UNIVERSITÀ DEGLI STUDI DI BARI

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

CORSO DI LAUREA IN MATEMATICA

L'ALBA DELL'ALGEBRA MODERNA NELLE *"DISQUISITIONES ARITHMETICAE"* DI CARL FRIEDRICH GAUSS

Relatore:
Chiar.ma Prof.ssa Margherita Barile

Laureando:
Cigliola Antonio

ANNO ACCADEMICO 2005-2006

Ai miei più cari amici,
Vito e Dario.

Introduzione.

Come per la maggior parte delle scienze moderne anche i fondamenti dell'algebra astratta sono stati posti nel XIX secolo. Un gran numero di strumenti e di oggetti introdotti nell'Ottocento dimostrano come sin da allora si sapesse lavorare con le strutture astratte. I vettori, le matrici, i quaternioni, i numeri reali e quelli complessi, le permutazioni delle radici di un polinomio, i resti della divisione per un intero, le forme intere del tipo $ax^2+bxy+cy^2$, i numeri algebrici ed altri ne sono esempio; questi oggetti venivano "composti" tra loro per creare elementi dello stesso tipo: si era dunque in possesso del concetto di legge di composizione interna e di gruppoide. Ma i concetti più generali ed astratti di *campo*, *corpo*, *gruppo*, *spazio vettoriale* furono introdotti solo negli ultimi anni del secolo XIX e fino ad allora si continuò a lavorare con quegli oggetti concreti in maniera complicata e molto laboriosa.

L'algebra moderna nacque dunque come studio consapevole delle proprietà generali delle strutture astratte, che studiate individualmente, erano non solo concrete, ma anche utilissime nelle applicazioni di tutti gli altri campi, si pensi ad esempio all'utilità della teoria degli spazi vettoriali nell'analisi e nella fisica. Ben presto però, le applicazioni e la praticità vennero perse di vista e gli algebristi cominciarono a dedicarsi allo studio delle proprietà formali in sé.

Ora che la teoria astratta dei gruppi esiste ed è ben solida, una delle attività preferite degli storici è rintracciare, nei lavori dei grandi del passato, le idee fondamentali di essa. Sono state per questo passate in rassegna le opere di Cauchy, Lagrange, Abel, Gauss, Galois ed altri cercando tra loro il padre della teoria dei gruppi. Diciamo subito che una ricerca del genere è tutt'altro che semplice e, cosa che potrebbe sembrare impensabile, crea tra le diverse scuole delle simpatiche "rivalità". Noi in questo lavoro ci schiereremo dalla parte dei gaussiani, trattando in particolare una delle opere giovanili del maestro *Friedrich Gauss*, quella che lo ha consacrato all'alta matematica, le *Disquisitiones Arithmeticae.* Secondo noi, infatti, all'interno di questo pregevole lavoro, si possono individuare molti dei concetti della teoria dei

gruppi (abeliani finiti) ed in particolare dei gruppi e sottogruppi ciclici. È altresì all'interno di questo trattato che per la prima volta vengono dimostrati alcuni dei più importanti teoremi della teoria dei polinomi, quali il "lemma di Gauss" ed il teorema di irriducibilità dei polinomi ciclotomici di ordine primo, dei quali è dunque indubbia la paternità.

Gauss, il principe dei matematici.

Le origini di Gauss, il *princeps mathematicorum*, furono tutt'altro che regali. Johannes Carl Friederich Gauss nacque a Braunschweig, in Germania, nell'aprile del 1777, da una famiglia poverissima. Dimostrò ben presto di essere un "enfant prodige", come raccontano i numerosi aneddoti sulla sua infanzia, e grazie all'appoggio della madre Dorotea, riuscì a compiere gli studi adeguati. All'età di quattordici anni la sua timidezza e la sua modestia conquistarono il duca "illuminato" di Braunschweig, Carlo Guglielmo Ferdinando. Questi permise a Gauss di entrare a far parte del Collegium Carolinum, e pagò tutte le spese finché la sua formazione non fu terminata. In questa scuola il giovane Federico imparò il latino, la lingua che ha utilizzato per compilare gran parte delle sue opere, e scoprì il *theorema aureum*, l'importantissima legge di reciprocità quadratica. Quando si licenziò da tale scuola aveva diciotto anni ed al momento di entrare all'Università di Göttingen era indeciso se proseguire gli studi di matematica o di filologia classica. La scoperta della costruzione del poligono regolare di diciassette lati lo convinse ad optare, fortunatamente, per la matematica. Nei primi tre anni dei suoi studi universitari conseguì innumerevoli ed importantissimi risultati che riguardano i più svariati campi. Già da tempo aveva pensato di raccogliere le sue ricerche sulla teoria dei numeri in un unico lavoro che, un anno prima della sua tesi di dottorato, prese forma nelle *Disquisitiones Arithmeticae*, la sua più grande opera. Questa fu

messa in circolazione però con un certo ritardo e per di più incompleta a causa di alcuni problemi tipografici.

Nel secondo periodo della sua vita il Maestro si dedicò in maggior parte agli studi di matematica applicata; i suoi studi di statistica, elettromagnetismo, geodesia, astronomia (che insegnò a lungo) lo condussero a notevoli risultati.
Tra le opere della maturità vanno ricordate in particolare le *Disquisitiones circa superficies curvas*, un trattato di geometria sulle superfici differenziali e la *Theoria motus corporum coelestium in sectionibus conicis solem ambientium*, un lavoro di meccanica celeste.
Negli ultimi anni della sua vita Gauss fu circondato da grande stima ed ammirazione da parte dei suoi colleghi ed allievi, ma indebolito da gravi malattie si spense all'età di settantotto anni, nel febbraio del 1855. Nel mondo delle scienze e del pensiero moderno non morirà mai.

Le *Disquisitiones Aritmeticae.*

Al serenissimo

Principe e Signore
Carlo Guglielmo Ferdinando
Duca di Braunschweig e Lüneburg

Serenissimo Principe,
considero la mia più grande fortuna che Voi mi abbiate accordato di adornare questo lavoro con il Vostro Nobilissimo nome, poiché sento il sacro dovere di dedicarlo a Voi. Se non fosse stato per il Vostro favore, Serenissimo Principe, non avrei potuto cominciare a studiare le scienze, se non fosse stato per i Vostri continui benefici a sostegno dei miei studi, non avrei potuto dedicarmi totalmente alle scienze matematiche, a cui sono portato da una grande

passione. È stata solo la Vostra benevolenza a permettermi di dedicare me stesso, libero da altre preoccupazioni per diversi anni, a quelle ricerche che questo libro espone in parte, ed infine a permettermi di pubblicarle. […]

Così scriveva l'allora ventiquattrenne Gauss al suo magnanimo mecenate, nella sua dedica delle *Disquisitiones Arithmeticae,* la sua prima grande opera matematica, pubblicata nel 1801. Ciò che più colpisce gli studiosi della letteratura matematica è che questo libro non sembra tanto un lavoro di un giovane ricercatore che scrive per affacciarsi al mondo delle scienze, quanto piuttosto l'opera di un grande matematico esperto che pubblica le sue ultime e brillanti scoperte rendendone partecipi tutti gli studiosi del mondo. La lingua usata da Gauss nelle Disquisitiones è un latino così classico ed elegante che " se Cicerone avesse avuto gli strumenti per capire i contenuti, non avrebbe apportato alcuna correzione alla forma del testo", come disse l'Autore stesso all'amico F. Meyerhoff, a cui chiese di revisionare l'opera. Dalla prefazione dell'opera sappiamo che le prime quattro sezioni erano state abbozzate fin dal 1796 quando era ancora diciannovenne, e che essa raggiunse la sua forma definitiva verso la fine del 1797, durante il suo secondo anno di studi universitari. Probabilmente la stesura finale fu data alla fine del 1800 e fino all'anno successivo non fu pubblicata a causa di non poche difficoltà.

Le *Disquisitiones Arithmeticae* sono divise in sette capitoli che il Maestro chiama *sezioni* secondo l'uso latino. Le prime tre hanno carattere introduttivo:

I. Numeri congrui in generale;
II. Congruenze di primo grado;
III. Residui di potenze.

Le tre successive rappresentano la parte centrale dell'opera e presentano gli importantissimi risultati conseguiti nella teoria dei numeri:

IV. Congruenze di secondo grado;
V. Forme ed equazioni indeterminate di secondo grado;
VI. Varie applicazioni delle ricerche precedenti.

