De divisore $3(2p+1)=d$.

533. Multitudo numerorum hoc divisore minorum et ad eum primorum est $=2.2p=4p$, inter quos duo ad minimum sunt, quorum quadrata idem residuum relinquunt, scilicet a^2 et $(d-a)^2$, unde numerus diversorum residuorum major quam $2p$ esse nequit.

534. Praeterea vero cum a per 3 non sit divisibile, vel $2p+1-2a$, vel $2(2p+1)-2a$ per 3 erit divisibile, sit quotus $=m$, et quadratum numeri $3m+a$ idem relinquet residuum, ergo vel $2p+1-a$, vel $2(2p+1)-a$, indeque praeterea vel $2(2p+1)+a$, vel $2p+1+a$ idem quoque residuum relinquet.

535. Hoc modo cum semper quaterna quadrata idem dent residuum, numerus residuorum diversorum erit tantum $=p$, ideoque idem ac pro divisore $2p+1$. In residuis autem nequit esse ullus numerus formae $3n-1$, cum nullum quadratum, tali numero minutum, per 3, neque ergo per $3(2p+1)$ dividi queat.

536. Omnia ergo residua divisoris $3(2p+1)$ erunt numeri formae $3n+1$, et si residua divisoris $2p+1$ sint $1, \alpha, \beta, \gamma$, etc. quodlibet vel ipsum, vel numero $2p+1$, vel $2(2p+1)$ auctum, quo prodeat numerus formae $3n+1$, erit residuum divisoris $3(2p+1)$.

Pro divisore $(2p+1)(2q+1)=d$.

537. Sint pro divisore $2p+1$ residua $1, \alpha, \beta, \gamma, \delta$, etc. numero $=p$, et pro divisore $2q+1$ residua $1, \pi, \varrho, \sigma, \tau$, etc. numero $=q$, ac numeri utrique ordini communes erunt residua divisoris $d=(2p+1)(2q+1)$.

538. At ad priorem ordinem pertinere censendus est numerus $m(2p+1)+\alpha$, ubi m ita potest definiri, ut fiat aequalis vel $n(2q+1)+1$, vel $n(2q+1)+\pi$, etc., sicque ex quovis residuo divisoris $2p+1$ producuntur q residua divisoris $2q+1$, sicque omnino pq residua diversa pro divisore $(2p+1)(2q+1)$ obtinentur.

539. Sit hujusmodi divisor compositus $5.7=35$, et cum sint residua pro divisore 5 haec duo 1, 4, et pro 7 haec tria 1, 2, 4; ergo pro divisore 35 residua erunt $7n+1$, $7n+2$, $7n+4$, quae scilicet vel in forma $5m+1$, vel $5m+4$ continentur. Erunt ergo haec residua numero sex: 1, 29; 9, 16; 4, 11.

540. Cum pro divisore $(2p+1)(2q+1)$ tantum dentur pq residua diversa, quaterna quadrata idem praebebunt residuum, quorum unum si sit $=aa$, reliquorum trium radices erunt:

$$(2p+1)(2q+1)-a, \quad m(2p+1)-a, \quad n(2p+1)+a,$$

sumendis numeris m et n ita, ut $m(2p+1)-2a$ et $n(2p+1)+2a$ dividi queant per $2q+1$, quod ob $2p+1$ et $2q+1$ primos inter se, semper fieri potest, ut m et n sint minores quam $2q+1$.

Caput XV.

De divisoribus numerorum formae $xx+yy$.

541. Hinc primo excludo casus, quibus numeri x et y habent communem divisorem; si enim maximus communis divisor esset $=\varphi$ et $x=p\varphi$ et $y=q\varphi$, ut p et q forent primi inter se, haberetur $xx+yy=(pp+qq)\varphi\varphi$, et inventio divisorum reduceretur ad formam $pp+qq$.

542. Sint ergo x et y primi inter se, atque evenire potest, ut $xx+yy$ fiat numerus primus, cui probando vel unicus casus sufficeret, quorum simplicissimus est 2. Ut autem $xx+yy$ fiat numerus primus, statim excluduntur casus, quibus ambo numeri x et y sunt impares.

543. Ponatur ergo alter par, alter impar, et evidens est omnes numeros primos $xx+yy$ in hac forma $4n+1$ contineri debere, sicque nullus numerus formae $4n-1$ duorum quadratorum summa esse potest.

544. Sin autem x et y sint numeri impares, seu $x=2p+1$ et $y=2q+1$, fieri poterit ut semissis $\frac{xx+yy}{2}=2pp+2p+2qq+2q+1$ fiat numerus primus. At est

$$2pp+2p+2qq+2q+1=(p+q+1)^2+(p-q)^2,$$

iterum summa duorum quadratorum, quorum alterum par, alterum impar, ob summam radicum $2p+1$ imparem.

