 2, \quad \text{et} \quad b = 4\beta \pm 1, \quad \text{eritque} \quad aa + bb = 16(\alpha^2 + \beta^2) \pm 16\alpha \pm 8\beta + 5.$$

Ergo per talem divisorem nunquam divisibilis erit haec forma $(16\alpha\beta \pm 4(\alpha \pm 2\beta) \pm 2)pp \pm qq$. Per numerum ergo primum $16(\alpha^2 + \beta^2) + 16\alpha + 8\beta + 5$ talis formula $16\alpha\beta + 4(2\beta + \alpha) + 2$ nunquam est divisibilis.

Corollarium 2. Sin autem manente $b = 4\beta + 1$ (ubi $\beta$ etiam negative capere licet) sit $a = 4\alpha$, erit $aa + bb = 16(\alpha\alpha + \beta\beta) + 8\beta + 1$, et nunc certi sumus, dari formulas $4\alpha(4\beta + 1)pp \pm qq$, quae divisorem habeant $16(\alpha\alpha + \beta\beta) + 8\beta + 1$.

Corollarium 3. Si igitur verum est, omnes numeros primos formae $8n + 1$ divisores esse posse formulae $x^4 + y^4$, sequitur nostram formulam $16(\alpha^2 + \beta^2) + 8\beta + 1$ omnes plane numeros $8n + 1$ in se continere siquidem fuerint primi. Aequemus ergo has formas et reperimus

$$n = 2(\alpha^2 + \beta^2) \pm \beta,$$

ubi $n$ denotat omnes plane numeros saltem eos, qui faciunt $8n + 1$ primos:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0, | 2, | 8, | 18, | 32, | 50, | 72, | 98 |
| 1, | 4, | 11, | 22, | 37, | 56, | 79, | 106 |
| 1, | 2, | 7, | 16, | 29, | 46, | 67, | 92 |

sive $2(\alpha^2+\beta^2)\pm\beta=0,$ 1, 3, 6, 10, 15, 21, 38, 36, 45, 55, 66, 78, 91, 105
2, 3, 5, 8, 12, 17, 23, 30, 38, 47, 57, 68, 80, 93, 107,
8, 9, 11, 14, 18, 23, 29, 36, 44, 53, 63, 74, 86, 99
18, 19, 21, 24, 28, 33, 39, 46, 54, 63, 73, 84, 96, 109
32, 33, 35, 38, 42, 47, 53, 60, 68, 77, 87, 98 . . . .
50, 51, 53, 56, 60, 65, 71, 78, 86, 95 . . . . . .
71, 72, 74, 77, 81, 86, 92, 99 . . . .
98, 99 . . . .

Hic omnes numeri non occurrunt, sed excluduntur 4, 7, 13, 16, 20, 22, 25, 26, 27, etc. at vero ex his omnibus $8n+1$ non fit primus.

Si igitur $A$ denotet numerum impariter parem $4n+2$ et $B$ numerum pariter parem sive $4n$, et $C$ numerum imparem $2n+1$, tum haec duo habentur theoremata:

I. Per numerum primum $A^2+C^2$ neutra formula $ACpp\pm qq$ unquam dividi potest; neque etiam summa duorum biquadratorum, unde sequitur, si singula quadrata per $A^2+C^2$ dividantur, tum in residuis neque $+AC$, neque $-AC$ occurrere, sed certo esse non-residua.

II. Sin autem divisor primus fuerit $B^2+C^2$, tum semper datur formula $BCpp\pm qq$ per eum divisibilis, ac propterea etiam summa duorum biquadratorum, atque in residuis quadratorum, per eundem numerum primum $B^2+C^2$ divisorum, tam $+BC$, quam $-BC$ reperientur.

Problema. Invenire omnes divisores primos formulae $fx^4+gy^4$.

Cum omnes constent divisores formulae $faa+gbb$, qui sive in formula $f\alpha\alpha+g\beta\beta$, sive in hac $\alpha\alpha+fg\beta\beta$ continentur, sit quilibet eorum $=d$, per quem formula $faa+gbb$ sit divisibilis; tum sumto $X=ma\pm\alpha d$ et $Y=mb\pm\beta d$, ut formula $fX^2+gY^2$ etiam per $d$ fiat divisibilis, jam reddatur primo $X$ quadratum, quod fit si $m=app$; tum vero erit $Y=abpp\pm\beta d$, quod etiam quadratum reddi debet, quod sit $\pm qq$, et nunc oportet ut $abpp\pm qq$ divisibile fiat per $d$, eritque $Y=\pm qq$ et $X=aapp$, quare sumto $x=ap$ et $y=q$ fiet $fx^4+gy^4$ per $d$ divisibile. Huc ergo redit quaestio: quibus casibus formula $abpp\pm qq$ dividi queat per memoratum divisorem $d$ qui est vel $f\alpha\alpha+g\beta\beta$, vel $\alpha\alpha+fg\beta\beta$.

Exemplum 1. Sit $f=1$ et $g=2$, ideoque $d=\alpha\alpha+2\beta\beta$, qui numeri sunt vel $8n+1$, vel $8n+3$, quos valores percurramus. Sit

I. $d=3$, per quem formula $aa+2bb$ divisibilis fit; si $a=1$ et $b=1$, unde quaeritur an formula $pp\pm qq$ divisibilis fieri queat per 3, quod cum eveniat, etiam 3 erit divisor formulae $x^4+2y^4$.

II. Sit $d=11$, erit $a=3$ et $b=1$, hinc nostra formula $3pp\pm qq$ divisibilis per 11, at ipsius $3pp+qq$ divisores sunt formae $12n+1$, $12n+7$, formulae autem $3pp-qq$ divisores sunt vel $12n+1$, vel $12n-1$, ideoque postremus casus quaestioni satisfacit, ergo datur formula $x^4+2y^4$ per 11 divisibilis.

III. Sit $d=17$, $a=3$, $b=2$, ergo formula nostra per 17 divisibilis erit $6pp\pm qq$, at prior $6pp+qq$ non est divisibilis, neque etiam posterior, unde sequitur nullam formam $x^4+2y^4$ dividi posse per 17.

IV. Sit $d=19$, erit $a=1$ et $b=3$ et formula per 19 divisibilis erit $3pp\pm qq$, id quod fieri potest ponendo ex. causa $p=1$ et $q=4$, hinc $x=1$ et $y=4$, atque formula $x^4+2y^4$ erit divisibilis per 19.

V. Sit $d=41$, erit $a=3$ et $b=4$, et haec formula nostra per 41 divisibilis reddenda fit $12pp\pm qq$, sive haec $3pp\pm qq$,* at 41 in nulla harum formularum $12n\pm1$, $12n+7$ continetur. Ergo non datur $x^4+2y^4$ per 41 divisibilis.

VI. Sit $d=43$, erit $a=5$ et $b=3$, hinc formula per 43 divisibilis $15pp\pm qq$, sive etiam $5pp\pm3qq$, id quod succedit, cum sit $43=3\cdot4^2-5\cdot1^2$, ergo datur forma $x^4+2y^4$ per 43 divisibilis. Si $x=ap=20$, $y=$ sive $x=4$, $y=1$.

VII. Sit $d=59$, erit $a=3$ et $b=5$, hinc formula $15pp \pm qq$, sive $5pp \pm 3qq$, ubi manifesto $15.2^2-1$, ergo $x=6$, $y=1$, et formula $x^4+2y^4$ per 59 divisibilis.

Corollarium 1. Videtur ergo, quoties fuerit $d=8n+3$, tum fore divisorem formae $x^4+2y^4$, nec non et hujus $abpp \pm qq$, at vero tum fiunt ambo numeri $a$ et $b$ impares; quoties ergo $aa+2bb$ fuerit numerus primus, semper datur formula $abpp \pm qq$ per eum divisibilis, sive inter residua quadratorum reperietur vel $+ab$, vel $-ab$.

Corollarium 2. Contra autem non omnes numeri $8n+1$ excluduntur, quia numerus $113=3^4+2.2^4$.

VIII. Sit $d=67$, $a=7$, $b=3$, formula $21pp \pm qq$, vel $7pp \pm 3qq$, $p=5$, $q=6$, vel $x=35$, $y=18$.

Exemplum 2. Sumatur $f=1$ et $g=3$, ut quaerantur divisores formulae $x^4+3y^4$ et divisor $d$ erit $aa+3bb$, erit ergo vel formae $12n+1$, vel $12n+7$.

I. Sit $d=7$, erit $a=2$ et $b=1$, et formula $\frac{2pp \pm qq}{7}$, quod succedit quia $7=2.2^2-1$, unde $p=2$, $q=1$, $x=4$, $y=1$.

II. Sit $d=13$, erit $a=1$ et $b=2$ et formula $\frac{2pp \pm qq}{13}$, quae est impossibilis.

III. Sit $d=19$, erit $a=4$ et $b=1$ et formula $\frac{4pp \pm qq}{19}$, quae succedit: $p=9$, $q=1$, $x=36$ et $y=1$.

IV. Sit $d=31$, erit $a=2$ et $b=3$ et formula $\frac{6pp \pm qq}{31}$, vel $\frac{3pp \pm 2qq}{31}$, $x=18$, $y=5$.

V. Sit $d=37$, erit $a=5$ et $b=2$ et formula $\frac{10pp \pm qq}{37}$, vel $\frac{5pp \pm 2qq}{37}$, $p=1$, $q=8$, $x=5$, $y=8$.

VI. Sit $d=43$, erit $a=4$ et $b=3$ et formula $\frac{12pp \pm qq}{43}$, vel $\frac{3pp \pm qq}{43}$, $x=12$, $y=8$, $x=3$, $y=2$.

Hic igitur maxime est mirandum, quod solus numerus 13 hic sit exclusus.

Problema superius de divisoribus $fx^4+gy^4$ ita concinnius resolvitur:

Sit $d$ divisor hujus formulae, qui necessario erit divisor talis formulae $fa^2+gb^2$. Cum igitur hae duae formulae $faa+gbb$ et $fx^4+gy^4$ habere debeant communem divisorem $d$, multiplicetur prior per $x^4$ et posterior per $aa$, horumque productorum differentia, quae est $gbbx^4-gaay^4=g(bx^2-ay^2)(bx^2+ay^2)$ etiam nunc erit divisibilis per $d$; unde si $d$ sit numerus primus, per quem neque $f$, neque $g$ divisibilis esse potest, ob

$$bbx^4-aay^4=(bx^2+ay^2)(bx^2-ay^2),$$

necesse est, ut horum factorum alter $bx^2 \pm ay^2$ sit divisibilis per $d$. Quare proposito numero primo $d$, qui dividat formulam $faa+gbb$, quoties assignari poterit formula $bxx \pm ayy$ per $d$ divisibilis, tunc etiam formula $fx^4+gy^4$ per eundem numerum $d$ divisibilis erit.

Corollarium. Si datur formula $bxx \pm ayy$ per $d$ divisibilis, etiam haec formula $zz \pm abyy$ divisibilis erit sumto $z=bx$; hoc autem eveniet, si inter residua quadratorum per $d$ divisorum, occurrat numerus $\pm ab$.

Theorema. Quoties divisor primus $d$ fuerit formae $4n-1$, isque dividat formulam $faa+gbb$, tum semper dabitur formula $fx^4+gy^4$ per $d$ divisibilis.

Demonstratio. Cum divisor $d$ sit formae $4n-1$, sive $4n+3$, si quadrata singula per eum dividantur, inter residua omnes plane numeri occurrent, sive signo plus, sive minus affecti, ergo etiam occurret numerus vel $+ab$, vel $-ab$, dabitur ergo formula $zz \pm abyy$, ideoque etiam $bxx \pm ayy$ per $d$ divisibilis.

Corollarium. At si $d$ fuerit formae $4n+1$, quia in residuis quadratorum non omnes numeri occurrunt, sed semissis adeo penitus excludatur, sive positive, sive negative capiantur, utique fieri potest, ut $\pm ab$ inter eas non occurrat et tum nulla dabitur formula $fx^4+gy^4$ per $d$ divisibilis. Observatum autem est (nondum vero demonstratum) omnes divisores formulae $axx \pm byy$ contineri in tali forma $4abn+kk$.

*

Hic jam duo occurrunt casus considerandi, prout vel ambo numeri $a$ et $b$ sunt impares, vel unus par et alter impar. Priori casu, semper possibile videtur, ut divisor $d$ in hac forma contineatur; at vero si $a$ fuerit numerus par, puta $2c$, forma divisorum erit $8bcn+kk$, quae reducitur ad formam $8n+1$. Quoties ergo hoc casu divisor $d$ formam habet $8n+5$, tum casus est impossibilis, unde sequitur haec conclusio:

*Quoties ergo* $d=8n+5$ *fuerit divisor formulae* $faa+gbb$, *insuperque alteruter numerorum* $a$ *et* $b$ *par, tum nulla dabitur formula* $fx^4+gy^4$ *per* $d$ *divisibilis.*

Theorema. Si numerus primus formae $4n+3$ dividat formulam $faa+gbb$, sive $aa+fgbb$, tum nulla dabitur formula $faa-gbb$, sive $aa-fgbb$ per $d$ divisibilis.

Demonstratio. Si enim formula $aa+fgbb$ divisibilis sit per $d$, tum inter residua quadratorum reperietur $-fg$, at $fg$ erit non-residuum, unde etiam nulla formula $aa-fgbb$ divisibilis erit per $d$.

Theorema. Si numerus primus formae $4n+1$ dividat formulam $faa+gbb$, sive $aa+fgbb$, tum etiam semper dabitur formula $faa-gbb$, sive $aa-fgbb$ divisibilis per $d$.

Demonstratio. Quia $d$ dividit formulam $aa+fgbb$, in residuis quadratorum occurret $-fg$, ideoque ob formam $4n+1$, ibidem quoque occurret $+fg$, ergo dabitur formula $faa-gbb$, sive $aa-fgbb$ itidem per $d$ divisibilis.

Corollarium. Quoties ergo evenit, ut formulae $faa+gbb$ divisor $d=4n+1$, non simul dividat formulam $fx^4+gy^4$, tum quia idem divisor est quoque formulae $faa-gbb$, forte erit divisor formulae $fx^4-gy^4$. Hoc autem secus evenit casu $f=1$, $g=2$ et $d=17$. Etsi enim $17=3^2+2.2^2$ et simul $17=2.3^2-1$, tamen neutra harum formularum $x^4+2y^4$ et $x^4-2y^4$ per 17 est divisibilis. Quo hoc accuratius scrutemur, consideremus residua ex divisione biquadratorum nata pro divisoribus $4n+1$, quae semper tantum numero $n$.

| Divisor | Residua |
|---|---|
| 5 | 1 |
| 13 | 1, 3, 9 |
| 17 | $+1$, $+4$ |
| | $-1$, $-4$ |
| 29 | $+1$, $+7$, $+20$ |
| | $-4$, $-5$, $-6$, $-13$ |
| 37 | $+1$, $+7$, $+9$, $+10$, $+12$, $+16$ |
| | $-3$, $-4$, $-11$ |
| 41 | $+1$, $+4$, $+10$, $+16$, $+18$ |
| | $-1$, $-4$, $-10$, $-16$, $-18$ |

Hinc ergo discimus, si divisor fuerit formae $8n+5$, tum numerum residuorum esse $2n+1$, ideoque imparem, unde nullum utroque signo occurrit, unde, si formula $fx^4+gy^4$ fuerit divisibilis, altera $fx^4-gy^4$ certe non erit divisibilis, quod autem vicissim non valet, quia numerus non-residuorum triplo major est, quam residuorum. Pro tali ergo divisoris forma vel neutra formularum $fx^4\pm gy^4$, vel unica saltem est divisibilis.

At si divisor fuerit formae $8n+1$, quodvis residuum utroque signo affectum occurrit, unde si una harum formularum fuerit divisibilis, etiam altera erit divisibilis, sive vel utraque, vel neutra divisibilis erit. Hinc sequitur *primo* si divisor primus $=8n+5$ dividat formulam $faa+gbb$, quo casu etiam dividet formulam $fa'a'-gb'b'$, illinc autem pro biquadratis formula $axx\pm byy$ per $d$ fuerit divisibilis, tum certe formula $a'x^2\pm b'y^2$ non erit divisibilis. *Deinde* si fuerit $d=8n+1$ et dividat tam formulam $faa+gbb$ quam $fa'a'-gb'b'$, tum si formula $axx\pm byy$ fuerit divisibilis, certe etiam altera $a'xx\pm b'yy$ erit divisibilis, et si illa non erit, etiam haec non erit.

A. m. T. I. p. 218—223.

**11.**

(*N. Fuss I.*)

Problema. Invenire omnes summas binorum biquadratorum $x^4+y^4$, quae sint divisibiles per datum numerum primum formae $8m+1=\Delta$.