La sezione settima, che è in realtà una monografia, presenta una delle sue scoperte più importanti, la scoperta della costruzione geometrica con riga e compasso del poligono regolare di diciassette lati:

VII. Equazioni che definiscono le sezioni di un cerchio.

Nella sezione I, di sole 5 pagine, Gauss introduce la relazione di *congruenza* tra numeri interi ed il moderno simbolo "≡", eliminando così le confusioni che comportavano i simboli usati da Legendre, Euler ed altri. A Gauss infatti spetta il merito di aver formalizzato ed esemplificato la notazione che si è tramandata fino ai nostri manuali di algebra. In questa sezione sono inoltre introdotte le nozioni di *minimo resto* e di *minimo resto assoluto* e vengono presentate le proprietà elementari delle congruenze, applicate poi come esempio ai criteri di divisibilità.

Nella sezione II, di 24 pagine, viene per la prima volta dimostrato il *teorema di fattorizzazione unica* dei numeri interi, una proprietà nota da tempi antichissimi, ma che non era mai stata provata rigorosamente, perché ritenuta *evidente*; Gauss effettua una dimostrazione per assurdo. Successivamente passa a risolvere le equazioni congruenziali di primo grado in una incognita, del tipo $ax+b\equiv c\ (\mathrm{mod.}\ m)$, i sistemi di congruenze lineari e dimostra il celebre teorema cinese del resto. Altra cosa degna di nota è l'attenzione posta alla funzione totiente di Euler, fondamentale per le ricerche successive.

La sezione III, di 35 pagine, contiene la teoria dei residui di potenze modulo un numero primo. Qui viene introdotto il concetto di *esponente* di un numero x rispetto ad un modulo m come il minimo esponente t per cui risulta $x^t\equiv 1\ (\mathrm{mod.}\ m)$. In linguaggio moderno t rappresenta il periodo dell'elemento $[x]_m$ come elemento del gruppo moltiplicativo $U(\mathbb{Z}_m)$. Successivamente, come applicazione, si dimostra il piccolo teorema di Fermat, ripercorrendo in una prima dimostrazione quella data da Euler per esaustione. Sempre ricollegandosi alle teorie del matematico svizzero, Gauss definisce le *radici primitive* di un modulo primo p, ovvero quei numeri g il cui esponente è

proprio $p-1$. In altre parole essi sono i generatori del gruppo $U(\mathbb{Z}_p)$, che è un gruppo di ordine $p-1$. Per facilitare lo studio della teoria dei residui e per risolvere congruenze lineari in un'incognita, Gauss introduce la nozione di *indice di un intero* n fissata una radice primitiva g di p, come l'esponente a tale che $n \equiv g^a \pmod{p}$. Poi egli studia le congruenze binomie del tipo $x^n \equiv A \pmod{p}$, ottenendo un criterio per il cosiddetto *carattere quadratico di un numero,* cioè per decidere se un numero è un residuo od un non-residuo quadratico relativamente al modulo p. Tra i risultati che seguono è da ricordare la dimostrazione del teorema di Wilson.

La sezione IV, di 47 pagine, è il coronamento delle sezioni precedenti, in quanto Gauss studia dapprima i residui quadratici e le proprietà relative ad essi, esamina molti casi particolari di residui quadratici ed infine espone la dimostrazione della *legge di reciprocità quadratica,* il *theorema fundamentale.* Esso mette in luce una semplice e sorprendente relazione, tutt'altro che evidente, tra la solubilità delle congruenze $x^2 \equiv p \pmod{q}$ e $x^2 \equiv q \pmod{p}$, con p e q moduli primi. Poi Gauss applica il teorema alla costruzione di forme lineari contenenti tutti i numeri che sono residui o non-residui quadratici di un dato numero. Infine mostra come ridurre una congruenza di secondo grado della forma $ax^2+bx+c \equiv 0 \pmod{m}$ ad una congruenza pura, cioè della forma $y^2 \equiv k \pmod{m}$.

La sezione V, di 260 pagine, si può considerare un libro nel libro. Questa rappresenta la prima trattazione sistematica della teoria delle forme quadratiche binarie di tipo $ax^2+2bxy+cy^2$. Dopo aver precisato che una forma di questo tipo si può rappresentare anche con la scrittura (a, b, c), Gauss comincia ad esporre la teoria delle forme, ponendo il problema principale della *rappresentazione di un numero* M mediante una forma quadratica e dimostra che ogni qualvolta ciò sarà possibile, il *determinante* della forma, $D=b^2-ac$, dovrà essere un residuo quadratico di M. Per la prima volta, anche se con un

significato differente da quello odierno, viene utilizzato il determinante di una forma quadratica. Gauss si serve di questa teoria per dimostrare una grande quantità di risultati profondi che riguardano i numeri interi, tra i tanti citiamo la rappresentazione dei numeri in somme di quadrati e multipli di quadrati. Altra cosa che dobbiamo ricordare è la risoluzione in numeri interi dell'equazione $ax^2 + by^2 + cz^2 = 0$.

Nella sezione VI, di 32 pagine, Gauss presenta parecchie applicazioni dei concetti prima discussi. Ricordiamo il problema di decomporre una frazione, il cui denominatore è il prodotto di due primi $p \cdot q$, nella somma di due nuove frazioni i cui denominatori sono q e p. Si considera poi il problema della determinazione dei periodi delle frazioni i cui denominatori sono primi o potenze di primi, che è strettamente connessa con i concetti di ordine, di radice primitiva e di indice. Ad ultimo è presentato un nuovo criterio per distinguere i numeri primi da quelli composti, e per fattorizzare questi ultimi.

La sezione VII, di 51 pagine, che conclude l'opera, è forse la parte più popolare delle Disquisitiones. Gauss risolve infatti il problema millenario della costruzione geometrica con riga e compasso dei poligoni regolari, che, in maniera a dir poco sorprendente, è connesso alle precedenti ricerche di aritmetica. Il problema della ciclotomia era già stato affrontato e risolto dal punto di vista algebrico da De Moivre e Cotes, che dimostrarono l'equivalenza del problema con la risoluzione dell'equazione $x^n - 1 = 0 \ (\mathrm{I})$.

Gauss esordisce dicendo che basta trattare il caso in cui n è un numero primo, dopodiché elimina la radice banale, l'unità, ottenendo l'equazione polinomiale $x^{n-1} + x^{n-2} + x^{n-3} + \ldots + 1 = 0 \ (\mathrm{II})$. A questo punto interviene la sua grande idea. Egli mostra che:

- le radici dell'equazione (II) si possono esprimere razionalmente mediante le radici di una successione di equazioni, i cui gradi sono i fattori primi di $n-1$;

- i coefficienti di ciascuna equazione della successione sono funzioni razionali delle equazioni precedenti e, cosa fondamentale, per ciascuno dei fattori primi di $n-1$, anche ripetuto, esiste un'equazione;
- infine, ciascuna di queste equazioni è risolubile per radicali, per cui anche la (I) sarà risolubile per radicali.

La novità sta nel fatto che Gauss per risolvere l'equazione (I) ordina le radici secondo le potenze di una radice primitiva del numero primo n e raggruppa queste potenze in *periodi*. Come corollari sui risultati ottenuti ridimostra alcuni teoremi sulle rappresentazioni dei numeri primi e, cosa molto apprezzata all'epoca, illustra dei metodi per il calcolo delle funzioni trigonometriche degli archi individuati dopo la ciclotomia. Queste osservazioni sono d'importanza capitale per la costruzione dei poligoni regolari di n lati, con n primo. Infatti se $n-1$ non contiene fattori diversi da 2, allora sarà possibile costruire con riga e compasso il poligono regolare poiché le equazioni che formano la successione saranno quadratiche e ciascuna delle loro radici potrà essere costruita in funzione dei coefficienti. Si possono così costruire tutti i poligoni regolari di n lati, con $n-1$ uguale ad una potenza di 2. Gauss prova inoltre che se n è primo ed è di tipo 2^m+1, allora $m=2^k$; sarà allora $n=2^{2^k}+1$, cioè un primo di Fermat. Se poi n è un numero composto, affinché il poligono regolare di n lati sia costruibile, n deve contenere tra i suoi fattori primi solo quelli di Fermat (non ripetuti) e potenze di 2.

In quello che segue presentiamo una traduzione integrale di quest'ultima sezione basata sull'originale latino pubblicato a Lipsia nel 1801, dal tipografo G. Fleischer figlio. Si può reperire tale versione nella raccolta *Werke, vol. I* delle opere di Gauss.

Richiami.

A causa dei riferimenti che attraversano tutta la sezione VII, ci sembra opportuno presentare, a questo punto, quegli articoli delle sezioni precedenti che vengono richiamati nel testo. Diciamo subito che la lettura di questa parte non è necessaria se si è intenzionati a procedere con una lettura veloce ed a titolo puramente informativo. Se ne consiglia invece lo studio se ci si vuole avvicinare di più agli argomenti di aritmetica discussi da Gauss. Si suggerisce altresì di fare riferimento ai concetti che abbiamo evidenziato nell'Introduzione in carattere corsivo, per lavorare con più dimestichezza con gli oggetti che presenteremo qui di seguito.