545. Si summa duorum quadratorum $aa+bb$ per aliam summam duorum quadratorum $cc+dd$ multiplicetur, productum $(aa+bb)(cc+dd)$ iterum erit summa duorum quadratorum, cum sit $=(ac\pm bd)^2+(ad\mp bc)^2$, quod ob ambiguitatem signi duplici modo evenire potest.

546. Hic inversa propositio se offert: si summa duorum quadratorum $pp+qq$ divisionem admittat per summam duorum quadratorum $aa+bb$, fore etiam quotum duorum quadratorum summam, cujus veritas autem inde non sequitur, sed peculiarem demonstrationem requirit.

547. Ad hoc demonstrandum primum animadverto formam $pp+qq$ per $aa+bb$ esse divisibilem; quanticunque sint numeri p et q, semper eos reduci posse ad numeros minores quam $aa+bb$, atque adeo quam $\frac{1}{2}(aa+bb)$, cum si $pp+qq$ sit divisibile per $aa+bb$, etiam

$$(\pm\alpha(aa+bb)\pm p)^2+(\pm\beta(aa+bb)\pm q)^2$$

divisibile evadat.

548. At si $\frac{pp+qq}{aa+bb}$ sit summa duorum quadratorum $cc+dd$, seu $p=ac+bd$ et $q=ad-bc$, sumendo $p=ac+bd+\alpha(aa+bb)$ et $q=ad-bc+\beta(aa+bb)$, tum $pp+qq$ utique per $aa+bb$ divisionem admittet, eritque quotus

$$=cc+dd+2\alpha(ac+bd)+2\beta(ad-bc)+(\alpha\alpha+\beta\beta)(aa+bb),$$

qui etiam est summa duorum quadratorum $(c+\alpha a-\beta b)^2+(d+\alpha b+\beta a)^2$.

549. Verum haec altius sunt petenda; dico ergo primo, si divisor $aa+bb$ sit numerus primus, per quem forma $pp+qq$ sit divisibilis, quotum esse summam duorum quadratorum; quod etsi in genere verum est, existente $aa+bb$ etiam numero composito, tamen demonstratio ab hoc casu derivanda videtur.

550. Cum a et b sint numeri primi inter se, ad eos p ita referri potest, ut sit $p=ma-nb$, idque infinitis modis, jam si esset $q=na+mb$, foret utique $\frac{pp+qq}{aa+bb}=mm+nn$; at si non sit $q=na+mb$, ponatur $q=na+mb+s$, eritque

$$pp+qq=(aa+bb)(mm+nn)+2s(na+mb)+ss.$$

551. Cum ergo $2s(na+mb)+ss$ sit divisibile per $aa+bb$, vel s, vel $s+2(na+mb)$ divisibile sit necesse est. Priori casu ponatur $s=t(aa+bb)$, erit

$$\frac{pp+qq}{aa+bb} = mm + nn + t\,(t\,(aa+bb) + 2\,(na+mb))$$
$$= mm + 2mbt + ttbb + nn + 2nat + aatt = (m+bt)^2 + (n+at)^2,$$

ideoque summa duorum quadratorum.

552. Altero casu ponatur $s + 2\,(na+mb) = t\,(aa+bb)$, erit $s = t\,(aa+bb) - 2\,(na+mb)$, ideoque $\frac{pp+qq}{aa+bb} = mm + nn + tt\,(aa+bb) - 2t\,(na+mb) = (m-bt)^2 + (n-at)^2$, ita ut utroque casu quotus sit summa duorum quadratorum.

553. Si ergo $pp+qq$ sit divisibile per numerum primum $aa+bb$, demonstratum est quotum esse quoque summam duorum quadratorum. Hinc si quotus non esset summa duorum quadratorum, divisor non foret numerus primus formae $aa+bb$, hoc est, vel si esset primus, non esset formae $aa+bb$, vel si esset formae $aa+bb$, non esset primus; vocabula autem quoti et divisoris inter se permutare licet.

554. Denotent, brevitatis gratia, litterae A, B, C, D, etc. numeros primos formae $aa+bb$, et si summa duorum quadratorum $pp+qq$ divisibilis sit per talium numerorum productum ABC, quotus quoque erit summa duorum quadratorum. Est enim $\frac{pp+qq}{A} = rr+ss$, tum vero

$$\frac{rr+ss}{B} = tt+uu, \quad \text{atque} \quad \frac{tt+uu}{C} = xx+yy, \quad \text{unde fit} \quad \frac{pp+qq}{ABC} = xx+yy.$$

555. Si ergo summa duorum quadratorum $pp+qq$ divisibilis esset per numerum non-summam duorum quadratorum, quotus, si esset primus, non foret summa duorum quadratorum, et si esset compositus, non foret productum ex talibus numeris primis, qui singuli essent summae duorum quadratorum.