Solutio. Cum haec formula $x^n+y^n$ alios divisores non admittat nisi formae $2in+1$, sequitur formulam $x^4+y^4$ alios divisores habere non posse nisi formae $8i+1$. Tales autem numeri sunt

17, 41, 73, 89, 97, 113, 137, 193, 233, 241, 257, 281, 313, 337, 353, 401, etc.

qui numeri cum omnes sint summae duorum quadratorum, sit $\Delta=aa+bb$. Deinde cum alter numerorum $x$ et $y$ pro lubitu accipi queat, sumatur $x=a$, et pro $y$ inveniendo quaeratur numerus quadratus formae $i\Delta\pm ab$, qui sit $pp$ atque sumi poterit $y=p$, vel in genere $y=\alpha\Delta\pm p$. Cum enim sit $pp=i\Delta\pm ab$, neglecto multiplo ipsius $\Delta$, quippe quod semper adjici potest, erit $y^4=p^4=aabb$, hinc ergo erit $x^4+y^4=aa(aa+bb)=aa\Delta$, ideoque $x^4+y^4$ divisorem habebit $\Delta$. Idem valor $y=p$ valet quoque pro $x=b$; tum enim erit

$$x^4+y^4=bb(aa+bb)=bb\Delta.$$

Praeter $p$ autem dabitur alius valor $q$, ut sit $p:q=a:b$, ideoque $q=\frac{bp}{a}$, sive $q=\frac{bp+i\Delta}{a}$; unde valor ipsius $q$ semper erit integer. Sumto enim

$$x=a \text{ et } y=q=\frac{bp}{a}, \text{ erit } x^4+y^4=a^4+\frac{b^4p^4}{a^4} \text{ et ob } p^4=aabb, \text{ erit } x^4+y^4=\frac{a^6+b^6}{aa}.$$

At vero $a^6+b^6$ semper habet factorem $aa+bb=\Delta$. Eodem modo patet, sumto $x=b$ et $y=q$, etiam $x^4+y^4$ factorem $\Delta$ esse habiturum. Sumto igitur sive $a$ sive $b$ pro $x$, tum pro $y$ sumi poterit sive $p$ sive $q$; unde patet, si pro $x$ capiatur vel $na$ vel $nb$, tum pro $y$ sumi debere vel $np$ vel $nq$, qui valores, cum semper multiplum ipsius $\Delta$ auferre liceat, omnes hos valores infra $\frac{1}{2}\Delta$ deprimere licebit. Praeterea vero ad singulos hos valores quaevis multipla ipsius $\Delta$ addi possunt. Hoc modo pro quovis divisore $\Delta$ tabula construi poterit duabus constans columnis, quarum prior binos valores ipsius $x$, altera vero binos ipsius $y$ exhibebit, id quod exemplis illustremus.

I. Sit $\Delta=17=4^2+1^2$, erit $a=1$ et $b=4$. Nunc igitur erit $pp=17n\pm4$, unde statim sumi potest $n=0$ et $p=2$ et ob $1:4=p:q$ erit $q=8$. Hinc

| $x$ | $y$ |
|---|---|
| 1, 4 | 2, 8 |
| 2, 8 | 4, 1 |
| 3, 5 | 6, 7 |

ubi, quia $x$ et $y$ sunt permutabiles, secundi valores, utpote in primis jam contenti, omitti possunt, ita ut tabula duos tantum casus involvit, scilicet pro $x$, 1, 4 et 3, 5, et pro $y$, 2, 8 et 6, 7. Ita v. gr. sumto $x=5$, sumi poterit $y=6$; quia igitur $5^4=625$ et $6^4=1296$, erit $x^4+y^4=1921=17.113$.

II. Sit $\Delta=41=4^2+5^2$, eritque $a=4$ et $b=5$, ideoque $pp=41n\pm20$, ideoque $n=4$ et $p=12$. Jam $4:5=12:q$, ergo $q=15$. Hinc pro divisore 41 nostra tabula erit:

| $x$ | $y$ |
|---|---|
| 1, 9 | 3, 14 |
| 2, 18 | 6, 13 |
| 4, 5 | 12, 15 |
| 7, 19 | 16, 20 |
| 8, 10 | 11, 17 |

Ita sumto $x=1$ et $y=3$, erit $x^4+y^4=82=41.2$.

Simili modo tabulam construximus pro sequentibus

$\Delta = 73$

| $x$ | $y$ |
|---|---|
| 1, 27 | 10, 22 |
| 5, 11 | 23, 36 |
| 2, 19 | 20, 29 |
| 3, 8 | 30, 7 |
| 4, 35 | 33, 15 |
| 6, 16 | 13, 14 |
| 9, 24 | 17, 21 |
| 12, 32 | 26, 28 |
| 18, 25 | 34, 31 |

$\Delta = 89$

| $x$ | $y$ |
|---|---|
| 1, 34 | 12, 37 |
| 2, 21 | 15, 24 |
| 3, 13 | 22, 36 |
| 4, 42 | 30, 41 |
| 5, 8 | 7, 29 |
| 6, 26 | 17, 44 |
| 9, 39 | 19, 23 |
| 10, 16 | 14, 31 |
| 11, 18 | 38, 43 |
| 20, 32 | 27, 28 |
| 25, 40 | 33, 35 |

$\Delta = 97$

| $x$ | $y$ |
|---|---|
| 1, 22 | 33, 47 |
| 2, 44 | 3, 31 |
| 4, 9 | 6, 35 |
| 5, 13 | 29, 41 |
| 7, 40 | 37, 38 |
| 8, 18 | 12, 27 |
| 10, 26 | 15, 39 |
| 11, 48 | 25, 32 |
| 14, 17 | 21, 23 |
| 16, 36 | 24, 43 |
| 19, 30 | 20, 45 |
| 28, 34 | 42, 46 |

Sit $\Delta = 89$ sumto $x = 5$ et $y = 7$, erit $x^4 + y^4 = 3026 = 89 . 34$.

Cum hae tabulae facillime ex positione litterarum $a$, $b$, et $p$, $q$ construantur, istam positionem pro singulis divisoribus $\Delta$ hic apponamus:

| $\Delta$ | $a$, $b$ | $p$, $q$ | $\Delta$ | $a$, $b$ | $p$, $q$ | $\Delta$ | $a$, $b$ | $p$, $q$ | $\Delta$ | $a$, $b$ | $p$, $q$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 17 | 1, 4 | 2, 8 | 193 | 7, 12 | 63, 85 | 353 | 8, 17 | 131, 146 | 569 | 13, 20 | 150, 187 |
| 41 | 4, 5 | 12, 15 | 233 | 8, 13 | 77, 96 | 401 | 1, 20 | 45, 98 | 577 | 1, 24 | 152, 186 |
| 73 | 3, 8 | 7, 30 | 241 | 4, 15 | 32, 120 | 409 | 3, 20 | 39, 198 | 593 | 8, 23 | 121, 171 |
| 89 | 5, 8 | 7, 29 | 257 | 1, 16 | 4, 64 | 433 | 12, 17 | 44, 82 | 601 | 5, 24 | 214, 295 |
| 97 | 4, 9 | 6, 35 | 281 | 5, 16 | 19, 117 | 449 | 7, 20 | 44, 195 | 617 | 16, 19 | 173, 244 |
| 113 | 7, 8 | 13, 31 | 313 | 12, 13 | 16, 65 | 457 | 4, 21 | 86, 223 | 641 | 4, 25 | 10, 258 |
| 137 | 4, 11 | 27, 40 | 337 | 9, 16 | 12, 91 | 521 | 11, 20 | 48, 182 | 673 | 12, 23 | 95, 126 |

Hic igitur praecipuum negotium in inventione quadrati $pp = n\Delta \pm ab$ consistit, quod autem sequenti modo haud difficulter praestabitur. Cum enim semper dentur numeri $p$ et $q$, minores quam $\frac{1}{2}\Delta$, eorum complementa etiam erunt $< \Delta$, semper ergo dantur quatuor tales numeri minores quam $\Delta$, quorum duo erunt pares et duo impares, atque cognito uno, reliqui tres facile inveniuntur.

Quaeramus igitur numerum imparem pro $p$ et cum sit $pp = n\Delta \pm ab$, tum vero $pp < \Delta\Delta$, singulos numeros $n$ tentando non ultra $n = \Delta$ progredi opus est. Deinde, quia $\Delta = aa + bb = 8m + 1$, numerorum $a$ et $b$ alter erit pariter par, alter vero impar, unde productum $ab$ habebit vel formam $8i + 4$, vel $8i$. Pro priore casu, quo $ab = 8i + 4$, quia $\Delta$ est $8\alpha + 1$, quadrata autem imparia formam habent $8i + 1$, ut talis forma oriatur, sumi debet $n = 5$, vel $n = 8\alpha + 5$, sicque casuum examinandorum numerus octies erit minor. Pro altero casu, quo $ab = 8m$, numeri pro $n$ sumendi erunt 1, 9, 17 ... $8i + 1$. Inter hos autem numeri etiam statim excludi possunt ii, qui desinunt in 3 vel 7, tum etiam ii, qui sunt formae $3i - 1$. Praeterea vero etiam ipsam formam $pp = n\Delta \pm ab$ in alias similes transformare licet. Si enim fuerit $ab + \alpha\Delta = ffA$, erit $pp = ff(n\Delta \pm A)$; tum vero si fuerit $\alpha\Delta + A = ggB$, erit etiam $pp = ffgg(n\Delta \pm B)$ et ita porro. Inter quas plurimas formas plerumque casus sponte se produnt, quibus quadrata emergunt. Ex his autem egregia theoremata deduci possunt:

I. Si fuerit $\Delta = aa + bb = 8m + 1$, haec formula $n\Delta \pm ab$ semper quadratum reddi potest.

II. Si fuerit $\Delta = aa + bb = 8m + 5$, tum ista formula $n\Delta \pm ab$ nunquam quadratum fieri potest. Ita si $\Delta = 5$, ob $a = 2$ et $b = 1$, haec forma $5n \pm 2$ nunquam esse potest quadratum, quod per se constat.

Deinde sumto $a=2$, $b=3$ et $\Delta=13$, haec forma $13n\pm 6$ nunquam quadratum esse potest. Item si $\Delta=29$, ob $a=2$, $b=5$, haec forma $29m\pm 10$ nunquam fit quadratum.

Alia Solutio problematis praecedentis. Sit $8m+1=aa+bb=\Delta$ esseque oportet

$$x^4+y^4=(aa+bb)(pp+qq).$$

Jam sit proxime $\frac{a}{b}=\frac{\alpha}{\beta}$, ita ut sit $a\beta-b\alpha=\pm 1$. Sit nunc $x=c$ et sumatur $p=bf\Delta+\beta cc$ et $q=af\Delta+\alpha cc$, et cum sit $xx=ap-bq$ et $yy=aq+bp$, erit $x^4+y^4=(aa+bb)(pp+qq)$, erit itaque $xx=(a\beta-b\alpha)cc=cc$ at $yy=(aa+bb)f\Delta+(a\alpha+b\beta)cc$, quod ergo esse debet quadratum. Sit nunc $cc=n\Delta+d$, fiet $yy=i\Delta\pm(a\alpha+b\beta)d$.

Exemplum 1. Sit $aa+bb=41=\Delta$, erit $a=5$ et $b=4$, hinc $\frac{5}{4}=\frac{\alpha}{\beta}$, proxime hinc $\alpha=1$ et $\beta=1$. Sumatur porro $c=1$, eritque $d=1$, ergo $yy=41i\pm 9=\square$, unde sumto $i=0$, erit $y=3$ et $x=1$, eritque $x^4+y^4=82=2\cdot 41$.

Exemplum 2. Sit $\Delta=601$, erit $a=24$ et $b=5$, tum vero $\alpha=5$ et $\beta=1$. Sumto ergo $x=1$, erit $d=1$ et $yy=601i\pm 125$, hinc sumto $i=6$, erit $y=59$.

Jam $x$ pro lubitu sumi potest, verbi gr. $x=c$, erit $y=59c\pm 601i$, unde omnes valores redigi possunt infra 300.

A. m. T. III. p. 171—174.

---

## 12.

*De divisoribus primis formae* $a^4+2b^4$.

Primo patet hanc formam alios divisores habere non posse, nisi qui dividant formam $a^2+2b^2$, qui omnes continentur vel in hac forma $8n+1$, vel in hac $8n+3$. Ac primo quidem omnes numeri primi hujus formae $8n+3$ possunt esse divisores cujuspiam numeri formae $a^4+2b^4$. Longe secus autem res se habet de altera forma $8n+1$. Non enim omnes numeri primi in hac forma contenti divisores esse possunt formae $a^4+2b^4$, sed tantum sequentes: 73, 89, 113, 233, 257, 281, 337, 353, 577, etc. Hinc ergo excluduntur hi numeri ejusdem formae: 17, 41, 97, 137, 193, 241, 313, 401, 409, 433, 449, 457, 569, etc., neque tamen ulla ratio patet, qua has duas species numerorum formae $8n+1$ a se invicem distinguere liceat.

Ad divisores formae $a^4+2b^4$ supra allatos et in formula $8n+1$ contentos insuper accedunt 601 et 617. Est enim 601 divisor ipsius $14^4+2\cdot 5^4$ et 617 divisor ipsius $16^4+2\cdot 7^4$.

A. m. T. III. p. 181. 182.

---

## 13.

Problema. Invenire exponentem $e$, ut formula $a^e-b^e$ per datum numerum $\Delta$ fiat divisibilis, si quidem numeri $a$ et $b$ sint primi ad $\Delta$.

Solutio. Sint $p$, $q$, $r$, $s$ numeri primi, et considerentur sequentes casus

| | | | |
|---|---|---|---|
| si | $\Delta=p$, | erit | $e=p-1$ |
| « | $\Delta=p^2$ | « | $e=p(p-1)$ |
| « | $\Delta=p^3$ | « | $e=p^2(p-1)$ |
| . . . | . . . | . . . | . . . |
| « | $\Delta=p^n$ | « | $e=p^{n-1}(p-1)$ |
| « | $\Delta=pq$ | « | $e=(p-1)(q-1)$ |
| « | $\Delta=pqr$ | « | $e=(p-1)(q-1)(r-1)$ |
| « | $\Delta=p^\lambda q^\mu r^\nu$ | « | $e=p^{\lambda-1}(p-1)q^{\mu-1}(q-1)r^{\nu-1}(r-1)$. |

Corollarium 1. Hinc si loco $a$ scribatur $a^\alpha$ et $b^\beta$ loco $b$, etiam haec formula $a^{\alpha e}-b^{\beta e}$ erit per $\Delta$ divisibilis.

Corollarium 2. Hinc si exponens $e$ divisorem habeat $n$, ut sit $e=dn$, tum semper dari poterit forma $x^n-y^n$ per $\Delta$ divisibilis. Cum enim $a^{dn}-b^{dn}$ sit divisibilis, sumatur $x=a^d$ et $y=b^d$, vel etiam $x=a^d\pm\alpha\Delta$ et $y=b^d\pm\beta\Delta$, vel adhuc generalius $x=fa^d\pm\alpha\Delta$ et $y=fb^d\pm\beta\Delta$.

NB. In his formulis, ubi productum $(p-1)(q-1)(r-1)$ occurrit, sufficit ejus loco minimum commune dividuum numerorum $p-1$, $q-1$, $r-1$, scribere.

Quoniam formula $x^n-y^n$ praeter $x-y$ nullos habet divisores, nisi in forma $\lambda n+1$ contentos, sic casu $n=5$ formae $x^5-y^5$, praeter $x-y$, divisores sunt $5\lambda+1$ hoc est: 11, 31, 41, 61, 71, 101, 131, etc. Si ergo proponatur formula $x^5-1$, eaque casu $x=a$ divisorem habeat $5\lambda+1$, eundem divisorem habebit casibus $x=a^2$, $x=a^3$, $x=a^4$, etc., sicque ex uno casu reliqui omnes deduci possunt, cum sit

$$x=a^\mu\pm M(5\lambda+1),$$

unde sequens tabula est confecta:

| Div. pr. $p$. | Valores $x$ | generatim |
|---|---|---|
| 11 | $1-\ 2+\ 4+\ 3+\ 5+$ etc. | $(-2)^\mu\pm 11M$ |
| 31 | $1+\ 2+\ 4+\ 8+\ 16+$ etc. | $(+2)^\mu\pm 31M$ |
| 41 | $1-\ 4+\ 16+\ 18+\ 10+$ etc. | $(-4)^\mu\pm 41M$ |
| 61 | $1-\ 3+\ 9-\ 27+\ 20+$ etc. | $(-3)^\mu\pm 61M$ |
| 71 | $1+\ 5+\ 25-\ 17-\ 14+$ etc. | $(+5)^\mu\pm 71M$ |
| 101 | $1-\ 6+\ 36-\ 14-\ 17+$ etc. | $(-6)^\mu\pm 101M$ |
| 131 | $1+\ 53+\ 58+\ 61-\ 42+$ etc. | $(-42)^\mu\pm 131M$ |
| $(11^2)$ 121 | $1+\ 3+\ 9+\ 27+\ 81+$ etc. | $(+3)^\mu\pm 121M$ |
| $(11^3)$ 1331 | $1-161+632-596+124+$ etc. | $(+124)^\mu\pm 1331M$ |

minimus autem valor ipsius $x$ ex proprietate supra allata reperitur. Ita si divisor $=31$, quia $a^{30}-1$ divisorem habet 31, sumatur $x=a^6$, fiet $x^5-1$. Sumatur $a=2$, erit $x=64\pm 2.31$, unde minimus $=2$. Ita si $p=101$, quia $a^{100}-1$ divisibile per 101, sumatur $x^5=a^{100}$, sive $x=a^{20}\pm 101M$.