38.

PROBLEMA: *Trovare quanti sono i numeri positivi più piccoli e coprimi con un dato numero positivo* A.

Indichiamo per brevità la quantità dei numeri positivi più piccoli che sono coprimi con un numero dato, con la lettera ϕ anteposta al numero. Cerchiamo dunque ϕA.

I. Quando A è primo, è chiaro che tutti i numeri da 1 fino ad $A-1$ sono primi con A; per cui in questo caso si ha

$$\phi A = A - 1$$

II. Quando A è una potenza di un numero primo, ad esempio $A = p^m$, tutti i numeri divisibili per p non saranno primi con A, i restanti sì. Quindi dei $p^m - 1$ numeri sono da scartare: p, $2p$, $3p \ldots . \left(p^{m-1} - 1\right) p$; rimangono dunque $p^m - 1 - \left(p^{m-1} - 1\right)$ ovvero $p^{m-1}\left(p-1\right)$. Segue di qui che

$$\phi p^m = p^{m-1}(p-1)$$

III. I casi restanti si riconducono a questi per mezzo della seguente proposizione: *Se* A *è risolto nel prodotto dei fattori coprimi* M, N, P *etc., sarà*

$$\phi A = \phi M \cdot \phi N \cdot \phi P \text{ etc.}$$

[…]

IV. È facile capire come si debba applicare tutto ciò al caso che stiamo per trattare. Si decompone A nei suoi fattori primi riducendolo alla forma $a^\alpha b^\beta c^\gamma$ etc., dove a, b, c etc. sono numeri primi diversi. Allora sarà

$$\phi A = \phi a^\alpha \cdot \phi b^\beta \cdot \phi c^\gamma \text{ etc.} = a^{\alpha-1}(a-1)b^{\beta-1}(b-1)c^{\gamma-1}(c-1)\text{etc.}$$

ovvero in maniera più coincisa

$$\phi A = A\frac{a-1}{a}\cdot\frac{b-1}{b}\cdot\frac{c-1}{c}\text{etc.} \qquad [\ldots]$$

42.

Se i coefficienti A, B, C .... N ; a, b, c .... n *di due funzioni di tipo*

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} \ldots . + N \quad . \quad . \quad . \quad . \quad . \quad (P)$$
$$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} \quad \ldots . + n \quad . \quad . \quad . \quad . \quad . \quad (Q)$$

sono tutti razionali e non tutti interi e se il prodotto di (P) *per* (Q) *è*

$$x^{m+\mu} + \mathsf{A}x^{m+\mu-1} + \mathsf{B}\,x^{m+\mu-2} + \text{etc.} + \mathsf{Z},$$

allora i coefficienti A, B .... Z *non possono essere tutti interi.* […]

60.

Così come il simbolo $\sqrt[n]{A}$ indica una radice dell'equazione $x^n = A$, allo stesso modo, aggiunto il modulo, con $\sqrt[n]{A}\ (\mathrm{mod.}\ p)$ sarà denotata una qualsiasi radice dell'equazione $x^n \equiv A(\mathrm{mod.}\ p)$. Diremo che l'espressione $\sqrt[n]{A}\ (\mathrm{mod.}\ p)$ assume tanti valori, quanti sono quelli incongrui modulo p. Infatti tutti quelli che sono congrui secondo il modulo p devono essere considerati equivalenti. […]

Se si pone $\sqrt[n]{A} \equiv x\ (\mathrm{mod.}\ p)$ sarà $n\ \mathrm{Ind.}x \equiv \mathrm{Ind.}A\ (\mathrm{mod.}\ p-1)$. Da questa congruenza, grazie alle regole degli articoli precedenti, si possono dedurre i valori dello stesso $\mathrm{Ind.}x$ e da questi, i corrispondenti valori di x. In verità è facile convincersi che abbiamo tanti valori per x quante sono le radici della congruenza $n\ \mathrm{Ind.}x \equiv \mathrm{Ind.}A\ (\mathrm{mod.}\ p-1)$. Ovviamente $\sqrt[n]{A}$ ammetterà un solo valore quando n è primo con $p-1$; quando invece i numeri n e $p-1$ hanno un divisore comune δ, e questo è il massimo, l' $\mathrm{Ind.}x$ assumerà δ valori incongrui secondo il modulo $p-1$, e quindi, $\sqrt[n]{A}$ assumerà lo stesso numero di valori incongrui modulo p, se $\mathrm{Ind.}A$ è divisibile per δ. Se manca questa condizione $\sqrt[n]{A}$ non ammette alcun valore reale. […]

61.

[…]

Cominciamo col caso semplicissimo caso in cui $A=1$; sono richieste dunque le radici della congruenza $x^n = 1\ (\mathrm{mod.}\ p)$. Qui, dopo aver preso una qualsiasi radice primitiva come base, deve essere $n\,\mathrm{Ind.}x \equiv 0\ (\mathrm{mod.}\ p-1)$. Questa congruenza, quando n e $p-1$ sono coprimi, avrà soltanto una radice e precisamente $\mathrm{Ind.}x \equiv 0\ (\mathrm{mod.}\ p-1)$. Di conseguenza *in questo caso,*

$\sqrt[n]{1}\,(\text{mod. } p)$ ammette un solo valore, $\equiv 1$. Ma quando i numeri n e $p-1$ hanno un massimo comune divisore δ, la soluzione completa della congruenza $n\,\text{Ind.}x \equiv 0\,(\text{mod. } p-1)$ sarà $\text{Ind.}x \equiv 0\left(\text{mod. } \frac{p-1}{\delta}\right)$; cioè Ind.$x$ modulo $p-1$ dovrà essere congruo ad uno dei numeri

$$0,\quad \frac{p-1}{\delta},\quad \frac{2(p-1)}{\delta},\quad \frac{3(p-1)}{\delta},\quad \ldots\quad \frac{(\delta-1)(p-1)}{\delta}$$

ovvero ammetterà δ valori che non sono congrui modulo $p-1$. In questo caso anche x avrà δ valori differenti (incongrui modulo p). Vediamo così che anche l'espressione $\sqrt[\delta]{1}$ ammette δ valori differenti i cui indici sono esattamente gli stessi visti prima. Per questo motivo l'espressione $\sqrt[\delta]{1}\,(\text{mod.}p)$ è del tutto equivalente a $\sqrt[n]{1}\,(\text{mod.}p)$. […]

62.

C'è un caso, però, che possiamo risolvere qui e precisamente quando $n=2$. Chiaramente i valori dell'espressione $\sqrt[2]{1}$ saranno $+1$ e -1, poiché essa non può averne più di due, e $+1$ e -1 saranno sempre incongrui a meno che il modulo non sia $=2$, nel qual caso $\sqrt[2]{1}$ può ovviamente avere un solo valore. Di qui segue che $+1$ e -1 saranno anche valori dell'espressione $\sqrt[2m]{1}$ quando m è primo con $\frac{p-1}{2}$. […]

79.

[…]

La somma di tutti gli elementi del periodo di un numero qualsiasi è $\equiv 0$.

[…]

(Qui per periodo si intende l'insieme di tutte le potenze di un numero che vanno dall'esponente 0 al più piccolo esponente per cui si ha una potenza $\equiv 1 \pmod{p}$, fissato il modulo p rispetto a cui lavorare, N.d.T.).

96.

Fissato un numero primo p *come modulo, metà dei numeri 1, 2, 3 ...* $p-1$ *saranno residui quadratici, i rimanenti saranno non-residui, avremo cioè* $\frac{1}{2}(p-1)$ *residui ed altrettanti non-residui.* […]

309.

PROBLEMA: *Decomporre una frazione* $\frac{m}{n}$*, il cui denominatore* n *è prodotto di due numeri coprimi* a *e* b*, nella somma di altre due i cui denominatori siano* a *e* b.

Soluzione: Siano le frazioni richieste $\frac{x}{a}$ ed $\frac{y}{b}$, avremo allora $bx + ay = m$. Questo vuol dire che x è una soluzione della congruenza $bx \equiv m \pmod{a}$, essa può essere trovata con i metodi della Sezione II; y sarà quindi $= \frac{m - bx}{a}$.