556. Quare si summa duorum quadratorum $pp+qq$ unum habeat factorem, qui non sit summa duorum quadratorum, inter reliquos factores primos ad minimum unus, qui etiam non sit summa duorum quadratorum, reperiatur necesse est.

557. Nunc igitur investigemus, an summa duorum quadratorum $pp+qq$ inter se primorum per ullum numerum $\mathfrak{A}$, qui non sit summa duorum quadratorum, divisibilis esse queat. Ad hoc sumamus $pp+qq$ divisibile esse per talem numerum $\mathfrak{A}$, atque etiam $(p-m\mathfrak{A})^2 + (q-n\mathfrak{A})^2$ divisibile erit per $\mathfrak{A}$ (*).

558. Poterit ergo talis summa duorum quadratorum $pp+qq$ exhiberi, quorum radices p et q minores sint quam $\mathfrak{A}$, quin etiam minores quam $\frac{1}{2}\mathfrak{A}$; cum etiam $(\mathfrak{A}-p)^2 + (\mathfrak{A}-q)^2$ divisionem admittere debeat, quorum quadratorum radices minores erunt quam $\frac{1}{2}\mathfrak{A}$; si p et q eo essent majores.

559. Dabitur ergo summa duorum quadratorum $pp+qq$ minor quam $\frac{1}{2}\mathfrak{A}\mathfrak{A}$ (cum sit $p < \frac{1}{2}\mathfrak{A}$ et $q < \frac{1}{2}\mathfrak{A}$) per numerum $\mathfrak{A}$ divisibilis; ponatur quotus $= \mathfrak{B}$, qui etiam vel ipse non erit summa duorum quadratorum, vel factorem talem habebit, eritque $\mathfrak{B} < \frac{1}{2}\mathfrak{A}$.

560. Cum jam $pp+qq$ divisibile sit per $\mathfrak{B}$, exhiberi poterit summa duorum quadratorum $rr+ss$ minor quam $\frac{1}{2}\mathfrak{B}\mathfrak{B}$, divisibilis per $\mathfrak{B}$, et quotus $\mathfrak{C}$, qui erit minor quam $\frac{1}{2}\mathfrak{B}$, pariter non erit summa duorum quadratorum, per quem cum divisibilis sit $rr+ss$, dabitur $tt+uu < \frac{1}{2}\mathfrak{C}\mathfrak{C}$ divisibilis per $\mathfrak{C}$, et quotus $\mathfrak{D} < \frac{1}{2}\mathfrak{C}$ itidem non erit summa duorum quadratorum.

(*) *Script. ad marg.* Quorum radices, si p et q sint primi inter se, etiam erunt primae inter se.

561. Hoc modo tandem pervenietur ad summam duorum quadratorum quantumvis parvam, quae foret divisibilis per numerum non-summam duorum quadratorum, quod cum sit absurdum, necessario sequitur, summam duorum quadratorum inter se primorum non esse divisibilem per ullum numerum, qui ipse non sit summa duorum quadratorum.

562. Proposito autem numero primo quocunque formae $4n+1$, quia inter residua quadratorum est -1, vel $4n$, semper summa duorum quadratorum per eum divisibilis exhiberi potest, unde sequitur omnes numeros primos formae $4n+1$ esse summas duorum quadratorum.

563. Deinde cum numeri formae $4n-1$ nunquam esse possint summae duorum quadratorum, nulla summa duorum quadratorum inter se primorum per ullum talem numerum $4n-1$ divisibilis esse potest.

564. Desideratur autem demonstratio succinctior, qua probetur, si summa duorum quadratorum $pp+qq$ divisibilis fuerit per summam duorum quadratorum $aa+bb$, quotum necessario quoque esse summam duorum quadratorum, quod sequenti ratiocinio perficere tentemus.

565. In divisore $aa+bb$ numeros a et b inter se primos assumere licet; si enim non essent primi inter se, sublatione communis factoris tales redderentur; erit ergo $aa+bb$ tam ad a quam ad b primus. Unde quicunque numeri fuerint p et q, ii ita repraesentari poterunt

$$p = m(aa+bb) \pm fa \quad \text{et} \quad q = n(aa+bb) \pm gb,$$

id quod infinitis modis fieri potest.

566. Cum igitur $pp+qq$ sit divisibile per $aa+bb$, etiam $ffaa+ggbb$ per $aa+bb$ erit divisibile, atque ob illas infinitas resolutiones, omnes casus, quibus $ffaa+ggbb$ per $aa+bb$ divisibile evadit, prodire debent, ergo etiam casus $g=f$ prodeat necesse est, quoniam hoc divisio succedit. (*)

---

567. Hoc concesso habebimus $p = m(aa+bb) \pm fa$ et $q = n(aa+bb) \pm fb$; unde fit

$$\frac{pp+qq}{aa+bb} = \begin{cases} mm(aa+bb) \pm 2fma \\ nn(aa+bb) \pm 2fnb \end{cases} + ff,$$

quae expressio est $= (f \pm ma \pm nb)^2 + (\pm na \mp mb)^2$, ideoque summa duorum quadratorum.