Ut formula $x^6+y^6$ divisibilis fiat per 37, numeri $x$ et $y$ ex sequenti schemate:

$$x\begin{cases}1, & 10, & 11\\ 2, & 17, & 15\\ 3, & 7, & 4\end{cases}\qquad y\begin{cases}8, & 6, & 14\\ 16, & 12, & 9\\ 13, & 18, & 5\end{cases}$$

scilicet ex eadem linea horizontali sumi debent.

At ut $x^6+y^6$ divisibile fiat per 61, $x$ et $y$ ex sequenti schemate sumuntur

$$x\begin{cases}1, & 13, & 14\\ 2, & 26, & 28\\ 4, & 9, & 5\\ 7, & 30, & 24\\ 8, & 18, & 10\end{cases}\qquad y\begin{cases}11, & 21, & 32\\ 22, & 19, & 3\\ 17, & 23, & 6\\ 16, & 25, & 20\\ 27, & 15, & 12\end{cases}$$

singulis autem his numeris adjici intelligenda est $\pm 61M$. Hinc casus simplicissimus est $2^6+3^6$. Singuli autem hi terniones in unica forma comprehendi possunt, quae simplicissima est $4n$, $5n$, $9n$, vel in hac $1n$, $13n$, $14n$.

Problema. Ut formula $x^6-1$ divisibilis fiat per divisorem idoneum $\Delta$, valores ipsius $x$ definire.

Solutio. Divisor $\Delta$ necessario debet contineri in hac formula $\Delta=\frac{a^3\pm 1}{a\pm 1}$, cujus factor quicunque dabit valorem idoneum pro $\Delta$; tum autem tres habebuntur valores principales pro $x$, qui sunt $1$, $\pm a$, $\pm aa$, quibus adjici potest $\pm M\Delta$. Ita si sumatur $a=2$, erit $\Delta=\frac{8\pm 1}{2\pm 1}$, ideoque vel $\Delta=3$, vel $\Delta=7$, et tum erit $x=1, 2, 4$. Si $a=3$, erit $\Delta=\frac{27\pm 1}{3\pm 1}$, ideoque vel $\Delta=7$, vel $\Delta=13$, eritque $x=1, 3, 9$. Si $a=4$, erit $\Delta=\frac{64\pm 1}{4\pm 1}$

ideoque vel $\Delta = 13$, vel $\Delta = 21 = 3.7$, tum $x = 1, 4, 16$. Si $a = 5$, erit $\Delta = \frac{125 \pm 1}{5 \pm 1}$; ideoque $\Delta = 21$, vel $\Delta = 31$, $x = 1, 5, 25$, etc.

Problema. Ut formula $x^{10} - 1$ divisibilis fiat per $\Delta$, valores ipsius $x$ assignare.

Solutio. Hic debet esse $\Delta = \frac{a^5 \pm 1}{a \pm 1}$, ac tum quinque habentur valores principales pro $x$, scilicet $1, a, aa, a^3, a^4$, quibus adjici potest $M\Delta$. Sic sumto $a = 2$, erit $\Delta = \frac{32 \pm 1}{2 \pm 1}$, vel $\Delta = 11$, vel $\Delta = 31$, eritque $x = 1, 2, 4, 8, 16$. Si $a = 3$, erit $\Delta = \frac{243 \pm 1}{3 \pm 1}$, ideoque vel $\Delta = 61$, vel $\Delta = 121$, hinc $x = 1, 3, 9, 27, 81$. Si $a = 4$, erit $\Delta = \frac{1024 \pm 1}{4 \pm 1}$, vel $\Delta = 205$, vel $\Delta = 341 = 11.31$ et $x = 1, 4, 16, 64, 256$. Si $a = 5$, erit $\Delta = \frac{3125 \pm 1}{5 \pm 1}$, ideoque vel $\Delta = 521$, vel $\Delta = 781 = 11.71$, $x = 1, 5, 25, 125, 625$, etc.

NB. Omnes divisores primi hic sunt formae $10n + 1$. Dato ergo tali divisore, veluti 131, quaeri debet numerus $a$, ut $a^5 \pm 1$ divisionem admittat per 131, quod hoc casu non evenit, nisi sumatur vel $a = 42$, vel $a = 53$, vel $a = 58$, vel $a = 70$; tum enim habebitur $x = 1, 42, 70, 58, 53$.

Quando autem divisor $\Delta$ datur, in forma $10n + 1$ contentus, valor litterae $a$ hoc modo eruetur. Cum $\Delta$ debeat esse divisor formae $a^5 - 1$, capiatur $a = b^n$, erit $a^5 = b^{5n}$, semper autem est $b^{10n} - 1$ divisibile per $10n + 1$, ideoque vel $b^{5n} + 1$, vel $b^{5n} - 1$, quocirca sumi debet $a = b^n$. Ita pro casu $\Delta = 131$ est $n = 13$, ideoque $a = b^{13}$; sumto ergo $b = 2$, erit $b^{13} = 8192$, quod divisum per 131 relinquit 61, et valores ipsius $x$ erunt $1, 61, 61^2, 61^3, 61^4$. Est vero $61^2 = 3721$, quod dat 53, et $61.53$ dat 42, et $61.42$ dat 58. Sicque $x = 1, 61, 53, 42, 58$. Eodem modo si proponatur $\Delta = 151$, erit $n = 15$ et $a = 19$; $a^2 = 59$, $a^3 = 64$, $a^4 = 8$.

Ut formula $x^8 + y^8$ divisibilis fiat per 97, numeri $x$ et $y$ ex sequenti tabula desumantur

| $x$ | | | | $y$ | | | |
|---|---|---|---|---|---|---|---|
| 1, | 33, | 22, | 47 | 8, | 27, | 18, | 12 |
| 2, | 31, | 44, | 3 | 16, | 43, | 36, | 24 |
| 4, | 35, | 9, | 6 | 32, | 11, | 25, | 48 |
| 5, | 29, | 13, | 41 | 40, | 38, | 7, | 37 |
| 10, | 39, | 26, | 15 | 17, | 21, | 14, | 23 |
| 46, | 13, | 42, | 28 | 29, | 19, | 45, | 30 |

ita casus simplicissimus est $5^8 + 7^8$.

Ut formula $x^{10} - 1$ dividi queat per $11^3$, valores ipsius $x$ erunt

$$1, \quad 124, \quad 596, \quad 699, \quad 161.$$

Cum enim $3^5 - 1 = 2.11^2$, ponatur $z = 3 + 11^2 y$, eritque $z^5 - 1 = 2.11^2 + 5.3^4.11^2 y +$ etc. quod divisum per $11^2$ dat $\frac{z^5 - 1}{11^2} = 2 + 5.3^4 y +$ etc. Tantum ergo $y$ ita sumatur, ut $2 + 5.81y$ divisibile sit per 11, sive $2 - 2y$, vel $1 - y$. Sumatur $y = -10$, erit $z = 1207 = 124$.

A. m. T. II. p. 162—164.

## c) *De numeris formae* $x^p \pm 1$.

### 14.

(*Lexell.*)

Problema. Invenire numerum formae $2^n + 1$, qui habeat datum divisorem.

Solutio. Divisor repraesentetur per simplices potestates binarii, et quotus quaeratur sequenti modo per partes; ubi tenendum est, quoniam tandem omnes minores potestates binarii in producto excludi debent, si ex aliquot partibus quoti prodierit productum $1 + 2^\alpha +$ etc. tum sequentem quoti partem esse debere $2^\alpha$, deinde tantum notetur esse $2^\alpha + 2^\alpha = 2^{\alpha+1}$.

EXEMPLUM I. Sit divisor $=1+2^7+2^9$, ac prima pars quoti erit 1, et operatio sequenti modo instituetur

| Partes quoti | Productum |
|---|---|
| $1$ | $1+{}_*2^{7}+{}_*2^{9}$ |
| $2^{7}$ | ${}_*2^{7}+{}_*2^{14}+{}_*2^{16}+{}_*2^{8}$ |
| $2^{8}$ | ${}_*2^{8}+{}_*2^{15}+{}_*2^{17}+{}_*2^{10}$ |
| $2^{10}$ | ${}_*2^{10}+{}_*2^{17}+{}_*2^{19}+{}_*2^{11}+{}_*2^{15}$ |
| $2^{11}$ | ${}_*2^{11}+{}_*2^{15}+{}_*2^{20}+{}_*2^{12}+{}_*2^{21}$ |
| $2^{12}$ | ${}_*2^{12}+{}_*2^{19}+{}_*2^{21}+{}_*2^{13}+{}_*2^{22}$ |
| $2^{13}$ | ${}_*2^{13}+{}_*2^{20}+{}_*2^{22}+{}_*2^{17}+{}_*2^{23}$ |
| $2^{17}$ | ${}_*2^{17}+{}_*2^{24}+{}_*2^{26}+{}_*2^{18}$ |
| $2^{18}$ | ${}_*2^{18}+{}_*2^{25}+{}_*2^{27}+{}_*2^{21}$ |
| $2^{21}$ | ${}_*2^{21}+{}_*2^{28}+{}_*2^{30}+{}_*2^{22}$ |
| $2^{22}$ | ${}_*2^{22}+{}_*2^{29}+{}_*2^{31}+2^{32}$ |

ergo forma est $2^{32}+1$, cujus divisor est $1+2^7+2^9=641$ et

quotus $=1+2^7+2^8+2^{10}+2^{11}+2^{12}+2^{13}+2^{17}+2^{18}+2^{21}+2^{22}$.

EXEMPLUM II. Sit divisor $73=1+2^3+2^6$.

| Partes quoti | Productum |
|---|---|
| $1$ | $1+{}_*2^{3}+{}_*2^{6}$ |
| $2^{3}$ | ${}_*2^{3}+{}_*2^{6}+{}_*2^{9}+{}_*2^{4}+{}_*2^{7}$ |
| $2^{4}$ | ${}_*2^{4}+{}_*2^{7}+{}_*2^{10}+{}_*2^{5}+{}_*2^{8}$ |
| $2^{5}$ | ${}_*2^{5}+{}_*2^{8}+{}_*2^{11}+{}_*2^{6}+{}_*2^{9}+{}_*2^{10}+{}_*2^{11}+{}_*2^{12}$ |
| $2^{6}$ | ${}_*2^{6}+{}_*2^{9}+{}_*2^{12}+{}_*2^{7}+{}_*2^{13}$ |
| $2^{7}$ | ${}_*2^{7}+{}_*2^{10}+{}_*2^{13}+{}_*2^{8}+{}_*2^{14}$ |
| $2^{8}$ | ${}_*2^{8}+{}_*2^{11}+{}_*2^{14}+{}_*2^{9}+{}_*2^{10}+{}_*2^{11}+{}_*2^{12}+{}_*2^{15}$ |
| $2^{12}$ | ${}_*2^{12}+{}_*2^{15}+{}_*2^{18}+{}_*2^{13}+{}_*2^{16}$ |
| $2^{13}$ | ${}_*2^{13}+{}_*2^{16}+{}_*2^{19}+{}_*2^{14}+{}_*2^{17}$ |
| $2^{14}$ | ${}_*2^{14}+{}_*2^{17}+{}_*2^{20}+{}_*2^{15}+{}_*2^{18}+{}_*2^{19}+{}_*2^{20}+{}_*2^{21}$ |
| $2^{15}$ | ${}_*2^{15}+{}_*2^{18}+{}_*2^{21}+{}_*2^{16}+{}_*2^{22}$ |
| $2^{16}$ | ${}_*2^{16}+{}_*2^{19}+{}_*2^{22}+{}_*2^{17}+{}_*2^{23}$ |
| $2^{17}$ | ${}_*2^{17}+{}_*2^{20}+{}_*2^{23}+{}_*2^{18}+{}_*2^{19}+{}_*2^{20}+{}_*2^{21}+{}_*2^{24}$ |
| $2^{21}$ | ${}_*2^{21}+{}_*2^{24}+{}_*2^{27}+{}_*2^{22}+{}_*2^{25}$ |
| $2^{22}$ | ${}_*2^{22}+{}_*2^{25}+{}_*2^{28}+{}_*2^{23}+{}_*2^{26}$ |
| $2^{23}$ | ${}_*2^{23}+{}_*2^{26}+{}_*2^{29}+{}_*2^{24}+{}_*2^{27}+{}_*2^{28}+{}_*2^{29}+{}_*2^{30}$ |
| $2^{24}$ | ${}_*2^{24}+{}_*2^{27}+{}_*2^{30}+{}_*2^{25}+{}_*2^{31}$ |
| $2^{25}$ | ${}_*2^{25}+{}_*2^{28}+{}_*2^{31}+{}_*2^{26}+{}_*2^{32}$ |
| $2^{26}$ | ${}_*2^{26}+{}_*2^{29}+{}_*2^{32}+{}_*2^{27}+{}_*2^{28}+{}_*2^{29}+{}_*2^{30}+{}_*2^{33}$ |
| $2^{30}$ | ${}_*2^{30}+{}_*2^{33}+2^{36}+2^{31}+2^{34}$ |

Plane non datur talis forma per 73 divisibilis.

EXEMPLUM III. Sit divisor $41=1+2^3+2^5$, erunt

| partes quoti | productum |
|---|---|
| $1$ | $1+{}_*2^{3}+{}_*2^{5}$ |
| $2^{3}$ | ${}_*2^{3}+{}_*2^{6}+{}_*2^{8}+{}_*2^{4}$ |
| $2^{4}$ | ${}_*2^{4}+{}_*2^{7}+{}_*2^{9}+{}_*2^{5}+{}_*2^{6}+{}_*2^{7}+{}_*2^{8}+{}_*2^{9}+2^{10}$ |

ergo forma $1+2^{10}$ divisibilis est per 41 et quotus erit $1+2^3+2^4=25$.

Exemplum IV. Sit divisor $11 = 1 + 2^1 + 2^3$, erunt

| partes quoti | productum |
|---|---|
| $1$ | $1 + {}_*2^1 + {}_*2^3$ |
| $2^1$ | ${}_*2^1 + {}_*2^2 + {}_*2^4 + {}_*2^2 + {}_*2^3 + {}_*2^4 + 2^5$ |

unde $1 + 2^5 = 11\,(1 + 2)$.

Exemplum V. Sit divisor $13 = 1 + 2^2 + 2^3$, erunt

| partes quoti | productum |
|---|---|
| $1$ | $1 + {}_*2^2 + {}_*2^3$ |
| $2^2$ | ${}_*2^2 + {}_*2^4 + {}_*2^5 + {}_*2^3 + {}_*2^4 + {}_*2^5 + 2^6$ |

unde $2^6 + 1 = 13\,(1 + 2^2)$.

Exemplum VI. Sit divisor $7 = 1 + 2 + 2^2$, erunt

| partes quoti | productum |
|---|---|
| $1$ | $1 + {}_*2 + {}_*2^2$ |
| $2^1$ | ${}_*2 + {}_*2^2 + {}_*2^3 + {}_*2^2 + {}_*2^3 + {}_*2^4$ |
| $2^2$ | ${}_*2^2 + {}_*2^3 + {}_*2^4 + {}_*2^3 + {}_*2^4 + {}_*2^5$ |
| $2^4$ | ${}_*2^4 + {}_*2^5 + {}_*2^6 + {}_*2^5 + {}_*2^6 + {}_*2^7$ |
| $2^5$ | ${}_*2^5 + {}_*2^6 + {}_*2^7 + {}_*2^6 + {}_*2^7 + {}_*2^8$ |
| $2^7$ | ${}_*2^7 + {}_*2^8 + {}_*2^9 + {}_*2^8 + {}_*2^9 + {}_*2^{10}$ |
| $2^8$ | ${}_*2^8 + {}_*2^9 + {}_*2^{10} + {}_*2^9 + 2^{10} + 2^{11}$ |
| $2^{10}$ | etc. |

Pro hoc ergo divisore non datur forma binomialis $1 + 2^n$; dantur autem trinomiales:

$1 + 2 + 2^2$, $1 + 2^2 + 2^4$, $1 + 2^4 + 2^5$, $1 + 2^5 + 2^7$, $1 + 2^7 + 2^8$, $1 + 2^8 + 2^{10}$, $1 + 2^{10} + 2^{11}$.

(*Krafft.*)

Problema. Invenire numerum formae $2^n - 1$, qui habeat datum divisorem.

Solutio. Primo notetur esse

$$2^n - 1 = 1 + 2 + 2^2 + 2^3 + 2^4 + \ldots 2^{n-1},$$

sicque omnes potestates ab unitate usque ad maximam occurrere debent. Si igitur, ut ante, quotus per partes quaeratur; in producto ex aliquot partibus orto notetur minima potestas, quae adhuc deficit, eaque ipsa erit nova pars quoti.