È chiaro che la congruenza $bx \equiv m$ ha infinite soluzioni, tutte congrue tra loro $\bmod a$, ma ne esiste solo una che è positiva e più piccola di a. Può capitare che y sia negativo. È fortemente necessario osservare che noi

possiamo anche ricavare y dalla congruenza $ay \equiv m \left(\mathrm{mod.}\, b\right)$ e x dall'equazione $x = \frac{m + ay}{b}$. Per esempio, data la frazione $\frac{58}{77}$, 4 sarà un valore dell'espressione $\frac{58}{11}$ $\left(\mathrm{mod.}\, 7\right)$, così $\frac{58}{77}$ sarà decomposta in $\frac{4}{7} + \frac{2}{11}$.

310.

Se è data la frazione $\frac{m}{n}$ il cui denominatore n è prodotto di fattori coprimi a, b, c, d, etc., si può, come nel precedente articolo, risolverla nella somma di due frazioni i cui denominatori sono a e bcd etc.; poi la seconda di queste va scritta come somma di due nuove frazioni i cui denominatori sono b e cd etc.; e così via fino ad esaurire i fattori di n per ottenere la forma:

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \mathrm{etc.}$$

[…]

SEZIONE SETTIMA

EQUAZIONI CHE DEFINISCONO LE SEZIONI DI UN CERCHIO.

———

335.

Tra gli splendidi risultati raggiunti dai matematici moderni, la teoria delle funzioni circolari occupa senza dubbio il posto più importante. Avremo occasione in molti contesti di far riferimento a tale straordinario esempio di quantità, e non c'è alcun ramo di tutta la matematica che non dipenda da esso. I più brillanti matematici moderni con la propria operosità e sagacia hanno formulato per essa una disciplina tanto vasta, che ci possiamo aspettare difficilmente che una qualsiasi parte di questa teoria, soprattutto i fondamenti, possa essere significativamente ampliata. Parlo della teoria delle funzioni trigonometriche corrispondenti ad archi commensurabili con la circonferenza, ovvero della teoria dei poligoni regolari, della quale solo una piccola parte si è finora sviluppata, come sarà chiarito in questa Sezione. Il lettore potrebbe essere sorpreso di trovare una discussione di questo argomento nel presente lavoro che tratta di una disciplina apparentemente così eterogenea; ma la

trattazione stessa chiarirà abbondantemente che c'è un intimo legame tra questa materia e l'Aritmetica superiore.

I principi della teoria che stiamo per spiegare in realtà si estendono più di quanto noi indicheremo. Infatti essi possono essere applicati non solo alle funzioni circolari ma anche alle altre funzioni trascendenti, ad esempio a quelle che dipendono dall'integrale $\int \frac{dx}{\sqrt{1-x^4}}$ ed anche a vari tipi di congruenze. Poiché, tuttavia, stiamo preparando un ampio lavoro sulle funzioni trascendenti e poiché parleremo a lungo delle congruenze durante le nostre ricerche di aritmetica, ci è sembrato opportuno considerare qui solo le funzioni circolari. E sebbene potessimo trattarle in tutta la loro generalità, ci ridurremo nei seguenti articoli al caso più semplice, sia per motivi di brevità sia perché i nuovi principi di questa teoria possano essere più facilmente appresi.

336.

Se indichiamo la circonferenza di un cerchio o quattro angoli retti con P e se m ed n sono interi, con n prodotto di fattori coprimi a, b, c etc., l'angolo $A = \frac{mP}{n}$ può essere ridotto con il metodo dell'articolo 310 alla forma $A = \left(\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \text{etc.} \right) P$ e le sue funzioni goniometriche possono essere espresse per mezzo delle funzioni goniometriche degli angoli $\frac{\alpha P}{a}$, $\frac{\beta P}{b}$ etc. Ora, poiché possiamo prendere a, b, c, etc. primi o potenze di primi, è sufficiente studiare la divisione della circonferenza in un numero di parti che è primo od una potenza di un primo, così da ottenere un poligono di n lati a partire dai poligoni di a, b, c etc. lati. Tuttavia restringeremo le nostre ricerche al caso in cui il circolo è diviso in un numero primo (dispari) di lati, per le ragioni che seguono. Le funzioni circolari dell'angolo $\frac{mP}{p^2}$ possono

essere determinate a partire da quelle dell'angolo $\frac{mP}{p}$ grazie alla risoluzione di un'equazione di grado p. A partire da queste poi si possono ricavare quelle corrispondenti all'angolo $\frac{mP}{p^3}$, etc. Così se è già dato un poligono di p lati, per determinare un poligono di p^λ lati dobbiamo necessariamente risolvere $\lambda - 1$ equazioni di grado p. In verità, nonostante sia possibile estendere la teoria seguente anche a questo caso, tuttavia per tale strada ci imbatteremmo nello stesso numero di equazioni di grado p, le quali, se p è un numero primo, non possono essere in nessun modo ridotte. Così, ad esempio, proveremo che il poligono regolare di 17 lati può essere costruito con riga e compasso, ma per costruire quello di 289 lati non si può ovviare in nessun modo alla risoluzione di un'equazione di grado 17.

337.

È ben noto che le funzioni trigonometriche degli angoli $\frac{kP}{n}$, denotando con k i numeri $0, 1, 2 \ldots n-1$, possono essere espresse per mezzo delle radici di un'equazione di grado n. Ad esempio *i seni* con le radici di questa (I):

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \text{etc.} \pm \frac{1}{2^{n-1}}nx = 0,$$

i coseni con le radici dell'equazione (II):

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \text{etc.} \pm \frac{1}{2^{n-1}}nx - \frac{1}{2^{n-1}} = 0$$

ed infine *le tangenti* con le radici dell'equazione (III):

$$x^n - \frac{n(n-1)}{1\cdot 2}x^{n-2} + \frac{n(n-1)(n-2)(n-3)}{1\cdot 2\cdot 3\cdot 4}x^{n-4} - \text{etc.} \pm nx = 0\,.$$

Queste equazioni (che sono vere in generale per un qualsiasi n dispari, la II anche per i valori pari) ponendo $n = 2m+1$, possono essere facilmente ridotte al grado m; e cioè, per I e III dividendo a sinistra per x e sostituendo x^2 con y. L'equazione II invece include la radice $x = 1\left(=\cos 0\right)$ e tutte le altre sono uguali a coppie ($\cos\frac{P}{n} = \cos\frac{(n-1)P}{n}$, $\cos\frac{2P}{n} = \cos\frac{(n-2)P}{n}$, etc.); così il membro a sinistra è divisibile per $x-1$ ed il quoziente sarà un quadrato. Estraendo la radice quadrata, l'equazione II si riduce alla seguente:

$$x^m + \frac{1}{2}x^{m-1} - \frac{1}{4}(m-1)x^{m-2} - \frac{1}{8}(m-2)x^{m-3}$$
$$+ \frac{1}{16}\frac{(m-2)(m-3)}{1\cdot 2}x^{m-4} + \frac{1}{32}\frac{(m-3)(m-4)}{1\cdot 2}x^{m-5} - \text{etc.} = 0$$

Le sue radici saranno i coseni degli angoli $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$, …, $\frac{mP}{n}$. Non saranno possibili ulteriori riduzioni di queste equazioni nel caso in cui n è un numero primo.

Tuttavia nessuna di queste equazioni è tanto maneggevole ed adatta ai nostri scopi quanto $x^n - 1 = 0$, le cui radici sono intimamente connesse con quelle delle equazioni precedenti. Cioè, se indichiamo con i per brevità la quantità immaginaria $\sqrt{-1}$, le radici dell'equazione $x^n - 1 = 0$ saranno:

$$\cos\frac{kP}{n} + i\sin\frac{kP}{n} = r$$

dove $k = 0,1,2...n-1$. Poiché $\frac{1}{r} = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$, le radici dell'equazione I saranno espresse per mezzo di $\left(r - \frac{1}{r}\right)\frac{1}{2i}$ o $\frac{i\left(1-r^2\right)}{2r}$; le radici dell'equazione

II , con $\frac{1}{2}\left(r+\frac{1}{r}\right)=\frac{1+r^2}{2r}$; infine le radici dell'equazione III ,con $\frac{i\left(1-r^2\right)}{1+r^2}$. Per questi motivi effettueremo le nostre ricerche a partire da considerazioni sulle radici dell'equazione $x^n-1=0$ e supporremo che n sia un numero primo dispari. Per non interrompere l'ordine delle nostre osservazioni premetteremo il seguente lemma.

338.

