Werk

Titel: De residuis cubicis commentatio numerosa.

Autor: Jacobi, J.G.D.

Jahr: 1827

PURL: https://resolver.sub.uni-goettingen.de/purl?243919689_0002|log11

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

7.

De residuis cubicis commentatio numerosa.

(Auct. Dr. *J. G. D. Jacobi* Regiom.)

1.

Theorema fundamentale de residuis quadraticis postquam pluribus demonstrationibus egregiis comprobaverat, Cl. Gaufs, iam ex longo temporis intervallo, de residuis cubicis et biquadraticis quaestionem moverat, nec non quae ea de re theoremata struxerit, communicaturum se cum arithmeticis pollicitus est. Ante biennium fere Vir ille Clarissimus commentationem primam de residuis biquadraticis conscriptam societati Gottingensi tradidit, quae tamen diu desiderata nondum lucem vidit. Quam ne nimis graviter ferant arithmetici moram, ipse praecipua, quae ibi adornaverat, theoremata iam tum temporis publici iuris facere voluit (vid. *Göttinger gelehrte Anzeiger Vol. I. A.* 1725.). Versari comperimus ea theoremata cum in aliis rebus gravissimis tum in explorandis indiciis, quibus cognoscatur, numerum 2 dati numeri primi esse residuum biquadraticum. Equidem dum ad egregia Viri inventa probe intelligenda animum bene praeparatum esse volebam, hisce quaestionibus intentus casu, ut fit, in methodum satis generalem incidi, cuius ope plurima de residuis dignitatum theoremata investigare, vel undecunque cognita comprobare posse mihi videor. Cuius ope eruta de residuis cubicis theoremata fundamentalia arithmeticis iam proponam.

2.

Quaestio de residuis dignitatum gravissima in eo maxime versatur, ut proposito numero q omnes numeri primi p formae $\lambda n + 1$ assignandi sint tales, ut congruentia $x^\lambda \equiv q \pmod{p}$ resolvi queat, sive, quod idem est, ut sit $q^{\frac{p-1}{\lambda}} \equiv 1 \pmod{p}$; quo casu dicetur, numerum q esse residuum λ^{tae} dignitatis, respectu numeri primi p. Sit $\lambda = 3$ sive p formae $3n+1$, notum est (v. Disquis. Ar., Sectio ult.), semper eiusmodi numeros L, M eosque unico tantum modo assignari posse, ut sit $LL+27MM=4p$. Numerum q in theorematibus fundamentalibus pro-

ponendis et ipsum primum statuemus; distinguendum autem nobis est inter casum, quo q erit formae $6n+1$, et casum, quo q formae $6n-1$. Casu primo, quo q formae $6n+1$, notum est, semper resolvi posse congruentiam $xx+3 \equiv 0 \pmod{q}$. Quibus positis, proponamus theorema sequens genuina forma, qua inventum est — varie enim transformare licet hoc et alterum —:

Theorema I. „Sint et p et q numeri primi formae $6n+1$, sit $4p = LL + 27MM$, sit porro $xx+3 \equiv 0 \pmod{q}$: erit q residuum cubicum, respectu numeri primi p, quoties $\frac{p(L+3Mx)}{2}$ sive etiam $\frac{L+3Mx}{L-3Mx}$ residuum cubicum respectu numeri primi q; sin minus, non erit."

3.

Altero casu, quo q formae $6n-1$, theorema fundamentale longius repetendum erit. Eo enim casu confugiendum est ad theoriam prorsus novam, nempe ad considerationem radicum imaginariarum congruentiarum. Casu nostro, quo q formae $6n-1$, notum est, congruentiam $x^{q+1} \equiv 1 \pmod{q}$ duas tantum habere radices reales ± 1, at reliquas, quarum $p-1$ numerus, sub forma imaginaria $a+b\sqrt{-3}$, ubi $aa+3bb \equiv 1 \pmod{q}$ assignare licet omnes. Nec non inter eas rursus radices primitivas distinguere licet, quarum idem numerus est atque numerorum numero $q+1$ minorum et ad ipsum $q+1$ primorum. De quibus et ipsis valet, quod de radicibus primitivis vulgo dictis, ut radices congruentiae omnes tamquam unius radicis primitivae dignitates repraesentari possint. Modum eiusmodi congruentiae radices exhibendi expeditissimum alibi tradam; adnotabo tantummodo, ubi $q+1 = mn$, atque r radix primitiva congruentiae $x^{q+1} \equiv 1 \pmod{q}$, fieri congruentiae $x^m \equiv 1 \pmod{q}$ radices: $1, r^n, r^{2n}, r^{3n}, \ldots, r^{(m-1)n}$.