Exemplum I. Sit divisor $23 = 1 + 2 + 2^2 + 2^4$, erunt

| partes quoti | productum |
|---|---|
| $1$ | $1 + 2 + 2^2 + {}_*2^4$ |
| $2^3$ | $2^3 + {}_*2^4 + {}_*2^5 + {}_*2^7 + {}_*2^5 + {}_*2^6$ |
| $2^4$ | $2^4 + 2^5 + {}_*2^6 + {}_*2^8 + {}_*2^7 + {}_*2^8 + 2^9$ |
| $2^6$ | $2^6 + 2^7 + 2^8 + 2^{10}$ |

unde erit $n = 11$ sicque $2^{11} - 1$ divisibile est per 23 quoto existente

$$1 + 2^3 + 2^4 + 2^6 = 89.$$

*Nota.* Forma numerorum perfectorum est $2^{n-1}(2^n - 1)$, quoties fuerit factor posterior $2^n - 1$ numerus primus.

Exemplum II. Sit divisor $47 = 1 + 2 + 2^2 + 2^3 + 2^5$, erunt

| partes quoti | productum |
|---|---|
| $1$ | $1+2+2^2+{}_*2^3+2^5$ |
| $2^4$ | $2^4+{}_*2^5+{}_*2^6+{}_*2^7+{}_*2^9+{}_*2^6+{}_*2^7+{}_*2^8$ |
| $2^5$ | $2^5+2^6+2^7+{}_*2^8+{}_*2^{10}+{}_*2^9+{}_*2^{10}+{}_*2^{11}$ |
| $2^8$ | $2^8+2^9+{}_*2^{10}+{}_*2^{11}+{}_*2^{13}+{}_*2^{12}$ |
| $2^{11}$ | $2^{11}+{}_*2^{12}+{}_*2^{13}+{}_*2^{14}+{}_*2^{16}+{}_*2^{13}+{}_*2^{14}+{}_*2^{15}$ |
| $2^{12}$ | $2^{12}+{}_*2^{13}+{}_*2^{14}+{}_*2^{15}+{}_*2^{17}+{}_*2^{14}+{}_*2^{15}+{}_*2^{16}+{}_*2^{17}+{}_*2^{18}$ |
| $2^{13}$ | $2^{13}+2^{14}+{}_*2^{15}+{}_*2^{16}+{}_*2^{18}+{}_*2^{16}+{}_*2^{17}+{}_*2^{19}$ |
| $2^{15}$ | $2^{15}+2^{16}+{}_*2^{17}+{}_*2^{18}+{}_*2^{20}+{}_*2^{18}+{}_*2^{19}+{}_*2^{20}+2^{21}$ |
| $2^{17}$ | $2^{17}+2^{18}+2^{19}+2^{20}+2^{22}$ |

ergo $n=23$ et $2^{23}-1$ divisibile est per 47, quoto existente

$$2^{17}+2^{15}+2^{13}+2^{12}+2^{11}+2^8+2^5+2^4+1=178481.$$

*(Lexell.)*

Verum haec omnia multo facilius atque adeo multo generalius per sequentem methodum expediri possunt.

Problema. Invenire exponentem $x$, ut formula $2^x-a$ datum habeat divisorem $=p$.

Solutio. Quaeritur ergo potestas binarii $2^x$, quae per numerum $p$ divisa relinquat residuum $=a$; notetur autem pro residuo $a$ in genere scribi posse $a+\lambda p$, loco $a$ igitur sumatur $a\pm p$, qui numerus cum sit par ac fortasse per majorem binarii potestatem divisibilis, ponatur $a\pm p=2^\alpha b$, atque potestas $2^{x-\alpha}$ dabit residuum $b$, cujus loco sumatur iterum $b\pm p$, quod sit $=2^\beta c$, sicque potestas $2^{x-\alpha-\beta}$ residuum dabit $c$, sive $c\pm p$ quod sit $=2^\gamma d$, sicque potestas $2^{x-\alpha-\beta-\gamma}$ residuum dabit $d$, atque hoc modo eo usque procedatur, donec ad residuum perveniatur $=1$, quod cum sit residuum potestatis $2^0$, evidens est ultimum exponentem

$$x-\alpha-\beta-\gamma-\delta-\text{etc. esse debere}=0,$$

consequenter habebitur

$$x=\alpha+\beta+\gamma+\delta+\text{etc.}$$

Tota haec operatio sequenti modo commode disponetur: Pro divisore $=p$:

| potestates | residua | sive |
|---|---|---|
| $2^x$ | $a$ | $a\pm p=2^\alpha b$ |
| $2^{x-\alpha}$ | $b$ | $b\pm p=2^\beta c$ |
| $2^{x-\alpha-\beta}$ | $c$ | $c\pm p=2^\gamma d$ |
| $2^{x-\alpha-\beta-\gamma}$ | $d$ | $d\pm p=2^\delta e$ |
| . | . | . |
| . | . | . |
| . | . | . |
| $2^{x-\alpha-\beta-\gamma-\delta-\cdots}$ | $+1$ | $x=\alpha+\beta+\gamma+\delta+\text{etc.}$ |

Exemplum I. Quaeratur formula $2^x+1$, quae divisorem habeat 641. Pro hoc divisore

| potestates | residua | sive |
|---|---|---|
| $2^x$ | $a=-1$ | $640=128.5=2^7.5$ |
| $2^{x-7}$ | $5$ | $-636=-2^2.159$ |
| $2^{x-9}$ | $-159$ | $-800=-2^5.25$ |
| $2^{x-14}$ | $-25$ | $+616=+2^3.77$ |
| $2^{x-17}$ | $+77$ | $-564=-2^2.141$ |
| $2^{x-19}$ | $-141$ | $+500=+2^2.125$ |
| $2^{x-21}$ | $+125$ | $-516=-2^2.129$ |
| $2^{x-23}$ | $-129$ | $512=+2^9.1$ |
| $2^{x-32}$ | $1$ | ergo $x=32$ |

Exemplum II. Quaerere formulam $2^x+1$, quae divisorem habeat 29. Pro hoc divisore

| potestates | residua | sive |
|---|---|---|
| $2^x$ | $-1$ | $-1+29=28=2^2.7$ |
| $2^{x-2}$ | $7$ | $+36=2^2.9$ |
| $2^{x-4}$ | $9$ | $-20=-2^2.5$ |
| $2^{x-6}$ | $-5$ | $24=2^3.3$ |
| $2^{x-9}$ | $3$ | $32=2^5.1$ |
| $2^{x-14}$ | $1$ | $x=14.$ |

Exemplum III. Quaerere formulam $2^x+1$, quae divisorem habeat 73. Pro divisore 73

| potestates | residua | sive |
|---|---|---|
| $2^x$ | $-1$ | $2^3.9$ |
| $2^{x-3}$ | $+9$ | $-64=-2^6.1$ |
| $2^{x-9}$ | $-1$ | $72=2^3.9$ |
| $2^{x-12}$ | $9$ | $-64=-2^6.1$ |
| $2^{x-18}$ | $-1$ | |

unde apparet hanc quaestionem esse impossibilem.

Exemplum IV. Quaerere formulam $2^x-1$, quae habeat divisorem 23:

| potestates | residua | sive |
|---|---|---|
| $2^x$ | $1$ | $24=2^3.3$ |
| $2^{x-3}$ | $3$ | $-20=-2^2.5$ |
| $2^{x-5}$ | $-5$ | $-28=-2^2.7$ |
| $2^{x-7}$ | $-7$ | $16=2^4.1$ |
| $2^{x-11}$ | $1$ | ergo $x=11.$ |

Exemplum V. Quaerere formam $2^x-3$, quae habeat divisorem 19:

| potestates | residua | sive |
|---|---|---|
| $2^x$ | $3$ | $-16=-2^4.1$ |
| $2^{x-4}$ | $-1$ | $-20=-2^2.5$ |
| $2^{x-6}$ | $-5$ | $-24=-2^3.3$ |
| $2^{x-9}$ | $-3$ | $16=2^4.1$ |
| $2^{x-13}$ | $1$ | $x=13.$ |

Problema generalius. Invenire exponentem $x$, ut formula $AR^x-a$ datum habeat divisorem $=p$.

Solutio. Numerus ergo $AR^x$ residuum dare debet $=a$, cui aequivalet $a\pm\lambda p=R^\alpha b$, unde numerus $AR^{x-\alpha}$ residuum dare debet $b$, sive $b\pm\lambda p=R^\beta c$, sicque numerus $AR^{x-\alpha-\beta}$ producet numerum $c$, sicque hoc modo procedendo, donec perveniatur ad numerum $A$, quod quia nascitur ex $AR^0$, manifestum est esse debere

$$x=\alpha+\beta+\gamma+\delta+\text{etc.}$$

Exemplum. Quaerere formulam $5^x-1$, quae divisorem habeat 17.

| potestates | residua | sive | potestates | residua | sive |
|---|---|---|---|---|---|
| $5^x$ | $1$ | $35=5.7$ | $5^{x-5}$ | $-6$ | $-40=-5.8$ |
| $5^{x-1}$ | $7$ | $-10=-5.2$ | $5^{x-6}$ | $-8$ | $-25=-5^2$ |
| $5^{x-2}$ | $-2$ | $15=5.3$ | $5^{x-8}$ | $-1$ | |
| $5^{x-3}$ | $3$ | $20=5.4$ | $5^{x-16}$ | $1$ | $x=16$ |
| $5^{x-4}$ | $4$ | $-30=-5.6$ | | | |

Problema. Invenire exponentem $x$, ut formula $2^{2x}+2^x+1$ datum habeat divisorem $p$.

Solutio. Cum ergo formula $2^{2x}+2^x$ residuum habere debeat $-1$, sive $-1+\lambda p$, ponamus potestatem $2^x$ habere residuum $r$, atque ejus quadratum $2^{2x}$ residuum habebit $rr$, ideoque illius formae residuum erit $rr+r$. Quaeratur ergo $r$, ut fiat

$$rr+r=-1+\lambda p,\quad \text{sive}\quad 4rr+4r+1=(2r+1)^2=4\lambda p-3,\quad \text{unde}\quad 2r+1=\sqrt{(4\lambda p-3)};$$

$\lambda$ igitur ita sumi debet, ut $4\lambda p-3$ sit quadratum. Invento autem $r$ quaeratur potestas $2^x$ residuum habens $r$, quod est problema superius.

Sit verbi gratia divisor $p=19$ et quadratum esse debet $76\lambda-3$, quod fit si $\lambda=3$, ergo $2r+1=\pm15$, consequenter vel $r=+7$, vel $r=-8$.

| | | | |
|---|---|---|---|
| I. Pro $r=+7$ | $2^x$ | resid. $+7$ | $-12=-2^2.3$ |
| | $2^{x-2}$ | $-3$ | $16=2^4$ |
| | $2^{x-6}$ | $1$ | hinc $x=6$ |

ideoque $2^{12}+2^6+1$ divisibile per 19.

| | | | |
|---|---|---|---|
| II. Pro $r=-8$ | $2^x$ | resid. $-8$ | $-2^3.1$ |
| | $2^{x-3}$ | $-1$ | $-20=-2^2.5$ |
| | $2^{x-5}$ | $-5$ | $-24=-2^3.3$ |
| | $2^{x-8}$ | $-3$ | $16=2^4$ |
| | $2^{x-12}$ | $1$ | $x=12$ |

ideoque $2^{24}+2^{12}+1$ divisibile per 19.

A. m. T. I. p. 143—149.

## 15.

(*J. A. Euler.*)

Cum sit $a^{2p}-1$ divisibile per $2p+1$, si $2p+1$ fuerit numerus primus, tum vel $a^p-1$, vel $a^p+1$ per eum dividi poterit. Duplicis ergo generis sunt potestates $a^p$, prouti vel formula $a^p-1$, vel $a^p+1$ fuerit divisibilis per $2p+1$.

Theorema. Cujus generis fuerit potestas $a^p$ ejusdem generis quoque erunt omnes istae

$$a^{2a+p},\quad a^{4a+p},\quad a^{6a+p}\quad \text{et in genere}\quad a^{2na+p},$$

ubi $a$ debet esse primus ad $2p+1$ et $n$ quoque potest esse numerus negativus.

Praeterea vero etiam ejusdem generis erunt hae potestates

$$a^{2a-p-1},\quad a^{4a-p-1},\quad a^{6a-p-1}\quad \text{et in genere}\quad a^{2na-p-1}$$

hoc autem posterius tantum valet, si $a$ fuerit numerus positivus; si enim sit negativus, hae posteriores potestates ad alterum genus pertinent. Ratio hujus exceptionis manifesta est: si enim $p$ fuerit numerus par, perinde est sive capiatur $+a$, sive $-a$; sin autem $p$ sit impar, loco $a$ sumendo $-a$, ipsa potestas fit negativa. Sicque si formula $(+a)^p\pm1$ fuerit per $2p+1$ divisibilis, tum $(-a)^p\mp1$ divisibilis erit.

Exemplum. Quia $2^1+1$ per $2.1+1=3$ est divisibile, ubi $a=2$ et $p=1$, ad idem genus pertinebunt hae potestates

$$2^1,\ 2^5,\ 2^9,\ 2^{13},\ 2^{17},\ 2^{21}\ \ldots\ 2^{4n+1}$$

deinde etiam istae

$$2^2,\ 2^6,\ 2^{10},\ 2^{14},\ 2^{18},\ 2^{22}\ \ldots\ 2^{4n+2}.$$

Examinemus casum $2^{21}$, an $2^{21}+1$ divisibile sit per 43, sive an $2^{21}$ per 43 divisum relinquat $-1$, quod ope methodi supra expositae ita fiet:

| divisor: 43 | residua |
|---|---|
| $2^{21}$ | $-1-43=-44=-2^2.11$ |
| $2^{21-2}$ | $-11+43=32=2^5.1$ |
| $2^{21-7}$ | 1. Capiatur cubus |
| $2^{3.21-21}$ | 1. At |
| $2^{2.21}$ | 1. Dividatur |
| $2^{21-21}$ | 1, vel |
| $2^0$ | 1 |

quod cum sit verum, etiam prima formula est vera.

Examinetur jam potestas $2^{18}$, num per 37 divisa relinquat $-1$. Calculus ita fiet

| divisor: 37 | residua |
|---|---|
| $2^{18}$ | $-1+37=2^2.9$ |
| $2^{18-2}$ | $+9-37=-2^2.7$ |
| $2^{18-4}$ | $-7-37=-2^2.11$ |
| $2^{18-6}$ | $-11$ |
| $2^{2.18}$ | $-1331=+1$, quod etiam est verum. |

Exemplum. Sit $a=3$ et $p=2$, erit $3^2+1$ divisibile per 5; hujus ergo generis erunt omnes hae potestates:

$$3^2,\ 3^8,\ 3^{14},\ 3^{20},\ 3^{26}\ldots\ 3^{6n+2},\ \text{item hae}$$

$$3^3,\ 3^9,\ 3^{15},\ 3^{21},\ 3^{27}\ldots\ 3^{6n+3}.$$

Examinetur $3^{26}$ an per 53 divisa relinquat $-1$:

| divisor: 53 | residua |
|---|---|
| $3^{26}$ | $+1+53=3^3.2$ |
| $3^{23}$ | $+2$ |
| $3^{46-26}$ vel $3^{20}$ | $+4$ |
| $3^{43-26}$ vel $3^{17}$ | $+8$ |
| $3^{14}$ | $+16$ |
| $3^5$ | $+128$ vel 22 |
| $3^2$ | 44 vel $-9$, |

quod cum sit falsum, residuum non erit $+1$ vel $-1$.

Examinetur $3^{33}$ an per 67 divisa relinquat $+1$.

| divisor: 67 | residua |
|---|---|
| $3^{33}$ | $1+134=3^3.5$ |
| $3^{30}$ | 5 |
| $3^{27}$ | 25 |
| $3^{24}$ | 125 vel $-9$ |
| $3^{18}$ | $-225$ vel $-24$ |
| $3^9$ | $+216$ vel $+15$ |
| $3^{33}$ vel $3^0$ | $-135$ vel $-1$ |

quod quia est falsum, nostra regula confirmatur.

Exemplum. Sit $a=6$ et fieri nequit $p=1$, quia neque $6^1+1$, neque $6^1-1$ per 3 est divisibile, ideoque excluduntur exponentes 1, 13, 25, 37, 49, etc., tum etiam

10, 22, 34, 46, 58, etc.

At $6^2-1$ est per 5 divisibile, sive $6^2$ per 5 divisum dat residuum $+1$, ergo $p=2$, et idem dabunt hae potestates

$6^{14}$, $6^{26}$, $6^{38}$, $6^{50}$, $6^{62}$, etc., tum etiam

$6^{9}$, $6^{21}$, $6^{33}$, $6^{45}$, $6^{57}$, etc.

Examinemus potestatem $6^{50}$ num per 101 divisa relinquat $+1$:

| divisor: 101 | residua |
|---|---|
| $6^{50}$ | $+1+101=102=6.17$ |
| $6^{49}$ | $17-101=-6.14$ |
| $6^{48}$ | $-14-202=-216=-6^3$ |
| $6^{45}$ | $-1$ |
| $6^{5}$ | $=1-101=-6.17$ |
| $6^{4}$ | $-17$ |
| $6^{3}$ | $+14$ |
| $6^{1}$ | $-196+202=+6$ |

quod quia est verum, patet regula.