PROBLEMA: *Data l'equazione*

$$(W)\ldots z^m+Az^{m-1}+\text{etc.}=0$$

trovare un'equazione (W') *le cui radici siano le* λ*-esime potenze delle radici dell'equazione* (W)*, dove* λ *è un dato esponente intero positivo.*

Soluzione: Se indichiamo le radici dell'equazione W con a, b, c, etc., le radici dell'equazione W' saranno a^λ, b^λ, c^λ, etc. Grazie ad un ben noto teorema di Newton, dai coefficienti dell'equazione W possiamo ricavare le somme di una qualsiasi potenza delle radici a, b, c, etc. Cerchiamo dunque le somme

$$a^\lambda+b^\lambda+c^\lambda+\text{etc.},\quad a^{2\lambda}+b^{2\lambda}+c^{2\lambda}+\text{etc.},\quad \text{etc. fino ad}\quad a^{m\lambda}+b^{m\lambda}+c^{m\lambda}+\text{etc.}$$

e con un procedimento inverso, stabilito nello stesso teorema, possiamo ricavare i coefficienti dell'equazione W'. Q. E. F.

È chiaro che se i coefficienti di W sono razionali, lo saranno anche quelli di W'. Con un altro metodo si può provare che se i primi sono interi, anche gli altri lo saranno. Non ci soffermeremo ancora su questo teorema, poiché non è necessario per il nostro scopo.

339.

L'equazione $x^n - 1 = 0$ (supporremo sempre che n sia un numero primo dispari) ha una sola radice reale, $x = 1$; le restanti $n-1$ radici, che sono date dall'equazione

$$x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0$$

sono tutte immaginarie; indicheremo il loro insieme con Ω e con X la funzione

$$x^{n-1} + x^{n-2} + \text{etc.} + x + 1 .$$

Se quindi r è una radice di Ω, avremo che $1 = r^n = r^{2n}$ etc. ed in generale $r^{en} = 1$ per ogni valore intero positivo o negativo di e. Così se λ e μ sono interi congrui modulo n, avremo che $r^\lambda = r^\mu$. Ma se λ, μ sono incongrui $\text{mod.}n$, allora r^λ e r^μ saranno diversi. In questo caso infatti può essere preso un intero ν tale che $(\lambda - \mu)\nu \equiv 1 \,(\text{mod.}n)$, allora $r^{(\lambda-\mu)\nu} = r$ e certamente $r^{(\lambda-\mu)}$ non è $= 1$. È chiaro anche che ogni potenza di r è una radice dell'equazione $x^n - 1 = 0$. Ora, poiché le quantità $1 \left(= r^0\right)$, r, r^2, …, r^{n-1} sono tutte diverse esse forniranno tutte le radici dell'equazione $x^n - 1 = 0$ e così i numeri r, r^2, …, r^{n-1} coincideranno con Ω. In generale, dunque, Ω coinciderà con r^e, r^{2e}, r^{3e}, …, $r^{(n-1)e}$ se e è un qualsiasi intero positivo o negativo non divisibile per n. Abbiamo quindi

$$X = \left(x - r^e\right)\left(x - r^{2e}\right)\left(x - r^{3e}\right)\ldots\left(x - r^{(n-1)e}\right)$$

da cui

$$r^e + r^{2e} + r^{3e} + \ldots + r^{(n-1)e} = -1 \qquad \text{e} \qquad 1 + r^e + r^{2e} + r^{3e} + \ldots + r^{(n-1)e} = 0 .$$

Chiameremo radici *reciproche* due radici del tipo r e $\frac{1}{r}\left(=r^{n-1}\right)$ o, più in generale, r^e ed r^{-e}. Ovviamente il prodotto di due fattori semplici del tipo $x-r$ e $x-\frac{1}{r}$ è reale ed è $=x^2-2x\cos\omega+1$, così che l'angolo ω è uguale all'angolo $\frac{P}{n}$ od ad un qualche suo multiplo.

340.

Poiché, indicata con r una qualsiasi radice di Ω, possiamo esprimere tutte le radici dell'equazione $x^n-1=0$ per mezzo di potenze di r, il prodotto di più radici di questa equazione può essere indicato con r^λ, in maniera tale che λ sia o 0 o positivo e $<n$. Così indicando con $\varphi(t,u,v...)$ una funzione algebrica razionale intera nelle indeterminate t, u, v etc. che può essere espressa come somma di addendi di tipo $ht^\alpha u^\beta v^\gamma...$: è chiaro che, sostituendo t,u,v etc. con alcune delle radici dell'equazione $x^n-1=0$, ad esempio $t=a$, $u=b$, $v=c$ etc., allora $\varphi(a,b,c...)$ può essere ridotta alla forma

$$A+A'r+A''r^2+A'''r^3+...+A^\nu r^{n-1}$$

in maniera tale che i coefficienti A,A', etc. (alcuni dei quali possono mancare ed essere così $=0$) siano quantità determinate. Tutti questi coefficienti saranno interi se tutti i coefficienti di $\varphi(t,u,v...)$, cioè tutte le h, lo sono. E se successivamente sostituiamo $a^2,b^2,c^2,...$ al posto di t,u,v etc. rispettivamente , ciascun termine $ht^\alpha u^\beta v^\gamma...$ che era stato ridotto alla forma r^σ ora diventerà $r^{2\sigma}$; così

$$\varphi\left(a^2,b^2,c^2...\right)=A+A'r^2+A''r^4+A'''r^6+...+A^\nu r^{(2n-2)}$$

In generale per un qualsiasi valore intero di λ,

$$\varphi\left(a^{\lambda}, b^{\lambda}, c^{\lambda} \ldots\right) = A + A' r^{\lambda} + A'' r^{2\lambda} + \ldots + A^{\nu} r^{(n-1)\lambda} .$$

Questa proposizione è veramente importante e fondamentale per le seguenti osservazioni. Di qui segue anche che

$$\varphi(1,1,1,\ldots) = \varphi\left(a^{n}, b^{n}, c^{n} \ldots\right) = A + A' + A'' + \ldots + A^{\nu} \qquad \text{e}$$

$$\varphi(a,b,c\ldots) + \varphi\left(a^{2}, b^{2}, c^{2} \ldots\right) + \varphi\left(a^{3}, b^{3}, c^{3} \ldots\right) + \ldots + \varphi\left(a^{n}, b^{n}, c^{n} \ldots\right) = nA$$

Tale somma sarà intera e divisibile per n quando tutti i coefficienti in $\varphi(t,u,v\ldots)$ sono interi.

341.

TEOREMA. *Se la funzione X è divisibile per la funzione di grado più basso*

$$P = x^{\lambda} + Ax^{\lambda-1} + Bx^{\lambda-2} + \ldots + Kx + L$$

i coefficienti A, B, …, L non possono essere tutti interi.

Dimostrazione. Sia $X = PQ$ e sia P l'insieme delle radici dell'equazione $P = 0$, Q l'insieme delle radici dell'equazione $Q = 0$, così che Ω sarà uguale a P e Q presi assieme. Sia inoltre R il complesso delle radici reciproche di P, S il complesso delle radici reciproche di Q e siano le radici che sono contenute in R radici dell'equazione $R = 0$ (che diventa $x^{\lambda} + \frac{K}{L} x^{\lambda-1} + \text{etc.} + \frac{A}{L} x + \frac{1}{L} = 0$ come si può facilmente dedurre) e quelle contenute in S le radici dell'equazione $S = 0$. Chiaramente anche le radici R

e S prese assieme ricoprono tutto Ω, e sarà $RS = X$. Ora bisogna distinguere quattro casi.

I. Quando P ed R coincidono e conseguentemente $P = R$. In questo caso chiaramente P sarà costituito di coppie di radici reciproche e così P sarà il prodotto di $\frac{\lambda}{2}$ fattori accoppiati di tipo $x^2 - 2x\cos\omega + 1$. Poiché un fattore del genere è $= (x - \cos\omega)^2 + \sin^2\omega$, è chiaro che per un qualsiasi valore reale di x, P assume un valore reale positivo. Siano le equazioni le cui radici sono le potenze quadrate, cubiche, quarte, …, $(n-1)$-me delle radici di P rispettivamente $P' = 0$, $P'' = 0$, $P''' = 0$, … $P^{\nu} = 0$ e siano p, p', p'', …, p^{ν} rispettivamente i valori delle funzioni P, P', P'', … P^{ν} che si ottengono ponendo $x = 1$. Ora per quanto detto prima, p sarà un valore positivo e per un motivo analogo p', p'', etc. saranno anch'essi positivi. Essendo p il valore della funzione $(1-t)(1-u)(1-v)$etc. ottenuto sostituendo a t, u, v, etc. le radici contenute in P; p' il valore della stessa funzione ottenuto sostituendo a t, u, v, etc. i quadrati delle radici; etc.; 0 il valore assunto quando $t = 1$, $u = 1$, $v = 1$ etc.: la somma $p + p' + p'' ... + p^{\nu}$ sarà un intero divisibile per n. Inoltre il prodotto $PP'P''...$ sarà $= X^{\lambda}$ e così $pp'p''... = n^{\lambda}$.