568. Hinc ergo statim sequitur, si quotus non sit summa duorum quadratorum, neque divisorem talem esse posse, neque ergo productum ex duobus numeris, quorum alter est summa duorum quadratorum, alter secus, summa duorum quadratorum esse potest.

569. Conjunctis cum hisce, quae ante § 558 et seqq. sunt proposita, evincitur summam duorum quadratorum inter se primorum nullos habere divisores, nisi qui ipsi sint summae duorum quadratorum, tum vero omnes numeros primos formae $4n+1$ esse summas duorum quadratorum.

(*) *Script. ad marg.* Hic dubium esse potest, an casus $g=f$ necessario ex divisibilitate formulae $pp+qq$ sequatur. Hoc dubium est fundatum, nam sit

$$a=7,\ b=4,\ p=17,\ q=6, \quad \text{erit} \quad aa+bb=65,\ pp+qq=325;$$

fieri autem nequit $17 = 65m \pm 7f$ simul $6 = 65n \pm 4f$, unde haec posterior demonstratio rejicienda. $\frac{17^2+6^2}{7^2+4^2} = 1^2+2^2$, etsi nullo modo sit $17 = 1.7 \pm 2.4$, vel $17 = 2.7 \pm 1.4$.

570. Si numerus quispiam N duplici modo est summa duorum quadratorum, scilicet

$$N = aa + bb = cc + dd,$$

tum non est primus. Cum enim sit $aa - cc = dd - bb$, erit $d + b = \frac{m(a+c)}{n}$ et $d - b = \frac{n(a-c)}{m}$, unde $b = \frac{m(a+c)}{2n} - \frac{n(a-c)}{2m}$, hinc

$$N = aa + bb = \frac{(mm+nn)}{4mmnn}(nn(a-c)^2 + mm(a+c)^2) = \frac{(mm+nn)}{4mm}((a-c)^2 + (b+d)^2),$$

ubi denominatoris factorem tollere nequit. (*)

Caput XVI.

De divisoribus numerorum formae $xx + 2yy$.

571. Sumtis x et y inter se primis, vel ambo sunt impares, vel alteruter tantum par, ergo vel x, vel y erit par; ex quo tres resultant casus considerandi, qui cujusmodi numeros ratione paritatis et imparitatis praebeant, investigasse juvabit.

572. Si ambo numeri x et y sint impares, eorum quadrata sunt numeri formae $8n + 1$, fietque $xx + 2yy$ numerus formae $8n + 3$; sin autem x impar et y par, ob

$$xx = 8m + 1 \quad \text{et} \quad 2yy = 2.4n,$$

fiet $xx + 2yy$ numerus formae $8n + 1$.

573. Si x sit par et y impar, ponatur $x = 2z$, et fiet $xx + 2yy = 2(2zz + yy)$; jam cum y sit impar, prout z fuerit vel par, vel impar, erit vel

$$xx + 2yy = 2(8n + 1), \quad \text{vel} \quad xx + 2yy = 2(8n + 3).$$

574. Omnes ergo numeri in forma $xx + 2yy$ contenti, dum x et y sunt primi inter se, vel saltem non ambo pares, si fuerint impares, pertinebunt vel ad formam $8n + 1$, vel ad $8n + 3$; sin autem illi numeri sint pares, vel ad formam $2(8n + 1)$, vel ad $2(8n + 3)$ erunt referendi, et casu hoc posteriori eorum semisses, scilicet $2zz + yy$ sunt etiam numeri formae $xx + 2yy$.

575. Numeri ergo impares, qui sunt vel formae $8n + 5$, vel formae $8n + 7$, certe non sunt numeri formae $xx + 2yy$, neque etiam dupla earum formarum in hac continentur, unde infiniti dantur numeri in forma $xx + 2yy$ non contenti.

576. Productum autem duorum numerorum hujus formae in eadem forma continentur; est enim $(aa + 2bb)(cc + 2dd) = (ac \pm 2bd)^2 + 2(ad \mp bc)^2$, unde simul patet talia producta duplici modo in ista forma contineri.

577. Jam demonstrandum est, si numerus $pp + 2qq$ dividi queat per $aa + 2bb$, fore quotum

(*) *Script. ad marg.* $(a+c)(a-c) = (b+d)(d-b) = pqrs$, $a+c = pq$, $a-c = rs$, $b+d = pr$, $d-b = qs$; $a = \frac{pq+rs}{2}$, $b = \frac{pr-qs}{2}$, $aa+bb = \frac{1}{4}(pp+ss)(qq+rr)$.