Examinetur potestas $6^{33}$ an per 67 divisa relinquat $+1$:

| divisor: 67 | residua |
|---|---|
| $6^{33}$ | $+1-67=-6.11$ |
| $6^{32}$ | $-11-67=-6.13$ |
| $6^{31}$ | $-13+67=+6.9$ |
| $6^{30}$ | $+9$ |
| $6^{27}$ | $+81$ vel $+14$ |
| $6^{21}$ | $+196$ vel $-5$ |
| $6^{9}$ | $+25$ |
| $6^{3}$ | $+350$ vel $15$ |
| $6^{0}$ | $+135-134$ vel $+1$ |

---

Utra formula $a^p\pm1$ per numerum primum $2p+1$ sit divisibilis sequens tabella ostendit:

| $2p+1$ *pro* $a=2$ | | $2p+1$ *pro* $a=3$ | | $2p+1$ *pro* $a=5$ | | $2p+1$ *pro* $a=6$ | |
|---|---|---|---|---|---|---|---|
| $8n\pm1$ | $2^p-1$ | $12n\pm1$ | $3^p-1$ | $20n\pm1$ | $5^p-1$ | $24n\pm1$ | $6^p-1$ |
| $8n\pm3$ | $2^p+1$ | $12n\pm5$ | $3^p+1$ | $20n\pm3$ | $5^p+1$ | $24n\pm5$ | $6^p-1$ |
| | | | | $20n\pm7$ | $5^p+1$ | $24n\pm7$ | $6^p+1$ |
| | | | | $20n\pm9$ | $5^p-1$ | $24n\pm11$ | $6^p+1$ |

| *pro* $a=7$ | | *pro* $a=8$ | | *pro* $a=10$ | | *pro* $a=11$ | |
|---|---|---|---|---|---|---|---|
| $28n\pm1$ | $7^p-1$ | $32n\pm1$ | $8^p-1$ | $40n\pm1$ | $10^p-1$ | $44n\pm1$ | $11^p-1$ |
| $28n\pm3$ | $7^p-1$ | $32n\pm3$ | $8^p+1$ | $40n\pm3$ | $10^p-1$ | $44n\pm3$ | $11^p+1$ |
| $28n\pm5$ | $7^p+1$ | $32n\pm5$ | $8^p+1$ | $40n\pm7$ | $10^p+1$ | $44n\pm5$ | $11^p-1$ |
| $28n\pm9$ | $7^p-1$ | $32n\pm7$ | $8^p-1$ | $40n\pm9$ | $10^p-1$ | $44n\pm7$ | $11^p-1$ |
| $28n\pm11$ | $7^p+1$ | $32n\pm9$ | $8^p-1$ | $40n\pm11$ | $10^p+1$ | $44n\pm9$ | $11^p-1$ |
| $28n\pm13$ | $7^p+1$ | $32n\pm11$ | $8^p+1$ | $40n\pm13$ | $10^p-1$ | $44n\pm13$ | $11^p+1$ |
| | | $32n\pm13$ | $8^p+1$ | $40n\pm17$ | $10^p+1$ | $44n\pm15$ | $11^p+1$ |
| | | $32n\pm15$ | $8^p-1$ | $40n\pm19$ | $10^p+1$ | $44n\pm17$ | $11^p+1$ |
| | | | | | | $44n\pm19$ | $11^p-1$ |
| | | | | | | $44n\pm21$ | $11^p+1$ |

| pro a = 12 | | pro a = 13 | | pro a = 14 | | pro a = 15 | |
|---|---|---|---|---|---|---|---|
| $48n \pm 1$ | $12^p - 1$ | $52n \pm 1$ | $13^p - 1$ | $56n \pm 1$ | $14^p - 1$ | $60n \pm 1$ | $15^p - 1$ |
| $48n \pm 5$ | $12^p + 1$ | $52n \pm 3$ | $13^p - 1$ | $56n \pm 3$ | $14^p + 1$ | $60n \pm 7$ | $15^p - 1$ |
| $48n \pm 7$ | $12^p + 1$ | $52n \pm 5$ | $13^p + 1$ | $56n \pm 5$ | $14^p - 1$ | $60n \pm 11$ | $15^p - 1$ |
| $48n \pm 11$ | $12^p - 1$ | $52n \pm 7$ | $13^p + 1$ | $56n \pm 9$ | $14^p - 1$ | $60n \pm 13$ | $15^p + 1$ |
| $48n \pm 13$ | $12^p - 1$ | $52n \pm 9$ | $13^p - 1$ | $56n \pm 11$ | $14^p - 1$ | $60n \pm 17$ | $15^p - 1$ |
| $48n \pm 17$ | $12^p + 1$ | $52n \pm 11$ | $13^p + 1$ | $56n \pm 13$ | $14^p - 1$ | $60n \pm 19$ | $15^p + 1$ |
| $48n \pm 19$ | $12^p + 1$ | $52n \pm 15$ | $13^p + 1$ | $56n \pm 15$ | $14^p + 1$ | $60n \pm 23$ | $15^p + 1$ |
| $48n \pm 23$ | $12^p - 1$ | $52n \pm 17$ | $13^p - 1$ | $56n \pm 17$ | $14^p + 1$ | $60n \pm 29$ | $15^p + 1$ |
| | | $52n \pm 19$ | $13^p + 1$ | $56n \pm 19$ | $14^p + 1$ | | |
| | | $52n \pm 21$ | $13^p + 1$ | $56n \pm 23$ | $14^p + 1$ | | |
| | | $52n \pm 23$ | $13^p - 1$ | $56n \pm 25$ | $14^p - 1$ | | |
| | | $52n \pm 25$ | $13^p - 1$ | $56n \pm 27$ | $14^p + 1$ | | |

A. m. T. I. p. 211—213. 215. 216.

## 16.

Theorema. Si potestas $a^p$ per $N$ divisa relinquat $r$, at potestas $a^q$ residuum $s$, tum formula $s^p - r^q$ per $N$ erit divisibilis.

Demonstratio. Cum $a^p - r$ sit divisibilis per $N$, tum etiam $a^{np} - r^n$ erit divisibilis, ergo etiam $a^{pq} - r^q$. Simili modo cum $a^q - s$ sit divisibilis per $N$, etiam $a^{pq} - s^p$ erit divisibilis; unde sequitur etiam $s^p - r^q$ fore divisibile per $N$. Hinc si $r = 1$, tum $s^p - 1$ erit divisibile.

Theorema. Si fuerit $r + \lambda N = a^\alpha s$, tum $a^{p-\alpha} - s$ est divisibile per $N$. Hic ergo est $r = a^\alpha s - \lambda N$ et $q = p - \alpha$; erit ergo

$$s^p - (a^\alpha s - \lambda N)^{p-\alpha} \text{ per } N \text{ divisibile.}$$

A. m. T. I. p. 214.

## 17.

(Krafft.)

Si fuerit $p$ numerus impar, tum $\frac{2^p+1}{3}$ semper est numerus integer, qui quoties $p$ est numerus primus, videtur etiam esse numerus primus, id quod examinetur.

Ponatur $\frac{2^p+1}{3} = y$; erit sequens $\frac{2^{p+2}+1}{3} = \frac{4.2^p+1}{3}$. At ex priore est $2^p = 3y - 1$; unde sequens erit $\frac{12y-3}{3} = 4y - 1$, unde formetur sequens series

$$\begin{array}{llllllllllll} p \ldots 1, & 3, & 5, & 7, & (9), & 11, & 13, & (15), & 17, & 19, & \text{etc.} \\ y \ldots 1, & 3, & 11, & 43, & (171), & 683, & 2731, & (10923), & 43691, & 174763, & \text{etc.} \end{array}$$

Hinc suspicio confirmatur usque ad ultimum 174763, qui sit $= a$, ita, ut sit $3a = 2^{19} + 1$; at hic numerus continetur in forma $2f^2 + g^2$, quae alios divisores non habet, nisi in eadem forma contentos; necesse ergo est, sit $174763 = 2r^2 + s^2$ idque unico modo. Si ergo hic numerus unico modo in forma $2r^2 + s^2$ contineatur, certo erit primus; sin autem pluribus modis contineatur, tum demum erit compositus; id quod non adeo difficile est explorare. Est autem

$$174763 = 2.295^2 + 713 = 2.294^2 + 1891 = 2.293^2 + 3065 \ldots (= 2.171^2 + 341^2).$$

(Lexell.)

At sine tanto calculo demonstrari potest hunc numerum esse primum. Si enim haberet divisorem, is *primo* minor esset, quam radix quadrata hujus numeri, quae est 418, sive $< 419$. *Secundo* divisor iste continebitur in forma vel $8n+1$, vel $8n+3$. Tertio divisor etiam formam habebit $19\lambda+1$, ubi $\lambda$ primo esse debet par; erit ergo vel $\lambda=8n$, vel $8n+2$, vel $8n+4$, vel $8n+6$. Prima dat formam $8n+1$, quae congruit cum priore; at $\lambda=8n+2$ dat $8n+39$, ideoque $\lambda=8n+2$ excluditur; similiter $\lambda=8n+4$ dat $8n+5$, unde $\lambda=8n+4$ excluditur; at $\lambda=8n+6$ dat $8n+3$, quae valet. Duae ergo formae relinquuntur pro $\lambda$, $8n$ et $8n+6$; ergo ex priori $19\lambda+1$ habentur: 1, 153, 305, 457, et ex posteriori $19\lambda+1$: 115, 267, 419. Hi autem numeri, minores quam 419, omnes sunt compositi.

Neque vero propositio supra memorata est vera, plures enim casus assignari possunt, quibus fallit. Cum enim numerus primus $2p+1$ quoties fuerit formae $8n+3$, sit divisor formulae $2^p+1$, ob $p=4n+1$ utique fieri potest, ut $p$ sit numerus primus; iis ergo casibus etiam formula $\frac{2^p+1}{3}$ divisorem habebit $8n+3$, hoc itaque evenit, quoties tam $4n+1$ quam $8n+3$ fuerint numeri primi, cujusmodi casus sunt:

5, 29, 41, 53, 89
11, 59, 83, 107, 179.

A. m. T. I. p. 217.

## 18.

(*J. A. Euler.*)

Ut formulae $x^4+1$ divisor sit 17, erit . . . . . . . . . . . . . . $x=2$, vel 8, vel 9, vel 15
Ut ejusdem formulae divisor sit 41, erit . . . . . . . . . . . . $x=3$, vel 14, vel 27, vel 38
" " " 73, erit . . . . . . . . . . . . . . . . $x=10$, vel 22, vel 51, vel 63
" " " 89, erit . . . . . . . . . . . . . . . . $x=12$, vel 37, vel 52, vel 77
In omnibus scilicet casibus, si fuerit $x=a$, erit etiam

$$x=a^3 \quad \text{et} \quad =a^5 \quad \text{et} \quad =a^7 \quad \text{etc.}$$

A. m. T. I. p. 201.

## d) *De divisoribus et residuis numerorum quadratorum.*

## 19.

Theorema, cujus demonstratio desideratur.

Si pro divisore $d$ inter residua quadratorum occurrat $\pm r$, tum etiam pro divisore $4nr+d$, si fuerit numerus primus, inter residua quadratorum idem quoque residuum $\pm r$ occurret. Ita si sit $d=7$, inter residua quadratorum occurrit 2; ideoque quoties $8n+7$ fuerit numerus primus, (eo divisore) inter residua quadratorum reperiatur 2 necesse est.

Ratio in eo quaerenda videtur, quod si $8n+7$ est numerus primus, tum numerus residuorum semper est $4n+3$, dum si non fuerit primus, multitudo residuorum multo est minor: scilicet pro $8n+7=15$, multitudo residuorum non est 7, sed tantum 5.

A. m. T. I. p. 210.

## 20.

Theoremata demonstranda.

I. Si per numerum primum $4n+1$ omnia quadrata dividantur, inter residua occurret non solum ipse numerus $n$, sed etiam omnes ejus divisores et quidem singuli utroque signo affecti.

II. Si per numerum primum $4n-1$ omnia quadrata dividantur, inter residua non solum occurret ipse numerus $n$, sed etiam omnes ejus divisores signo $+$ affecti; iidem enim signo $-$ affecti erunt non-residua. Haec duo theoremata ita generalius proponi possunt: Denotante $i$ numerum imparem quemcunque,

I. si per numerum primum $4n+i$ quadrata dividantur, inter residua occurrent omnes divisores numeri $n$ tam signo $+$ quam signo $-$ affecti.

I. Corollarium. Hinc si $4n+ii$ est numerus primus et $d$ aliquis divisor numeri $n$, semper dari poterit formula $xx+dyy$ per illum numerum $4n+ii$ divisibilis.

II. Si per numerum primum $4n-ii$ quadrata dividantur, inter residua occurrent omnes divisores numeri $n$ positive sumti, iidem vero negative sumti erunt non-residua.

Corollarium. Ergo si $d$ fuerit divisor quicunque numeri $n$, semper dabuntur hujusmodi formulae $xx-dyy$ per numerum primum $4n-ii$ divisibiles: contra vero nulla dabitur talis formula $xx+dyy$ per hunc numerum primum divisibilis. A. m. T. I. p. 224

## 21.

**(Krafft.)**

Problema. Invenire omnes numeros primos formae $4n+1$, per quos si quadrata dividantur, inter residua occurrat datus numerus $\pm a$.

Solutio. Ante vidimus, si divisor primus fuerit $4ap+ii$, inter residua certo occurrere $\pm a$. Statuatur ergo $4n+1=4ap+ii$, et quia $i$ est impar, ponatur $i=2c+1$, ut prodeat

$$4n+1=4ap+4c^2+4c+1, \text{ seu } n=ap+c^2+c.$$

Quoties ergo fuerit $n=ap+c^2+c$, quicunque numeri pro $c$ et $p$ statuantur, tum numerus $4n+1$ satisfaciet, siquidem fuerit primus.

Corollarium. Simili modo patebit, ut divisori primo $4n-1$ conveniat in residuis numerus $+a$, tum sumi debere $n=ap-c^2-c$.

Formula autem $c^2+c$ hos praebet numeros: 0, 2, 6, 12, 20, 30, 42, 56, etc., quibus per $a$ divisis sit quodvis residuum $=r$, quodvis autem non-residuum sit $\varrho$, atque sequentia theoremata obtinebuntur:

I. Si fuerit $4n+1$ primus et $n=ap+r$, tum in residuis quadratorum per $4n+1$ divisorum occurrunt numeri $+a$ et $-a$, ideoque dabuntur formulae $x^2+ay^2$ et $x^2-ay^2$ per $4n+1$ divisibiles; tum vero etiam formula $a^{2n}-1$ quoque erit divisibilis.

II. Existente $4n+1$ numero primo, si fuerit $n=ap+\varrho$, tum in residuis quadratorum neque $+a$ neque $-a$ occurret, et neutra formula $x^2+ay^2$ et $x^2-ay^2$, neque etiam haec $a^{2n}-1$ erit divisibilis per $2n+1$; cum ergo $a^{4n}-1$ sit divisibilis, sequitur, formulam $a^{2n}+1$ fore divisibilem per $4n+1$.

III. Si divisor primus $=4n-1$ atque $n=ap-r$, tum in residuis quadratorum occurret $+a$, non vero $-a$, ideoque dabitur formula $xx-ayy$ per $4n-1$ divisibilis, non vero $xx+ayy$; tum vero formula $a^{2n-1}-1$ divisibilis erit per $4n-1$.

IV. Si divisor primus $4n-1$ at $n=ap-\varrho$, inter residua quadratorum non occurret $+a$, sed $-a$, ideoque dabitur formula $xx+ayy$ divisibilis per $4n-1$, et jam formula $(-a)^{2n-1}-1$, sive $a^{2n-1}+1$ divisibilis erit per $4n-1$.

In his autem theorematibus praecedentia fere omnia continentur, id quod sequentibus ostendamus exemplis.

1) Sit $a=2$, erit $r=0$ et $\varrho=1$, unde sequitur

pro I. $n=2p$, ideoque divisor $4n+1=8p+1$; sequentes igitur dabuntur formulae per $8p+1$ divisibiles: $x^2+2y^2$; $x^2-2y^2$ et $2^{4p}-1$;

pro II. $n=2p+1$, ergo $4n+1=8p+5$, per quem numerum scilicet primum neutra formularum $x^2+2y^2$ et $x^2-2y^2$, at vero $2^{4p+2}+1$ erit divisibilis;

pro III. $n=2p$ et divisor primus $4n-1=8p-1$, per quem divisibilis erit formula $x^2-2y^2$, tum vero etiam $2^{4p-1}-1$;

pro IV. $n=2p-1$ et divisor $4n-1=8p-5$, sive $8p+3$, per quem divisibiles erunt formulae $x^2+2y^2$ et $a^{4p-3}+1$, sive $a^{4p-3}+1$.