Se tutti i coefficienti in P fossero razionali, anche tutti i coefficienti in P', P'', etc. sarebbero razionali per l'articolo 338. Tuttavia per l'articolo 42 tutti questi coefficienti saranno necessariamente interi. Così anche p, p', p'', etc. saranno interi. Giacché il loro prodotto è n^{λ} ed il loro numero è $n - 1 > \lambda$, alcuni di essi (almeno $n - 1 - \lambda$) devono essere $= 1$, ed i rimanenti uguali ad n o a potenze di n. Se così g di essi sono $= 1$, la somma $p + p' +$ etc. sarà $\equiv g \pmod{n}$ e di certo non divisibile per n. Per questo la nostra supposizione è inconsistente.

II. Quando P e R non coincidono, ma contengono alcune radici comuni, sia T il loro insieme e $T = 0$ l'equazione di cui sono radici. Allora T

sarà il massimo comun divisore delle funzioni P ed R (come è chiaro dalla teoria delle equazioni).Tuttavia, coppie di radici in T saranno reciproche e per quello che abbiamo mostrato prima i coefficienti di T non possono essere tutti razionali. Questo sicuramente accade se tutti i coefficienti di P e anche quelli di R sono razionali, come risulta chiaro dalla natura delle operazioni per la ricerca del massimo comun divisore. Perciò la supposizione è assurda.

III. Quando Q e S coincidono od hanno alcune radici comuni, possiamo mostrare esattamente nello stesso modo che non tutti i coefficienti di Q possono essere razionali; ma essi sarebbero razionali se tutti i coefficienti di P fossero razionali; così ciò è impossibile.

IV. Se P non ha alcuna radice comune con R, né Q con S, tutte le radici di P saranno necessariamente trovate in S, e tutte quelle di Q in R. Dunque $P=S$ e $Q=R$, e così $X=PQ$ sarà prodotto di P per R; cioè

$$\text{di } x^{\lambda}+Ax^{\lambda-1}...+Kx+L \quad \text{per} \quad x^{\lambda}+\frac{K}{L}x^{\lambda-1}...+\frac{A}{L}x+\frac{1}{L}$$

che ponendo $x=1$, diventa

$$nL=\left(1+A...+K+L\right)^2.$$

Ora se tutti i coefficienti di P fossero razionali, e quindi per l'articolo 42 anche interi, L, che deve dividere l'ultimo coefficiente in X, ovvero l'unità, necessariamente sarebbe $=\pm 1$, e di conseguenza $\pm n$ un quadrato. Visto che questo contraddice le ipotesi, la supposizione è inconsistente.

Da questo teorema è chiaro che indipendentemente da come X è decomposto in fattori, alcuni coefficienti saranno irrazionali e così questi non possono essere determinati se non per mezzo di un'equazione di grado superiore al primo.

342.

Il piano delle seguenti ricerche, che non sarà affatto inutile illustrare in poche parole, mira a ridurre X in più fattori GRADUALMENTE, ed in maniera tale che i coefficienti di questi siano determinati grazie ad equazioni di grado più piccolo possibile. Così facendo perverremo infine ai fattori semplici o alle radici stesse di Ω. Mostreremo che, se il numero $n-1$ è decomposto in un qualunque modo in fattori interi α, β, γ etc. (ciascuno dei quali possiamo assumere essere un numero primo) X può essere risolto in α fattori di dimensione $\frac{n-1}{\alpha}$, i coefficienti dei quali saranno determinati per mezzo di equazioni di grado α; ciascuno di questi a sua volta sarà risolto in altri β di dimensione $\frac{n-1}{\alpha\beta}$ con l'aiuto di un'equazione di grado β etc., così che indicando con ν il numero dei fattori α, β, γ etc. la determinazione delle radici di Ω è ricondotta alla risoluzione di ν equazioni di grado α, β, γ etc. Per esempio, per $n=17$, dove $n-1=2\cdot 2\cdot 2\cdot 2$, bisognerà risolvere quattro equazioni quadratiche; per $n=73$ tre quadratiche e due cubiche.

In quanto segue saranno spesso considerate alcune potenze di una radice r i cui esponenti sono a loro volta delle potenze. Poiché espressioni di questo tipo sono difficilmente rappresentabili con i caratteri tipografici, per facilitare la scrittura d'ora in poi seguiremo la seguente abbreviazione. Al posto di r, r^2, r^3 etc. scriveremo $[1]$, $[2]$, $[3]$ etc. ed in generale per r^λ scriveremo $[\lambda]$. Espressioni di questo tipo non sono completamente determinate, ma esse lo diventano non appena fissiamo una determinata radice di Ω per r ovvero per $[1]$. In generale $[\lambda]$ e $[\mu]$ sono uguali o diversi a seconda che λ e μ siano congrui o meno modulo n. Inoltre $[0]=1$; $[\lambda]\cdot[\mu]=[\lambda+\mu]$; $[\lambda]^\nu=[\lambda\nu]$; la somma $[0]+[\lambda]+[2\lambda]...+[(n-1)\lambda]$ vale 0 o n a seconda che λ sia non divisibile o divisibile per n.

343.

Se relativamente al modulo n, g è un numero come quelli che nella Sezione III abbiamo definito radici primitive, gli $n-1$ numeri 1, g, g^2, … g^{n-2} saranno congrui ai numeri 1, 2, 3, … $n-1$ modulo n, sia pure in un altro ordine, cioè ogni numero nella prima serie sarà congruo ad uno della seconda. Da questo segue immediatamente che le radici $[1]$, $[g]$, $[g^2]$, … $[g^{n-2}]$ coincidono con Ω; e allo stesso modo, più in generale, le radici

$$[\lambda],\ [\lambda g],\ [\lambda g^2],\ \ldots\ [\lambda g^{n-2}]$$

coincideranno con Ω, indicando con λ un qualsiasi intero non divisibile per n. Inoltre poiché $g^{n-1} \equiv 1 \pmod{n}$ è facile vedere che due radici $[\lambda g^\mu]$ e $[\lambda g^\nu]$ saranno identiche o diverse a seconda che μ e ν siano congrui o meno relativamente al modulo $(n-1)$.

Se quindi G è un'altra radice primitiva, le radici $[1]$, $[g]$, $[g^2]$ …$[g^{n-2}]$ coincideranno anche con $[1]$, $[G]$ …$[G^{n-2}]$ se non si dà importanza all'ordine. Inoltre, come sarà facilmente dimostrato, se e è un divisore di $n-1$, e $n-1 = ef$, $g^e = h$ e $G^e = H$, anche gli f numeri 1, h, h^2 … h^{f-1} saranno congruenti ad 1, H, H^2 … H^{f-1} modulo n (non ordinatamente). Supponiamo infatti che $G \equiv g^\omega \pmod{n}$, sia poi μ un numero arbitrario positivo e $< f$, e ν il minimo residuo di $\mu\omega \pmod{f}$. Sarà allora $\nu e \equiv \mu\omega e \pmod{n-1}$, di qui segue che $g^{\nu e} \equiv g^{\mu\omega e} \equiv G^{\mu e} \pmod{n}$, ovvero $H^\mu \equiv h^\nu$, cioè ogni numero della seconda serie 1, H, H^2 etc. sarà congruo ad un numero nella serie 1, h, h^2 …, e viceversa. È chiaro allora che le f radici $[1]$, $[h]$, $[h^2]$ …$[h^{f-1}]$

saranno uguali alle radici $[1]$, $[H]$, $\left[H^2\right]$ $\ldots\left[H^{f-1}\right]$. Allo stesso modo si ottiene facilmente che coincidono le più generali serie

$$[\lambda], [\lambda h], \left[\lambda h^2\right] \ldots\left[\lambda h^{f-1}\right] \quad \text{e} \quad [\lambda], [\lambda H], \left[\lambda H^2\right] \ldots\left[\lambda H^{f-1}\right].$$

Indicheremo la *somma* di tali f radici, $[\lambda]+[\lambda h]+\text{etc.}+\left[\lambda h^{f-1}\right]$, con (f, λ). Poiché esso non varia prendendo al posto di g un'altra radice primitiva, deve essere considerato indipendente da g. Chiameremo poi il *complesso* delle stesse radici il *periodo* (f, λ), nel quale non viene data importanza all'ordine delle radici *).

Per indicare un periodo di quel tipo sarà utile ridurre ciascuna radice, di cui è composto, alla loro forma più semplice, cioè sostituire ai numeri λ, λh, λh^2, etc. i loro minimi residui $\mod. n$. Volendo sarà possibile sistemare i termini del periodo in ordine crescente.