Jam omnes radices congruentiae $x^{\frac{q+1}{3}} \equiv 1 \pmod{q}$, quippe qui sunt cubi radicum congruentiae $x^{q+1} \equiv 1 \pmod{q}$, denominemus in sequentibus residua cubica numeri primi q. Quibus positis, theorema sequens enuntiare licet.

Theorema II. „Sit p numerus primus formae $6n+1$, atque $4p = LL + 27MM$; sit porro q numerus primus formae $6n-1$: erit q residuum cubicum numeri primi p, quoties est $\frac{L+M\sqrt{-3}}{L-M\sqrt{-3}}$ residuum cubicum numeri primi q; sin minus, non erit."

3.

Haec duo theoremata fundamentalia tamquam primae lineae theoriae residuorum cubicorum amplissimae consideranda sunt. Eorum ope adornari poterit tabula, cuius initium hic exhibemus:

q	Congruentiae conditionales respectu moduli q, ut sit q R.C. moduli p; $(4p=LL+27MM)$			
2	$M\equiv 0$			
3	$M\equiv 0$			
5	$L\equiv 0$; $M\equiv 0$			
7	$L\equiv 0$; $M\equiv 0$			
11	$L\equiv 0$; $M\equiv 0$;	$L\equiv\pm 4M$		
13	$L\equiv 0$; $M\equiv 0$;	$L\equiv\pm M$		
17	$L\equiv 0$; $M\equiv 0$;	$L\equiv\pm 3M$		
		$L\equiv\pm 9M$		
19	$L\equiv 0$; $M\equiv 0$;	$L\equiv\pm 3M$		
		$L\equiv\pm 9M$		
23	$L\equiv 0$; $M\equiv 0$;	$L\equiv\pm 8M$;	$L\equiv\pm 2M$	
		$L\equiv\pm 11M$		
29	$L\equiv 0$; $M\equiv 0$;	$L\equiv\pm M$;	$L\equiv\pm 11M$	
		$L\equiv\pm 2M$	$L\equiv\pm 13M$	
31	$L\equiv 0$; $M\equiv 0$;	$L\equiv\pm 5M$;	$L\equiv\pm 6M$	
		$L\equiv\pm 7M$	$L\equiv\pm 11M$	
37	$L\equiv 0$; $M\equiv 0$;	$L\equiv\pm 3M$;	$L\equiv\pm 7M$;	$L\equiv\pm 8M$
		$L\equiv\pm 9M$	$L\equiv\pm 12M$	
		etc.	etc.	

Ubi e congruentiis, quas conditionales diximus, una aliqua locum habet, erit q residuum cubicum numeri primi p; sin minus, non erit. Congruentias eas, quarum numerus $\frac{q\pm 1}{3}$, ita disposuimus, ut binarum

$$L\equiv\pm aM,$$
$$L\equiv\pm bM,$$

coëfficientes a, b in se ducti fiant ± 27 (mod. q). Ubi singulae inveniuntur, quod semper fit, ubi q est formae $12n\pm 1$, erit coëfficientis quadratum $\equiv 27$ (mod. q).

Additamentum. Cl. Gauſs loco laudato (*Götting. gel. Anz.*) theorema egregium annunciavit sequens:

„Sit p numerus primus $= 4k+1$, atque resolvatur in duo quadrata $ee+ff$, designante ee quadratum impar, ff quadratum par, fore $\pm e$ residuum minimum (quod inter $-\frac{1}{2}p$ et $+\frac{1}{2}p$ continetur), numeri $\frac{1}{2}\cdot\frac{(k+1)(k+2)(k+3)\ldots.2k}{1\ .\ 2\ .\ 3\ \ldots..\ k}$, per p divisi; hoc insuper residuum minimum per 4 divisum semper residuum $+1$ relinquere; ita ut sit aut numerus negativus formae $-(4n+3)$, aut positivus formae $4n+1$."

Cuius insignis theorematis demonstrandi periculum faciens, in fontem uberrimum incidi, e quo inter alia et demanare sequentia theoremata vidi, illius simillima:

„Sit p numerus primus $= 3n+1$, ac ponatur, quod fieri posse constat, $4p = LL + 27MM$: erit L residuum minimum numeri $-\frac{(n+1)(n+2)\ldots.2n}{1\ .\ 2\ \ldots.\ n}$, per p divisi, quod residuum per 3 divisum semper relinquet $+1$ residuum."

„Sit p numerus primus $= 7n+1$, ac ponatur, quod licet, $p = LL + 7MM$, erit L residuum minimum numeri $\frac{1}{2}\cdot\frac{(2n+1)(2n+2)\ldots.3n}{1\ .\ 2\ \ldots.\ n}$, per p divisi, quod residuum per 7 divisum semper relinquet $+1$ residuum.

D. 22. m. Junii, a. 1827.