2) Sit $a = 3$, ubi $r = 0, 2$ et $\varrho = 1$, ergo

pro I. $n = 3p + 0$, vel $3p + 2$, ideoque $4n + 1 = 12p + 1$, $12p + 9$, ubi casus posterior est rejiciendus ...

... ut sit $4n + 1 = 12p + 1$, per quem divisibiles sunt $x^2 \pm 3y^2$ et $3^{2n} - 1$;

pro II. $n = 3p + 1$ et divisor $4n + 1 = 12p + 5$, per quem divisibilis est formula $3^{2n} + 1$;

pro III. $n = 3p + 0, 2$, et divisor $4n - 1 = 12p - 1$, sive $12p - 9$, quod sponte excidit, per quem formulae divisibiles $x^2 - 3y^2$ et $3^{2n-1} - 1$;

pro IV. $n = 3p - 1$, hinc $4n - 1 = 12p - 5$; formulae divisibiles $x^2 + 3y^2$ et $3^{2n-1} + 1$.

3) Sit $a = 5$, ubi $r = 0, 2, 1$ et $\varrho = 3, 4$, sive $= -1, -2$.

Pro I. $n = 5p + 0, 1, 2$; $4n + 1 = 20p + 1, (5), 9$; formulae divisibiles $x^2 \pm 5y^2$ et $5^{2n} - 1$;

pro II. $n = 5p - 1, -2$; $4n + 1 = 20p - 3, -7$; formula divisibilis $5^{2n} + 1$;

pro III. $n = 5p - 0, 1, 2$; $4n - 1 = 20p - 1, (-5), -9$; formulae divisibiles $x^2 - 5y^2$, $5^{2n-1} - 1$;

pro IV. $n = 5p + 1, 2$; $4n - 1 = 20p + 3, 7$, formulae divisibiles $x^2 + 5y^2$ et $5^{2n-1} + 1$;

4) Sit $a = 6$, $r = 0, 2$ et $\varrho = 1, 3, 4, 5$, sive $= -2, -1$.

Pro I. $n = 6p + 0, 2$; $4n + 1 = 24p + 1$; formulae divisibiles $x^2 \pm 6y^2$ et $6^{2n} - 1$;

pro II. $n = 6p + 1, 3, -2, -1$; $4n + 1 = 24p + 5, 13, -7$; formula divisibilis $6^{2n} + 1$;

pro III. $n = 6p - 0, 2$ et $4n - 1 = 24p - 1, 9$; formulae divisibiles $x^2 - 6y^2$ et $6^{2n-1} - 1$;

pro IV. $n = 6p - 1, -3, +2, +1$; $4n - 1 = 24p - 5, -13, +7$; formulae divisib. $x^2 + 6y^2$ et $6^{2n-1} + 1$.

Ubi notandum est, unitatem hic perperam referri ad $\varrho$, valores enim literarum $r$ et $\varrho$ inter se aequales esse debent et oporteret 1 ad $r$ referre, ita ut pro 1 sit etiam $4n + 1 = 24p + 5$, quod etiam confirmatur per residua; si enim $n = 0$, pro divisore 5 utique occurrit residuum 6, utpote $1 + 5$.

Idem inconveniens occurret, quoties $n$ est numerus par; id vero incongruum ita diluendum videtur: Cum per divisorem 6 dividi debeant numeri 0, 2, 6, 12, 20, etc. utrinque diviso per 2, habebuntur numeri 0, 1, 3, 6, 10, etc. per 3 dividendi; unde manifesto oritur residuum 1 praeter praecedentia, quod ergo ex $\varrho$ expungi debet: Ita si $a = 10$, primo pro $r$ reperimus hos valores 0, 2, 6; per binarium autem dividendo insuper accedunt ad $r$ 1, 3, ita, ut valores ipsius $r$ jam sint 0, 1, 2, 3, 6, ergo ipsius $\varrho$:

4, 5, 7, 8, 9; $4r + 1 = 1, (5), 9, 13, (25)$; $4\varrho + 1 = 17, 21, 29, 33, 37$, sive $17, -19, -11, -7, -3$;

hic ergo etiam numerus 9 ab $\varrho$ ad $r$ est transferendus.

(*Lexell.*)

Vera autem solutio hujus difficultatis in indole numeri $a$ est quaerenda, qui si fuerit primus, valores pro $r$ et $\varrho$ supra assignati recte se habent; sin autem est compositus, valores quidem pro $r$ oriundi recte se habent, sed non omnes per regulam supra datam reperiuntur, sed aliunde insuper alii accedunt. Ut enim formula $(ab)^x - 1$ divisibilis sit per numerum primum $2x + 1$, id duplici modo contingere potest: priori quando $a^x - 1$ et $b^x - 1$ divisionem admittunt; si enim $a^x - 1$ est divisibile, erit etiam $(ab)^x - b^x$; addatur formula divisibilis $b^x - 1$, prodit formula divisibilis $(ab)^x - 1$, atque hos casus regula nostra suppeditat. Praeterea vero formula $(ab)^x - 1$ erit divisibilis, si istae $a^x + 1$ et $b^x + 1$ fuerint divisibiles; cum enim ex priori sequatur $(ab)^x + b^x$ divisibilis, auferendo hinc $b^x + 1$ remanet $(ab)^x - 1$ divisibilis. Hinc igitur novi valores ad $r$ accedunt, qui supra ad $\varrho$ perperam erant relati. Totum igitur hoc argumentum accuratius sequenti modo simulque concinnius pertractatur.

Denotet $2m + 1$ semper numerum primum, et supra affirmavimus, si fuerit $2m + 1 = 4ab + ii$ (denotantibus $i$ numeros impares), tum in residuis quadratorum tam $+a$ quam $-a$ reperiri; sin autem fuerit $2m + 1 = 4ab - ii$, tum tantum $+a$ in residuis occurrere; utroque autem casu, hoc est si $2m + 1 = 4ab \pm ii$, formulam $a^m - 1$ divisibilem esse per $2m + 1$. Hujus quidem demonstratio nondum perfecta habetur, sed tamen non longe abest videmur, cum enim quadrata per numerum $2m+1$ dividi debeant, ut residua eruantur, per $2m+1=4ab+ii$ dividatur ipsum quadratum $ii$, et residuum erit $-4ab$, ideoque etiam $-ab$, et quia divisor est formae $4n+1$, etiam $+ab$ erit residuum. Superest igitur tantum, ut demonstretur, tam $+a$ quam $+b$ seorsim inter residua occurrere; si enim ambo essent non-residua, nihilominus productum $ab$ foret residuum. Ad hoc dilucidandum, proponatur divisor primus $2m+1=4ab+(2c+1)^2$, ita ut $ab$ certe sit residuum; quoniam hic numerus pluribus aliis modis similiter exhiberi potest. Statuamus $2m+1=4p+(2q+1)^2$, et nunc etiam $p$ certe erit residuum. Aequentur hae duae formulae inter se, et reperiemus $p=ab+cc+c-qq-q$, ubi $q$ pro lubitu assumere licet, sicque plura alia residua prodibunt, inter quae si occurrat alteruter numerus $a$ vel $b$, etiam alter certe erit residuum. Ut hoc uberius explicetur, notasse juvabit, inter residua primum omnia occurrere quadrata; deinde si occurrant numeri $\alpha$, $\beta$, $\gamma$, etc., etiam producta ex binis vel pluribus occurrent. Et si occurrant numeri $\alpha$ et $\alpha\gamma$, etiam $\gamma$ occurret, et si occurrat $\alpha\gamma^2$, etiam $\alpha$ occurret; hoc igitur exemplis illustremus.

Exemplum I. Sit $a=2$, $b=2$, ideoque $2m+1=16+(2c+1)^2$.

1) Sit $c=0$ eritque $p=4-qq-q=4-(0, 2, 6, 12)$, hinc capiatur $p=4-2=2$, ergo 2 certe est residuum.

2) Sit $2c+1=5$, erit $p=4+6-qq-q=10-(0, 2, 6, 12)$ et sumto $q=1$, erit $p=8=2.4$, ergo 2 residuum.

3) Sit $c=4$ sive $2m+1=97$, unde $p=24-qq-q$; sumatur $q=2$, erit $p=18$, ideoque 2 residuum.

Exemplum II. Sit $a=2$ et $b=3$ et $2m+1=24+(2c+1)^2$. Sit $c=3$, ut fiat $2m+1=73$, ergo $p=6+12-qq-q=18-qq-q$; sumatur $q=0$ fit $p=2.9$, ergo et 2 et 3 residua.

Exemplum III. Sit $a=3$ et $b=3$ et $2m+1=36+(2c+1)^2$. Sit $c=0$, ut fiat $2m+1=37$, ergo $p=9-qq-q=9-(0, 2, 6)$; sumto $q=2$, $p=3$. Sit deinde $c=2$, unde $2m+1=61$, hinc

$$p=9+6-qq-q=15-(0, 2, 6), \quad \text{ergo} \quad p=15-12=3.$$

Exemplum IV. Sit $ab=2.3.5$, ideoque $2m+1=8.3.5+(2c+1)^2$. Sumto $c=5$, ut sit $2m+1=241$, erit

$$p=2.3.5+30-qq-q=60-(0, 2, 6, 12, 20, 30, 42, 56).$$

At $60-6$ dat $54=6.9$, ergo 6 est residuum, ergo et 5; deinde $p=60-12$ dat $48=3.16$, unde 3 est residuum et 2, sicque singuli factores 2, 3, 5 sunt residua.

Exemplum V. Sit $ab=3.5.7=105$, ideoque $2m+1=420+(2c+1)^2$ et sumto $c=0$, $2m+1=421$, unde

$$p=105-q(q+1)=105-(0, 2, 6, 12, 20, 30, 42, 56, 72, 90, 110).$$

Hinc $105-30=75=3.25$, ergo 3 est residuum, ideoque et 35. Deinde $p=105-42=63=7.9$, ideoque 7 residuum ut et 5; sicque singuli factores sunt residua.

Hinc ergo tuto concludi posse videtur, quotcunque etiam factores habeat productum $ab$, singulos semper quoque inter residua occurrere, quod idem simili modo de altera forma $4ab-(2c+1)^2$ ostenditur; posito enim

$$4ab-(2c+1)^2=4p-(2q+1)^2, \quad \text{erit} \quad p=ab-cc-c+qq+q,$$

ubi $p$ certo est residuum.

Exemplum I. Sit $ab=2.2$, $2m+1=16-(2c+1)^2$, sumto $c=1$, $2m+1=7$, ergo

$$p=4-2+qq+q=2+qq+q,$$

unde, si $q=0$, patet 2 esse residuum.

Exemplum II. Sit $ab=2.3=6$, erit $2m+1=24-(2c+1)^2$; posito $c=0$, $2m+1=23$, ergo

$$p=6+qq+q=6+(0, 2, 6, 12, 20), \text{ unde } p=6+2=8=2.4;$$

ergo 2 residuum, ideoque et 3, sive $p=6+6=12=3.4$, ergo 3 residuum.

Exemplum III. Sit $ab=2.2.3.5=60$ et $2m+1=240-(2c+1)^2$; posito

$$c=0, \; 2m+1=239, \text{ unde } p=60+(0, 2, 6, 12, 20, 30, 42, \text{etc.}).$$

Hinc $p = 60 + 12 = 72 = 2.36$, ergo 2 est residuum. Porro $p = 60 + 20 = 5.16$, ergo 5 residuum, ideoque etiam 3. Sive sumto $p = 60 + 30 = 90 = 10.9$, ergo 10 residuum, hinc etiam 5. Sumto autem $a = 2$, erit $2m + 1 = 191$ primus, ergo $p = 60 + 12 + qq + q = 48 + qq + q = 48 + (0, 2, 6, 12, 20, 30, 42)$. Hinc statim $p = 48 = 3.16$ dat 3 pro residuo, deinde $p = 50 = 2.25$ dat 2 pro residuo. Porro $p = 48 + 42 = 90 = 10.9$, ergo 10 residuum, ideoque et 5.

Quamquam haec prorsus certa videntur, tamen demonstratio desideratur.

*Uberior consideratio formulae* $2m + 1 = 4ab \pm ii$,

ubi primo inquirendum, quibusnam casibus $a$ inter residua reperiatur. Quia $ii$ semper est numerus formae $4r + 1$, nostra formula ita referetur $4ab \pm (4r + 1)$, at formula $4r + 1$ continet primo omnia quadrata imparia, quae quidem cum $4ab$ numeros primos dare possunt, majora autem infra $4a$ deprimi possunt, dum ab iis subtrahitur $4a$ quoties fieri possit, hocque modo pro quovis casu numeri $a$, formula $4r + 1$ certos sortietur valores minores, quam $4a$, ac si $a$ fuerit numerus primus, hoc modo omnes prodeunt idonei valores pro $4r + 1$, qui autem numeri hujus formae non occurrunt, eos formula $4\varrho + 1$ indicemus, atque his numeris utriusque generis $4r + 1$ et $4\varrho + 1$ pro quovis numero primo $a$ definitis, sequentia habebimus theoremata.

I. Si fuerit $2m + 1 = 4ab \pm (4r + 1)$, tum formula $a^m \mp 1$ semper erit divisibilis per $2m + 1$, ac casu signi superioris tam $+a$ quam $-a$ inter residua quadratorum reperientur, casu autem signi inferioris, tantum $+a$ erit residuum, et $-a$ non-residuum.

II. Si fuerit $2m + 1 = 4ab \pm (4\varrho + 1)$, tum semper formula $a^m \pm 1$ dividi poterit per $2m + 1$, tum vero pro signo superiore $+$ neque $a$ nec $-a$ erit residuum, sive neque $xx + ayy$ nec $xx - ayy$ unquam per $2m + 1$ dividi poterit. Pro signo autem inferiore $-$, inter residua erit $-a$, sive formula $xx + ayy$ divisibilis erit per $2m + 1$; probe autem hic notetur, haec tantum valere, si $a$ fuerit numerus primus, numeri enim compositi aliam requirunt evolutionem. Nunc igitur pro singulis numeris primis $a$ exhibeamus numeros illos duplicis generis in formulis $4r + 1$ et $4\varrho + 1$ contentos.

$$a = 2 \left\{ \begin{array}{l|l} 4r + 1 = 1, & 9,\ 17,\ 25,\ 33,\ 41,\ 49,\ 57,\ \text{etc.} \\ 4\varrho + 1 = 5, & 13,\ 21,\ 29,\ 37,\ 45,\ 53,\ 61,\ \text{etc.} \end{array} \right.$$

$$a = 3 \left\{ \begin{array}{l|l} 4r + 1 = 1, & 13,\ 25,\ 37,\ 49,\ 61,\ 73,\ \text{etc.} \\ 4\varrho + 1 = 5, & 17,\ 29,\ 41,\ 53,\ 65,\ 77,\ \text{etc.} \end{array} \right.$$

$$a = 5 \left\{ \begin{array}{l|l} 4r + 1 = 1,\ 9, & 21,\ 29,\ 41,\ 49,\ 61,\ 69,\ 81,\ 89,\ \text{etc.} \\ 4\varrho + 1 = 13,\ 17, & 33,\ 37,\ 53,\ 57,\ 73,\ 77,\ 93,\ 97,\ \text{etc.} \end{array} \right.$$

$$a = 7 \left\{ \begin{array}{l|l} 4r + 1 = 1,\ 9,\ 25, & 29,\ 37,\ 53,\ 57,\ 65,\ 81,\ \text{etc.} \\ 4\varrho + 1 = 5,\ 13,\ 17, & 33,\ 41,\ 45,\ 61,\ 69,\ 73,\ \text{etc.} \end{array} \right.$$

$$a = 11 \left\{ \begin{array}{l|l|l} 4r + 1 = 1,\ 5,\ 9,\ 25,\ 37, & 45,\ 49,\ 53,\ 69,\ 81, & 89,\ 93,\ 97,\ \text{etc.} \\ 4\varrho + 1 = 13,\ 17,\ 21,\ 29,\ 41, & 57,\ 61,\ 65,\ 73,\ 85, & 101,\ 105,\ \text{etc.} \end{array} \right.$$

$$a = 13 \left\{ \begin{array}{l|l} 4r + 1 = 1,\ 9,\ 17,\ 25,\ 29,\ 49, & 53,\ 61,\ 69,\ 77,\ 81,\ 101,\ \text{etc.} \\ 4\varrho + 1 = 5,\ 21,\ 33,\ 37,\ 41,\ 45, & 57,\ 73,\ 85,\ 89,\ 93,\ 97,\ \text{etc.} \end{array} \right.$$

$$a = 17 \left\{ \begin{array}{l|l} 4r + 1 = 1,\ 9,\ 13,\ 21,\ 25,\ 33,\ 49,\ 53, & 69,\ 77,\ 81,\ 89,\ 93,\ 101,\ \text{etc.} \\ 4\varrho + 1 = 5,\ 29,\ 37,\ 41,\ 45,\ 57,\ 61,\ 65, & 73,\ 97,\ 105,\ \text{etc.} \end{array} \right.$$

$$a = 19 \left\{ \begin{array}{l|l} 4r + 1 = 1,\ 5,\ 9,\ 17,\ 25,\ 45,\ 49,\ 61,\ 73, & 77,\ 81,\ 85,\ \text{etc.} \\ 4\varrho + 1 = 13,\ 21,\ 29,\ 33,\ 37,\ 41,\ 53,\ 65,\ 69, & \text{etc.} \end{array} \right.$$

$$a = 23 \left\{ \begin{array}{l} 4r + 1 = 1,\ 9,\ 13,\ 25,\ 29,\ 41,\ 49,\ 73,\ 77,\ 81,\ 85,\ \text{etc.} \\ 4\varrho + 1 = 5,\ 17,\ 21,\ 33,\ 37,\ 45,\ 53,\ 57,\ 61,\ 65,\ 89,\ \text{etc.} \end{array} \right.$$

Geminas has series pro quovis numero primo $a$ facile in infinitum continuare licet, eas autem in periodos distinximus, quarum prima continet numeros formae $4n+1$, minores quam $4a$, secunda periodus continet eosdem numeros $+4a$. Tertia continet numeros secundae periodi $+4a$ et ita porro.