Per esempio, per $n=19$, di cui 2 è una radice primitiva, il periodo $(6, 1)$ è costituito dalle radici $[1]$, $[8]$, $[64]$, $[512]$, $[4096]$, $[32768]$ ovvero $[1]$, $[7]$, $[8]$, $[11]$, $[12]$, $[18]$. Allo stesso modo il periodo $(6, 2)$ è formato da $[2]$, $[3]$, $[5]$, $[14]$, $[16]$, $[17]$. Il periodo $(6, 3)$ coincide col precedente. Il periodo $(6, 4)$ contiene $[4]$, $[6]$, $[9]$, $[10]$, $[13]$, $[15]$.

---

*) In quello che segue chiameremo la somma il valore numerico del periodo, o semplicemente periodo, se non c'è rischio di ambiguità.

Facciamo subito le seguenti osservazioni sui periodi di questo tipo:

I. Poiché $\lambda h^f \equiv \lambda$, $\lambda h^{f+1} \equiv \lambda h$, etc. $(\mathrm{mod.}\ n)$, è chiaro che (f, λ), $(f, \lambda h)$, $(f, \lambda h^2)$, etc. sono costituiti dalle stesse radici. Più in generale se $[\lambda']$ è una radice di (f, λ), questo periodo sarà del tutto identico a (f, λ'). Se dunque due periodi costituiti dallo stesso numero di radici (che definiamo *simili*) hanno una radice in comune, essi coincideranno. Di conseguenza non può accadere che due radici siano contenute in un medesimo periodo e che solo una di esse venga ritrovata in un altro periodo simile. Inoltre se due radici $[\lambda]$, $[\lambda']$ appartengono allo stesso periodo di f termini, il valore dell'espressione $\frac{\lambda'}{\lambda} (\mathrm{mod.}\ n)$ è congruo ad una qualche potenza di h, possiamo allora supporre $\lambda' \equiv \lambda g^{ve} (\mathrm{mod.}\ n)$.

II. Se $f = n-1$, $e = 1$, il periodo $(f, 1)$ coinciderà con Ω. Nei casi restanti Ω sarà composto dai periodi $(f, 1)$, (f, g), (f, g^2) … (f, g^{e-1}). Tali periodi dunque saranno completamente diversi l'uno dall'altro ed è chiaro che ogni altro periodo simile (f, λ) coinciderà con uno di essi se $[\lambda]$ appartiene ad Ω, cioè se λ non è divisibile per n. Il periodo $(f, 0)$ ovvero (f, kn) è composto di f unità. È anche chiaro che se λ è un qualsivoglia numero non divisibile per n, anche il complesso degli e periodi (f, λ), $(f, \lambda g)$, $(f, \lambda g^2)$ … $(f, \lambda g^{e-1})$ coinciderà con Ω. Così per esempio, posto $n = 19$, $f = 6$, Ω sarà composto dei tre periodi $(6, 1)$, $(6, 2)$, $(6, 4)$. Ogni altro periodo simile, tranne $(6, 0)$, può essere ridotto ad uno di questi.

III. Se $n-1$ è prodotto di tre numeri positivi a, b, c, segue che ogni periodo di bc termini è composto da b periodi di c termini; per esempio

(bc, λ) è formato da (c, λ), $(c, \lambda g^a)$, $(c, \lambda g^{2a})$ … $(c, \lambda g^{ab-a})$. Così diremo che questi ultimi sono contenuti nei primi. Allora per $n = 19$ il periodo $(6, 1)$ è formato dai tre periodi $(2, 1)$, $(2, 8)$, $(2, 7)$, dei quali il primo contiene le radici r ed r^{18}; il secondo r^8 e r^{11}; il terzo r^7 e r^{12}.

345.

TEOREMA. *Siano* (f, λ) *ed* (f, μ) *due periodi simili, identici o diversi; sia* (f, λ) *costituito dalle radici* $[\lambda]$, $[\lambda']$, $[\lambda'']$ *etc. Allora il prodotto di* (f, λ) *per* (f, μ) *sarà la somma di* f *periodi simili, ovvero*

$$= (f, \lambda + \mu) + (f, \lambda' + \mu) + (f, \lambda'' + \mu) + \text{etc.} = W$$

Dimostrazione. Sia come sopra $n - 1 = ef$; g una radice primitiva per la congruenza modulo n e $h = g^e$, e quindi come abbiamo visto prima, $(f, \lambda) = (f, \lambda h) = (f, \lambda h^2)$ etc. Il prodotto richiesto sarà allora

$$= [\mu] \cdot (f, \lambda) + [\mu h] \cdot (f, \lambda h) + [\mu h^2] (f, \lambda h^2) + \text{etc.}$$

e quindi

$$\begin{aligned} &= [\lambda \quad + \mu] \quad + [\lambda h \quad + \mu] \quad \ldots + [\lambda h^{f-1} + \mu] \\ &+ [\lambda h \quad + \mu h] \quad + [\lambda h^2 + \mu h] \quad \ldots + [\lambda h^f \quad + \mu h] \\ &+ [\lambda h^2 + \mu h^2] + [\lambda h^3 + \mu h^2] \ldots + [\lambda h^{f+1} + \mu h^2] \text{ etc.} \end{aligned}$$

Questa espressione contiene in tutto f^2 radici. Se poi sommiamo le singole colonne verticali abbiamo

$$(f, \lambda + \mu) + (f, \lambda h + \mu) + \ldots + (f, \lambda h^{f-1} + \mu).$$

Tale espressione coincide con W poiché per ipotesi i numeri λ, λ', λ'' etc. sono congruenti a λ, λh, λh^2, … λh^{f-1} modulo n (senza dare alcuna importanza all'ordine). Di conseguenza anche $\lambda+\mu$, $\lambda'+\mu$, $\lambda''+\mu$ etc. saranno congruenti a $\lambda+\mu$, $\lambda h+\mu$, $\lambda h^2+\mu$ … $\lambda h^{f-1}+\mu$. Q.E.D.

Aggiungiamo a questo teorema i seguenti corollari:

I. Se k è un intero qualsiasi, il prodotto di $(f, k\lambda)$ per $(f, k\mu)$ sarà

$$=(f, k(\lambda+\mu))+(f, k(\lambda'+\mu))+(f, k(\lambda''+\mu))+\text{etc.}$$

II. Poiché ogni singolo termine in W coincide con la somma $(f, 0)$ che è $= f$, o con una delle somme $(f, 1)$, (f, g), (f, g^2) … (f, g^{e-1}), W può essere ridotta alla forma seguente

$$W = af + b(f, 1) + b'(f, g) + b''(f, g^2) + \ldots + b^{\varepsilon}(f, g^{e-1})$$

dove i coefficienti a, b, b' etc. sono interi positivi (oppure qualcuno $=0$). È inoltre chiaro che il prodotto di $(f, k\lambda)$ per $(f, k\mu)$ diventa

$$= af + b(f, k) + b'(f, kg) + \ldots + b^{\varepsilon}(f, kg^{e-1})$$

Per esempio se $n=19$ il prodotto della somma $(6, 1)$ per sé stessa, ovvero il quadrato di questa, sarà $=(6, 2)+(6, 8)+(6, 9)+(6, 12)+(6, 13)+(6, 19)=$ $6+2(6, 1)+(6, 2)+2(6, 4)$.

III. Poiché il prodotto dei singoli termini di W per un periodo simile (f, ν) può essere ridotto ad una forma analoga, è facile convincersi che il prodotto di tre periodi $(f, \lambda)\cdot(f, \mu)\cdot(f, \nu)$ può essere riscritto nella forma $cf + d(f, 1) \ldots + d^{\varepsilon}(f, g^{e-1})$ e i coefficienti c, d etc. saranno interi e positivi (od $=0$) e per ogni valore intero di k abbiamo

$$(f, k\lambda)\cdot(f, k\mu)\cdot(f, k\nu) = cf + d(f, k) + d'(f, kg) + \text{etc.}$$

Questo teorema può essere esteso al prodotto di un qualsiasi numero di periodi simili, e non importa se essi sono diversi od in parte o del tutto identici.

IV. Da ciò segue che se in una qualunque funzione algebrica razionale intera $F = \varphi(t,u,v...)$ sostituiamo le indeterminate t, u, v etc. rispettivamente con i periodi simili (f, λ), (f, μ), (f, ν) etc., il suo valore sarà sempre riducibile alla forma

$$A + B(f, 1) + B'(f, g) + B''(f, g^2) + ... + B^{\varepsilon}(f, g^{e-1})$$

e i coefficienti A, B, B' etc. saranno interi se tutti i coefficienti di F sono interi. Se invece sostituiamo t, u, v etc. con $(f, k\lambda)$, $(f, k\mu)$, $(f, k\nu)$ etc. rispettivamente, il valore di F sarà ridotto a $A + B(f, k) + B'(f, kg) + \text{etc.}$

346.