Hinc igitur pro casibus, quibus $a$ est primus, judicare licet, utrum formula $a^m-1$ an $a^m+1$ per numerum primum $2m+1$ sit divisibilis; prius scilicet evenit, quoties fuerit $2m+1=4ab\pm(4r+1)$, posterius vero quoties fuerit $2m+1=4ab\pm(4\varrho+1)$. Circa has series notari oportet, in qualibet periodo contineri $\frac{a-1}{2}$ terminos, ita ut in ordine $4\varrho+1$ totidem sint termini quot in $4r+1$; deinde omnes termini ordinis $4r+1$ vel ipsi sunt quadrata, vel tales, ut $4r+1+4an$ fieri possit quadratum. Contra vero numeri $4\varrho+1$ omnes ita sunt comparati, ut formula $4\varrho+1+4an$ nunquam fieri possit quadratum, quicunque numerus pro $n$ capiatur.

Problema. Nunc videamus, quomodo judicium institui debeat, quando numerus $a$ habet factores, scilicet tum etiam investigemus tam terminos $4r+1$ quam $4\varrho+1$ tali numero $a$ convenientes.

Solutio. Sit $a=fg$ et $f$ et $g$ numeri primi. Quaerantur primo pro $f$ numeri tam formae $4r+1$ quam $4\varrho+1$, qui ita designentur ${}^f(4r+1)$ et ${}^f(4\varrho+1)$, eodemque modo pro numero $g$ habeantur formulae ${}^g(4r+1)$ et ${}^g(4\varrho+1)$, quo facto excerpantur omnes numeri binis formulis ${}^f(4r+1)$ et ${}^g(4r+1)$ communes, cujusmodi sit $P$, et ex praecedentibus patet, si divisor fuerit $4fp\pm P=2m+1$, tum formulam $f^m-1$ fore divisibilem per $2m+1$. Simili modo pro divisore $2m+1=4gq\pm P$ formulam $g^m-1$ esse divisibilem. Fiat nunc $p=gn$ et $q=fn$, ut prodeat communis divisor $4fgn\pm P$, per quem ambae formulae $f^m-1$ et $g^m-1$ erunt divisibiles, unde sequitur, quoque formulam $(fg)^m-1=a^m-1$ fore divisibilem. Praeterea cum $a^m-1$ quoque sit divisibile, si tam $f^m+1$ quam $g^m+1$ dividi queant, id quod evenit, si ex ordinibus ${}^f(4\varrho+1)$ et ${}^g(4\varrho+1)$ termini communes excerpantur, quam ob rem pro numero proposito $a=fg$ ordo $4r+1$ primo continebit omnes terminos communes ordinum ${}^f(4r+1)$ et ${}^g(4r+1)$, praeterea vero etiam terminos communes ordinibus ${}^f(4\varrho+1)$ et ${}^g(4\varrho+1)$. Reliqui vero numeri formae $4n+1$ hic non occurrentes ad ordinem $4\varrho+1$ sunt referendi, ubi ergo occurrent primo termini communes ordinibus ${}^f(4r+1)$ et ${}^g(4\varrho+1)$, tum vero etiam communes ordinibus ${}^g(4r+1)$ et ${}^f(4\varrho+1)$; hoc igitur modo pro numero $a=fg$ facile colligentur numeri ordinis $4r+1$ et $4\varrho+1$.

Corollarium 1. Si fuerit $g=f$, ita ut $a$ fiat quadratum $=ff$, tum pro ordine $4r+1$ omnes plane numeri ordinis $4n+1$ occurrent, alter vero ordo $4\varrho+1$ plane manebit vacuus, id quod etiam inde manifestum est, quod si $a$ fuerit quadratum $=ff$, semper formulam $a^m-1=f^{2m}-1$ esse divisibilem per numerum $2m+1$.

Corollarium 2. Sin autem factores $f$ et $g$ fuerint dispares, ex praecedentibus ordinibus serierum facile pro quovis numero $a=fg$ termini utriusque ordinis colligentur, quemadmodum ex sequentibus exemplis patebit.

Exemplum I. Sit $a=2.3$, ideoque $4a=24$, et terminus communis ordinum ${}^2(4r+1)$ et ${}^3(4r+1)$ est 1 cum sequentibus 25, 49, 73, 97; at vero terminus ordinibus ${}^2(4\varrho+1)$ et ${}^3(4\varrho+1)$ communis est 5, unde in primo ordine tantum occurrunt 1, 5, at pro ordine $(4\varrho+1)$ terminus communis ordinibus ${}^2(4r+1)$ et ${}^3(4\varrho+1)$ est 17, ordinibus autem ${}^3(4r+1)$ et ${}^2(4\varrho+1)$ communis est 13. Qui ordines ita referantur

$$a=6,\quad 4a=24\left\{\begin{array}{l|l} 4r+1=1,\ 5, & 25,\ 29,\ 49,\ 53,\ 73,\ 77,\ 97,\ 101 \\ 4\varrho+1=13,\ 17, & 37,\ 41,\ 61,\ 65,\ 85,\ 89 \end{array}\right.$$

Exemplum 2. Sit $a=2.5=10$ et $4a=40$. Hic termini communes ordinum ${}^2(4r+1)$ et ${}^5(4r+1)$ sunt 1, 9, at termini communes ordinum ${}^2(4\varrho+1)$ et ${}^5(4\varrho+1)$ sunt 13, 37. At pro ordine $4\varrho+1$ sunt termini communes ${}^2(4r+1)$ et ${}^5(4\varrho+1)$, 17, 33, at ordines ${}^5(4r+1)$ et ${}^2(4\varrho+1)$ communes habent 21, 29, unde fit

$$a=10,\quad 4a=40\left\{\begin{array}{l|l} 4r+1=1,\ 9,\ 13,\ 37, & 41,\ 49,\ 53,\ 77,\ 81,\ 89,\ 93 \\ 4\varrho+1=17,\ 21,\ 29,\ 33, & 57,\ 61,\ 69,\ 73,\ 97 \end{array}\right.$$

EXEMPLUM 3. Si $a = 2 \cdot 7 = 14$ et $4a = 56$

$$\begin{array}{l|l} 4r+1 = 1,\ 5,\ 9,\ 13,\ 25,\ 45, & 57,\ 61,\ 65,\ 69,\ 81,\ 101 \\ 4\varrho+1 = 17,\ 29,\ 33,\ 37,\ 41,\ 53, & 73,\ 85,\ 89,\ 93,\ 97,\ 109 \end{array}$$

EXEMPLUM 4. Sit $a = 3 \cdot 5 = 15$ et $4a = 60$

$$\begin{array}{l|l} 4r+1 = 1,\ 17,\ 49,\ 53, & 61,\ 77,\ 109 \\ 4\varrho+1 = 13,\ 29,\ 37,\ 41, & 73,\ 89,\ 97 \end{array}$$

COROLLARIUM. Si fuerit $a = ffg$, quia factor $ff$ in ordine $r$ continet numeros, in ordine $\varrho$ autem nullos termini communes ordinibus $r$ sunt omnes, qui pro $g$ habentur, at termini ordinibus $\varrho$ communes sunt nulli ergo pro hoc casu ordo $4r+1$ congruit cum numero $g$, similique modo congruit ordo $4\varrho+1$. Id quod his casibus apparet

$$a = 8,\quad 4a = 32 \begin{cases} 4r+1 = 1,\ 9,\ 17,\ 25, & \vert\ 33,\ 41,\ 49,\ 57,\ \vert\ 65,\ 73,\ 81,\ 89 \\ 4\varrho+1 = 5,\ 13,\ 21,\ 29, & \vert\ 37,\ 45,\ 53,\ 61,\ \vert\ 69,\ 77,\ 85,\ 93 \end{cases}$$

$$a = 4 \cdot 3 = 12,\quad 4a = 48 \begin{cases} 4r+1 = 1,\ 13,\ 25,\ 37, & \vert\ 49,\ 61,\ 73,\ 85,\ \vert\ 97 \\ 4\varrho+1 = 5,\ 17,\ 29,\ 41, & \vert\ 53,\ 65,\ 77,\ 89, \end{cases}$$

A. m. T. I. p. 226—235

## 22.

(*Krafft.*)

Si fuerit $4n+1$ numerus primus, in residuis quadratorum non solum hi numeri $n - qq - q$, sed etiam omnes eorum divisores occurrent.

Quia numerus residuorum diversorum est $= 2n$, omnia prodibunt, si loco $q$ substituantur numeri $0, 1, 2, 3 \ldots (2n-1)$. Reliqui ergo haec residua erunt, ut sequens tabella indicat, ubi ultima columna ostendit ea quadrata, unde haec residua nascuntur:

| | |
|---|---|
| $n - 0$ | $4n^2$ |
| $n - 2$ | $(2n-1)^2$ |
| $n - 6$ | $(2n-2)^2$ |
| $n - 12$ | $(2n-3)^2$ |
| $n - 20$ | $(2n-4)^2$ |
| $- 4n^2 + 3n$ | $1$ |

Nunc autem demonstrandum restat, etiam omnes factores horum residuorum esse residua, quod eo magis est mirandum, quod cum etiam hae formulae

$$\lambda(4n+1) + n - qq - q$$

pariter residua exhibeant, tamen non omnes factores etiam futuri sint residua.

A. m. T. I. p. 255

## 23.

(*N. Fuss I.*)

OBSERVATIO. Formula $xx+1$ divisibilis erit per sequentes numeros quadratos:

| | | | | |
|---|---|---|---|---|
| I. | per | $5^2$ | si fuerit | $x = 5^2 t \pm 7$ |
| II. | " | $13^2$ | " | $x = 13^2 t \pm 70$ |
| III. | " | $17^2$ | " | $x = 17^2 t \pm 38$ |

| | | | | |
|---|---|---|---|---|
| IV. | per $25^2$ | si fuerit | $x = 25^2 t \pm 57$ |
| V. | „ $29^2$ | „ | $x = 29^2 t \pm 41$ |
| VI. | „ $37^2$ | „ | $x = 37^2 t \pm 117$ |
| VII. | „ $41^2$ | „ | $x = 41^2 t \pm 378$ |
| VIII. | „ $53^2$ | „ | $x = 53^2 t \pm 500$ |
| IX. | „ $61^2$ | „ | $x = 61^2 t \pm 682$ |
| X. | „ $65^2$ | „ | $x = 65^2 t \pm 268$ |
| XI. | „ $73^2$ | „ | $x = 73^2 t \pm 74$ |

Hinc etiam valores ipsius $x$ assignari poterunt, ut haec formula $xx + aa$ per eosdem numeros fiat divisibilis; sicque $xx + aa$ divisibilis erit per $41^2$, si fuerit $x = 41^2 t + 378a$; ita hoc problema resolvi potest, quo quaeruntur valores ipsius $x$, ut haec formula $xx + aa$ divisibilis fiat per $(ff + gg)^2$.

Problema. Invenire numerum $x$, ut $xx + 1$ dividi queat per $aa + bb$.

Solutio. Primo patet, si satisfaciat $x = \alpha$, etiam satisfacturum esse $x = m(a^2 + b^2) \pm \alpha$. Deinde sumto $x = \frac{a}{b}$ satisfacit, quia fit $xx + 1 = \frac{aa + bb}{bb}$. Ponatur ergo $x = \frac{m(aa + bb) \pm a}{b}$, qui ergo numerus debet esse integer. Quia vero est $x = mb + \frac{a(ma \pm 1)}{b}$, debet esse $ma \pm 1$ divisibile per $b$. Quaeratur fractio $\frac{\alpha}{\beta}$ fractioni $\frac{a}{b}$ proxime aequalis, quod fit si $\alpha b - \beta a = \pm 1$. Sumatur ergo $m = \beta$ eritque $x = \beta b + \frac{a(\beta a \pm 1)}{b}$. Cum igitur sit $\beta a \pm 1 = \alpha b$, erit $x = \beta b + \alpha a$. In genere ergo $x = m(aa + bb) \pm (\alpha a + \beta b)$.

Problema. Invenire numerum $x$, ut formula $x^4 + 1$ divisibilis fiat per $a^4 + b^4$.

Solutio. Primo patet hoc fieri, si $x = \frac{a}{b}$. Ponatur ergo $x = \frac{m(a^4 + b^4) \pm a}{b} = mb^3 + \frac{a(ma^3 \pm 1)}{b}$. Quaeratur nunc fractio $\frac{\alpha}{\beta}$ proxime aequalis huic $\frac{a^3}{b}$, ita ut sit $\beta a^3 - \alpha b = \pm 1$, et sumatur $m = \beta$ eritque $x = \beta b^3 + \alpha a$, generaliter ergo

$$x = m(a^4 + b^4) \pm (\beta b^3 + \alpha a).$$

Potuissemus etiam ponere

$$x = \frac{aa}{bb}, \text{ fiat igitur } x = \frac{m(a^4 + b^4) \pm aa}{bb} = mb^2 + \frac{a^2(ma^2 \pm 1)}{bb}.$$

Quaeratur nunc fractio $\frac{\gamma}{\delta}$ proxime aequalis ipsi $\frac{aa}{bb}$, ut sit $\gamma bb - \delta aa = \pm 1$, sumaturque $m = \delta$ eritque

$$x = \delta bb + \gamma aa \quad \text{et generaliter} \quad x = m(a^4 + b^4) \pm (\delta bb + \gamma aa),$$

quod ergo debet esse quadratum, cujus radix jam ante est assignata, unde patet hanc formulam

$$m(a^4 + b^4) \pm (\gamma aa + \delta bb)$$

semper ad quadratum reduci posse, sive si omnia quadrata dividantur per divisorem $a^4 + b^4$, inter residua certe occurret tam $\gamma aa + \delta bb$ quam $-\gamma aa - \delta bb$. Sit $a = 3$ et $b = 2$ et quaeratur fractio $\frac{\alpha}{\beta}$ proxime aequalis ipsi $\frac{27}{2}$, erit $\alpha = 13$ et $\beta = 1$, hinc ergo erit $x = 97m \pm 47$. Potuissemus quoque facere $a = 2$ et $b = 3$, et fractio $\frac{\alpha}{\beta}$ proxime $= \frac{8}{3}$, quod fit sumendo $\alpha = 3$ et $\beta = 1$, tum erit $x = 97m \pm 33$. Patet ergo tam $47^4 + 1$ quam $33^4 + 1$ divisibile esse per 97.

A. m. T. II. p. 147.

---

## e) Diversa.

### 24.

(Krafft.)

Formulae in producendis numeris primis foecundae:

I. $x^2 + x + 17$ dat: 17, 19, 23, 29, 37, 47, 59, 73, 89, 107, 127, 149, 173, 199, 227, 257, 289.

II. $x^2 + x + 41$ dat: 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281.

Jam autem demonstratum est, nullam dari hujusmodi formulam algebraicam, cujus omnes plane termini sint numeri primi.

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

---

## 25.

(N. Fuss I.)

THEOREMA. Haec formula $x^{2n}+x^n+1$ semper est divisibilis per $xx+x+1$, dummodo $n$ non sit multiplum ternarii.

DEMONSTRATIO. Si enim illa formula multiplicetur per $x^n-1$, productum $x^{3n}-1$ semper est divisibile per $x^3-1$, ideoque etiam per $xx+x+1$; quia ergo multiplicator $x^n-1$ non est divisibilis, necesse est ipsam formulam esse divisibilem. Q. e. d.

THEOREMA. Haec formula $x^{4n}+x^{3n}+x^{2n}+x^n+1$ semper est divisibilis per $x^4+x^3+x^2+x+1$, dummodo exponens $n$ non fuerit multiplum ipsius 5.

DEMONSTRATIO similis praecedenti.

THEOREMA. Si capiatur angulus $\vartheta=\left(\frac{m}{n\pm1}\right)360^\circ$, haec formula $x^{2n}-2x^n\cos\vartheta+1$ semper est divisibilis per hanc $xx-2x\cos\vartheta+1$. A. m. T. I. p. 285.

## 26.

THEOREMA, cujus demonstratio etiamnunc desideratur. Si haec formula $4mnk+maa+nbb$ fuerit numerus primus, puta $P$, tum semper assignari possunt numeri $x$ et $y$, ut fiat $mxx+nyy=P$.

Sit $m=3$, $n=2$, $a=1$ et $b=1$, erit $maa+nbb=5$ et $4mnk+5=24k+5$. Sumatur $k=2$, erit $P=53$ et esse debebit $3xx+2yy=53$, sit $x=1$ et $y=5$. Plerumque quidem tales numeri pro $x$ et $y$ dantur integri, interdum tamen non nisi fractos assignare licet, veluti si fuerit $m=7$ et $n=2$, praeterea vero $a=1$ et $b=1$, ita ut sit $P=56k+9$, unde sumto $k=4$ fit $P=233$, qui numerus in integris esse nequit $=7xx+2yy$. At si capiatur $x=\frac{5}{3}$, erit $233=\frac{175}{9}+2yy$, ergo $2yy=\frac{1922}{9}$, ergo $y^2=\frac{961}{9}$ et $y=\frac{31}{3}$. A. m. T. I. p. 300.

## 27.

THEOREMA. Non dantur tria biquadrata, quorum summa esset divisibilis vel per 5, vel per 29, quae sola excipiuntur. A. m. T. II. p. 161.

## 28.

OBSERVATIO. Proposito quocunque numero primo $p=2n+1$, omnes numeri eo minores, qui sunt $1, 2, 3, 4 \ldots 2n$, semper tali ordine disponi possunt, ut certis multiplis ipsius $p$ aucti, progressionem geometricam constituant, sive tales assignari possunt numeri $x$, ut progressionis geometricae $1, x, x^2, x^3, x^4 \ldots$ si singuli termini per $p$ divisi deprimantur, omnes numeri ipso $p$ minores prodeant, uti ex sequentibus exemplis patebit. Notetur autem potestatem $x^{2n}$ hoc modo semper dare unitatem, propterea quod $x^{2n}-1$ semper per $p$ dividi potest, unde sequentes potestates $x^{2n+1}$, $x^{2n+2}$, $x^{2n+3}$, etc. eosdem reproducunt numeros, ut ab initio.

I. Sit $p=3$ et $n=1$ et progressio geometrica erit $1, x, xx$. Sumto ergo $x=2$, progressio geometrica erit 1, 2, 1, 2, 1, 2, 1, 2, etc.

II. Sit $p=5$ et $n=2$ et progressio geometrica $1, x, x^2, x^3$, etc. Hinc sumto $x=2$ habetur

1, 2, 4, 3, 1, 2, 4, 3, 1, etc.

sumto autem $x=3$, erit ea 1, 3, 4, 2, 1, 3, 4, 2, 1, etc.

III. Sit $p=7$ et $n=3$, erit progressio $1, x, x^2, x^3, x^4$, etc. Hinc sumto $x=2$, erit ea 1, 2, 4, unde patet, hinc tantum terminos pares oriri, unde $x$ ita sumi debet, ut fiat $xx-2=7m$, ideoque $x=3$ et progressio geometrica erit 1, 3, 2, 6, 4, 5, 1, 3, 2, etc. Loco $x$ autem etiam sumi posset alia potestas si modo $\lambda$ ad 6 fuerit primus, ita sumto $\lambda = 5$, capi poterit $x = 5$, unde oritur 1, 5, 4, 6, 2, 3, 1, quae est prioris retrograda. Semper autem series retrograda aeque satisfacit.

IV. Sit $p = 11$ et $n = 5$, at sumto $x = 2$ erit progressio

$$\begin{matrix} 1, & 2, & 4, & 8, & 5, & 10, & 9, & 7, & 3, & 6, & 1 \\ & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \end{matrix}$$

Hic autem primo etiam retrograda valet:

$$1,\ 6,\ 3,\ 7,\ 9,\ 10,\ 5,\ 8,\ 4,\ 2,\ 1.$$

Praeterea posito $x = x^3,\ x^7,\ x^9$, qui numeri sunt 8, 7 et 6, tum erit progressio:

$$1,\ 8,\ 9,\ 6,\ 4,\ 10,\ 3,\ 2,\ 5,\ 7,\ 1,$$

cujus retrograda oritur sumto $x = 7$.

V. Sit $p = 13$ et $n = 6$, at sumto $x = 2$, erit progressio

$$\begin{matrix} 1, & 2, & 4, & 8, & 3, & 6, & 12, & 11, & 9, & 5, & 10, & 7, & 1 \\ & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & \end{matrix}$$

Dein pro $x$ sumi possunt numeri 6, 11, 7. Sumto igitur $x = 6$, ea erit

$$1,\ 6,\ 10,\ 8,\ 9,\ 2,\ 12,\ 7,\ 3,\ 5,\ 4,\ 11,\ 1.$$

Reflexiones generales. 1. Perpetuo hic potestati $x^n$ conveniet numerus $2n$. Cum enim ejus quadratum $x^{2n}$ det 1, erit $x^n = \sqrt{1}$, ergo $x^n = -1 = p - 1 = 2n$.

2. Si potestati $x^\lambda$ respondeat numerus $a$, tum potestati $x^{n+\lambda}$ respondebit numerus $p - a = 2n + 1 - a$. Cum enim sit

$$x^\lambda = +a \text{ et } x^n = -1, \text{ erit } x^{\lambda+n} = -a = p - a = 2n + 1 - a.$$

Sufficit ergo seriem usque ad medium $2n$ continuare, quia sequentes sunt complementa priorum.

3. Posito $x = a$, ejus reciprocum vocemus $\frac{1}{a}$, sive $\frac{mp+1}{a}$, ut prodeat numerus integer, quem designemus per $\alpha$, ut sit $\alpha = \frac{1}{a}$, eodemque modo $\beta = \frac{1}{b}$, $\gamma = \frac{1}{c}$ etc. Ita casu $p = 13$, si fuerit

$$a = 2,\ 3,\ 4,\ 5,\ 6,\ 7, \text{ etc.}$$
$$\text{erit } \alpha = 7,\ 9,\ 10,\ 8,\ 11,\ 2.$$

Notetur enim complementorum reciproca etiam esse complementa.

4. Constitutis his reciprocis, si fuerit $x^\lambda = a$, tum erit $x^{2n-\lambda} = \alpha$, propterea quod productum potestatum est $x^{2n} = 1$, ideoque $a\alpha = 1$. Deinde vidimus esse $x^{n+\lambda} = p - a$, erit igitur $x^{n-\lambda} = p - \alpha$, ita ut, cognito uno termino, simul quatuor innotescant, quod exemplis illustretur.

Sit $p = 19$, $n = 9$.

| potestates | numeri | potestates | numeri |
|---|---|---|---|
| 1 | 1 | $x^9$ | 18 |
| $x^1$ | $a$ | $x^{10}$ | $19 - a$ |
| $x^2$ | $b$ | $x^{11}$ | $19 - b$ |
| $x^3$ | $c$ | $x^{12}$ | $19 - c$ |
| $x^4$ | $d$ | $x^{13}$ | $19 - d$ |
| $x^5$ | $p - \delta$ | $x^{14}$ | $\delta$ |
| $x^6$ | $p - \gamma$ | $x^{15}$ | $\gamma$ |
| $x^7$ | $p - \beta$ | $x^{16}$ | $\beta$ |
| $x^8$ | $p - \alpha$ | $x^{17}$ | $\alpha$ |

Hic igitur notetur esse debere $b = a^2$, $c = a^3$, $d = a^4$, etc. Si ergo sumatur $a = 2$, erit $b = 4$, $c = 8$, $d = 16$, tum vero $\alpha = 10$, $\beta = 5$, $\gamma = 12$, $\delta = 6$, unde formatur haec progressio geometrica

*

1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17

Loco $x$ autem quoque sumi possunt numeri potestati $x^{\lambda}$ respondentes, si modo $\lambda$ ad 18 fuerit primus. Cum autem $18 = 2.3^2$, multitudo numerorum ad 18 primorum est 6 et valores pro $\lambda$ sunt 1, 5, 7, 11, 13, 17, unde pro $x$ sumi possunt hi numeri 2, 13, 14, 10, 3, 15, unde sex progressiones geometricas formare licet, quarum tres erunt priorum retrogradae.

Exemplum. Sit $p = 41$ et $n = 20$, et sumatur $x = 2$, unde progressio geometrica oritur

1, 2, 4, 8, 16, 32, 23, 5, 10, 20, 40
1 2 3 4 5 6 7 8 9 10

unde pro $x^{20}$ prodit $+1$, ita ut sit $2^{20} = +1$, unde patet esse $xx = 2$, ideoque $x = \sqrt{(2 + 41m)} = 17$ (posito $m = 7$). Factum hinc est sequens schema:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 41) | 0 | 1 | | | | | | |
| | 1 | 17 | 11 | 11 | 21 | 23 | 31 | 30 |
| | 2 | 2 | 12 | 23 | 22 | 39 | 32 | 18 |
| | 3 | 34 | 13 | 22 | 23 | 7 | 33 | 19 |
| | 4 | 4 | 14 | 5 | 24 | 37 | 34 | 36 |
| | 5 | 27 | 15 | 3 | 25 | 14 | 35 | 38 |
| | 6 | 8 | 16 | 10 | 26 | 33 | 36 | 31 |
| | 7 | 13 | 17 | 6 | 27 | 28 | 37 | 35 |
| | 8 | 16 | 18 | 20 | 28 | 25 | 38 | 21 |
| | 9 | 26 | 19 | 12 | 29 | 15 | 39 | 29 |
| | 10 | 32 | 20 | 40 | 30 | 9 | 40 | 1 |

Jam ad 40 valores ipsius $\lambda$ primi sunt 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, unde pro $x$ accipi poterunt sequentes numeri: 17, 34, 13, 26, 11, 22, 6, 12, 24, 7, 28, 15, 30, 19, 35, 29.
Si sumsissemus $x = 3$, prodiisset progressio

1, 3, 9, 27, 40,
1 2 3 4

sequeretur $3^4 = x^{20}$, ergo $3 = x^5$. Supra autem invenimus esse $2 = x^2$, ergo $4 = x^4$, unde oritur $x = \frac{3}{4}$, sive $x = \frac{3 + 41m}{4} = 11$. Cum igitur formula $a^{40} - 1$ semper dividi queat per 41 h. e. si fuerit $a = x^{\lambda}$, denotante $\lambda$ numero quocunque, ista formula $b^{20} - 1$ dividi poterit per 41, si fuerit $b = aa$, h. e. si fuerit $b = x^{2\lambda}$. Quoniam igitur $a^{40} - 1 = (a^{20} - 1)(a^{20} + 1)$, prior vero factor $a^{20} - 1$ divisibilis sit casibus $a = x^{2\lambda}$, sequitur reliquis casibus, h. e. casibus $a = x^{2\lambda + 1}$, formulam $a^{20} + 1$ divisibilem esse per 41, h. e. si fuerit

$a = 17,\ 34,\ 27,\ 13,\ 26,\ 11,\ 22,\ 3,\ 6,\ 12,\ 24,\ 7,\ 14,\ 28,\ 15,\ 30,\ 19,\ 38,\ 35,\ 29.$

Porro quia $a^{20} - 1$ divisibile per 41 si $a = x^{2\lambda}$, erit $b^{10} - 1$ divisibile per 41 si $b = x^{4\lambda}$; hinc sequitur formulam $b^{10} + 1$ divisibilem esse per 41 si $b = x^{4\lambda + 2}$. Porro $a^8 - 1$ divisibile per 41 si $a = x^{5\lambda}$. At $a^4 - 1$ divisibile per 41 si $a = x^{10\lambda}$, ergo $a^4 + 1$ divisibile per 41 si $a = x^5$, $x^{15}$, $x^{25}$, $x^{35}$, etc. h. e. si $a = x^{10\lambda + 5}$. Consequenter formula $a^4 + 1$ divisibilis per 41 his casibus: $a = 27$, 3, 14, 38. Porro quia $a^4 - 1$ divisibile per 41, si $a = x^{10\lambda}$, et $a^2 - 1$ per 41, si $a = x^{20\lambda}$, sequitur fore $a^2 + 1$ divisibile per 41, si $a$ fuerit $x^{20\lambda + 10}$, qui casus sunt $a = 32$ et 9, hoc est in genere si $a = 41m \pm 9$. A. m. T. II. p. 170. 171.

## 29.

Regula facilis explorandi numeros formae $4m + 1$, qui desinunt vel in 3, vel in 7, utrum sint primi, nec ne?

Sit $N$ talis numerus, et a $2N$ subtrahatur quadratum proxime minus, desinens in 5, cujus radix sit $5n$, sitque residuum $= R$. Ad hoc continuo addantur numeri $100(n - 1)$, $100(n - 3)$, $100(n - 5)$, $100(n - 7)$, etc.

ut prodeant sequentes numeri: $R$, $R+100(n-1)$, $R+200(n-2)$, $R+300(n-3)$, etc. Quodsi jam inter hos numeros unicus occurrat quadratus, tum numerus propositus $N$ certo est primus, vel per hoc quadratum divisibilis, sin autem vel nullus occurrat quadratus, vel duo pluresve, tum numerus $N$ non est primus. Sit $N=637$, erit $2N=1274$. Proximum quadratum in 5 desinens erit $1225=5^2.7^2$, ideoque $n=7$ et numeri addendi numero $R=49$ erunt 600, 400, 200, unde prodit 649, 1049, 1249, inter quos numeros unicum occurrit quadratum 49, unde numerus propositus vel erit primus, vel per 49 divisibilis.

Sit $N=1073$, erit $2N=2146$; proximum quadratum in 5 desinens $=2025=5^2.9^2$, unde $n=9$ et $R=121$. Numeri addendi sunt 800, 600, 400, 200 eritque 921, 1521, 1921, 2121; inter quos sunt quadrata 121 et 1521, ideoque numerus non est primus.

Sit $N=697$, $2N=1394$; proximum quadratum in 5 desinens $1225=5^2.7^2$, $R=169$ et numeri addendi 600, 400, 200; inde prodeunt 769, 1169, 1369. Hic duo occurrunt quadrata $169=13^2$ et $1369=37^2$, unde numerus ille non est primus, est enim $697=17.41$.

Sit $N=1697$, erit $2N=3394$, proximum quadratum $3025=5^2.11^2$, hinc $R=369$ et numeri addendi 1000, 800, 600, 400, 200; hinc prodeunt 1369, 2169, 2769, 3169, 3369, inter quos unicum est quadratum $1369=37^2$, unde numerus est primus, quandoquidem per 1369 non est divisibilis.

A. m. T. II. p. 188.

## 30.

(Golovin.)

Tabula exhibens per intervallum 420 omnes numeros, qui restant, deletis numeris sequentium formarum: $3n+2$, $4n+3$, $5n+1$, $5n+4$, $7n+3$, $7n+5$ et $7n+6$.

| | | | | | |
|---|---|---|---|---|---|
| 0 | 78 | 148 | 232 | 310 | 373 |
| 18 | 85 | 162 | 238 | 312 | 378 |
| 22 | 88 | 165 | 240 | 322 | 382 |
| 25 | 93 | 168 | 252 | 330 | 385 |
| 28 | 100 | 172 | 253 | 333 | 393 |
| 30 | 102 | 177 | 268 | 337 | 400 |
| 37 | 105 | 190 | 270 | 340 | 403 |
| 42 | 112 | 193 | 273 | 345 | 408 |
| 57 | 120 | 205 | 277 | 350 | 417 |
| 58 | 130 | 210 | 280 | 352 | 420 |
| 60 | 133 | 217 | 282 | 357 | |
| 70 | 142 | 225 | 288 | 358 | |
| 72 | 145 | 228 | 298 | 372 | |

A. m. T. II. p. 195.

## 31.

(N. Fuss I.)

### Theoremata numerica.

NB. Denotet hoc signum :: divisibile, ita ut $a :: p$ denotet, numerum $a$ per $p$ esse divisibilem.

Theorema fundamentale, a me olim demonstratum. Proposito numero quocunque $P$, atque ab 1 usque ad $P$ reperiantur $\pi$ numeri ad $P$ primi, qui scilicet cum eo praeter unitatem nullum habeant factorem communem: tum semper $(a^\pi - 1) :: P$. Hinc fluunt sequentia theoremata:

I. Si fuerit $p$ numerus primus, cum semper sit $(a^p - a) :: p$; si fuerit $a=b^p$ erit $(a^p-a) :: p^2$. At si fuerit $a=b^{pp}$, erit $(a^p-a) :: p^3$. Et in genere si $a=b^{p^n}$ erit $(a^p-a) :: p^{n+1}$.

II. Si $p$, $q$, $r$, $s$ etc. fuerint primi inter se diversi, fueritque $a = b^{q-1}$, erit $(a^p - a) :: pq$. Porro, si $a = b^{(q-1)(r-1)}$ 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 $\Delta$ tum etiam $(x^\Delta - y^\Delta) :: P$.

Demonstratio. Ponatur $m = \mu\Delta$ et $n = \nu\Delta$, et quia $\Delta$ est maximus communis divisor, erunt $\mu$ et $\nu$ primi inter se. Dari igitur poterunt numeri $\alpha$ et $\beta$, 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 $N - ab = \Delta p + \Delta(p - a + b) + \Delta r$, 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