TEOREMA. *Sia λ un numero non divisibile per n, e per brevità si indichi con p il periodo (f, λ), ogni periodo simile (f, μ), dove si suppone che anche μ non sia divisibile per n, può essere ridotto alla forma*

$$\alpha + \beta p + \gamma p^2 + ... + \theta p^{e-1}$$

in maniera tale che i coefficienti α, β etc. siano determinate quantità razionali.

Dimostrazione. Per motivi di brevità indicheremo gli $e-1$ periodi $(f, \lambda g)$, $(f, \lambda g^2)$, $(f, \lambda g^3)$ etc. fino a $(f, \lambda g^{e-1})$ con p', p'', p''' etc.: (f, μ) deve necessariamente coincidere con uno di questi. Si ha immediatamente l'equazione

$$0 = 1 + p + p' + p'' + p''' + \text{etc}.....(\text{I}).$$

Calcolando ora, in accordo con i precedenti articoli, le potenze di p fino alla $e-1$-ma, otteniamo altre $e-2$ equazioni

$$\begin{aligned}
0 &= p^2 + A + ap + a'p' + a''p'' + a'''p''' + \text{etc}...(\text{II}) \\
0 &= p^3 + B + bp + b'p' + b''p'' + b'''p''' + \text{etc}...(\text{III}) \\
0 &= p^4 + C + cp + c'p' + c''p'' + a'''p''' + \text{etc}...(\text{IV}) \text{ etc.}
\end{aligned}$$

dove tutti i coefficienti A, a, a' etc. B, b, b' etc. etc. saranno interi e, come segue immediatamente dai precedenti articoli, completamente indipendenti da λ; il che vale a dire che le stesse equazioni continuano a valere indipendentemente dal valore assegnato a λ. Questa osservazione può essere estesa anche all'equazione I se a λ si sostituiscono valori non divisibili per n. Supponiamo che $(f, \mu) = p'$; è facile poi vedere che se (f, μ) è uguale ad uno degli altri periodi tra p'', p''' etc., i calcoli seguenti possono essere applicati in maniera del tutto analoga. Poiché il numero delle equazioni I, II, III etc. è $e-1$, le quantità p'', p''' etc., il cui numero è $= e-2$, possono essere eliminate secondo metodi noti, in maniera tale che l'equazione risultante (Z)

$$0 = \mathsf{A} + \mathsf{B}\,p + \mathsf{C}p^2 + \text{etc}. + \mathsf{M}\,p^{e-1} + \mathsf{N}p'.$$

sia libera da essi. Questo può essere fatto in maniera tale che i coefficienti A, B, … N siano interi e certamente non tutti $= 0$. Ora se qui non è $\mathsf{N} = 0$, può essere determinato p' come è stato enunciato nel teorema. Non resta che provare, come faremo, che non può essere $\mathsf{N} = 0$.

Supponendo $\mathsf{N} = 0$, l'equazione Z diventa $\mathsf{M}\,p^{e-1} + \text{etc}. + \mathsf{B}\,p + \mathsf{A} = 0$, la quale, poiché non supera di certo il grado $e-1$, non può essere soddisfatta da più di $e-1$ valori diversi dello stesso p. Ma poiché le equazioni da cui Z è stata dedotta, sono indipendenti da λ, segue che anche Z non dipende da λ,

ovvero essa ha luogo per un qualsiasi valore intero di λ non divisibile per n. Per cui l'equazione Z è soddisfatta da ciascuna delle e somme $(f, 1)$, (f, g), (f, g^2), … (f, g^{e-1}), ad una delle quali p è uguale, e quindi segue che tali somme non possono essere tutte distinte, ma che almeno due di esse sono uguali. Supponiamo che una delle due somme uguali contenga le radici $[\zeta]$, $[\zeta']$, $[\zeta'']$ etc., e l'altra $[\eta]$, $[\eta']$, $[\eta'']$ etc., e supponiamo (il che è legittimo) che tutti i numeri ζ, ζ', ζ'' etc., η, η', η'' etc. siano positivi e $< n$. Chiaramente essi sono diversi tra loro e nessuno è $= 0$. Indichiamo con Y la funzione

$$x^{\zeta} + x^{\zeta'} + x^{\zeta''} + \text{etc.} - x^{\eta} - x^{\eta'} - x^{\eta''} - \text{etc.}$$

Il suo termine di grado massimo non supera x^{n-1} ed è $Y = 0$ se si pone $x = [1]$. Allora Y contiene il fattore $x - [1]$ in *comune* con quella funzione che precedentemente abbiamo indicato con X : ciò in verità è assurdo, come sarà facilmente dimostrato. Se infatti Y ed X avessero un fattore comune, il *massimo* comun divisore delle funzioni X ed Y (che di certo non può raggiungere le $n-1$ dimensioni poiché Y è divisibile per x), avrebbe coefficienti tutti razionali, come è chiaro dalla natura delle operazioni per la ricerca del massimo comun divisore tra due funzioni i cui coefficienti sono razionali. Ma nell'articolo 341 abbiamo mostrato che X non può avere un fattore di grado minore di $n-1$ a coefficienti razionali: quindi la supposizione che $\mathsf{N} = 0$ è inconsistente.

Esempio. Per $n = 19$, $f = 6$, diviene $p^2 = 6 + 2p + p' + 2p''$, inoltre da $0 = 1 + p + p' + p''$ si deduce $p' = 4 - p^2$, $p'' = -5 - p - p^2$. Per cui

$$\begin{aligned}
(6, 2) &= 4 - (6, 1)^2, \quad & (6, 4) &= -5 - (6, 1) + (6, 1)^2 \\
(6, 4) &= 4 - (6, 2)^2, \quad & (6, 1) &= -5 - (6, 2) + (6, 2)^2 \\
(6, 1) &= 4 - (6, 4)^2, \quad & (6, 2) &= -5 - (6, 4) + (6, 4)^2
\end{aligned}$$

347.

TEOREMA. *Se* $F = \varphi(t, u, v...)$ *è una funzione algebrica razionale intera invariabile* *) *nelle* f *indeterminate* t, u, v *etc., e se al posto di queste sostituiamo le* f *radici contenute nel periodo* (f, λ), *il valore della* F *si riduce alla forma*

$$A + A'[1] + A''[2] + \text{etc.} = W$$

per quanto detto nell'articolo 340: in questa espressione le radici che appartengono allo stesso periodo di f *termini avranno coefficienti uguali.*

Dimostrazione. Siano $[p]$, $[q]$ due radici appartenenti allo stesso periodo, e supponiamo che p, q siano positivi e minori di n. Dobbiamo dimostrare che $[p]$ e $[q]$ hanno lo stesso coefficiente in W. Sia $q \equiv pg^{\nu e} \pmod{n}$; siano $[\lambda]$, $[\lambda']$, $[\lambda'']$ etc. le radici contenute in (f, λ), dove supponiamo i numeri λ, λ', λ'' etc. positivi e minori di n; siano poi i minimi residui positivi dei numeri $\lambda g^{\nu e}$, $\lambda' g^{\nu e}$, $\lambda'' g^{\nu e}$ etc. i numeri μ, μ', μ'', secondo il modulo n. Questi ultimi sono identici, in ordine trasposto, ai numeri λ, λ', λ'' etc. Già dall'articolo 340 è chiaro che

$$\varphi\left(\left[\lambda g^{\nu e}\right], \left[\lambda' g^{\nu e}\right], \left[\lambda'' g^{\nu e}\right] ...\right) = (\mathrm{I})$$

può essere ridotta a

$$A + A'\left[g^{\nu e}\right] + A''\left[2g^{\nu e}\right] + \text{etc.} \qquad \text{od a} \qquad A + A'[\theta] + A''[\theta'] + \text{etc.} = (W'),$$

---

*) Le funzioni invariabili sono quelle in cui le indeterminate sono contenute tutte nello stesso modo, ovvero, in maniera più semplice, quelle che non subiscono cambiamenti in qualsiasi modo vengano permutate tra loro le indeterminate; ne sono esempio la somma di esse, il loro prodotto, la somma dei prodotti di tutte le coppie di essi etc.

indicando con θ, θ' etc. i minimi residui dei numeri g^{ve}, $2g^{ve}$ etc. secondo il modulo n, da cui è manifesto che $[q]$ ha in (W') lo stesso coefficiente che ha $[p]$ in (W). È facile convincersi che manipolando l'espressione (I), si ottiene la stessa cosa che si ottiene manipolando $\varphi([\mu], [\mu'], [\mu''] \text{ etc.})$, essendo $\mu \equiv \lambda g^{ve}$, $\mu' \equiv \lambda' g^{ve}$ etc. $(\mathrm{mod.}\, n)$. Ora questa espressione produce lo stesso risultato di $\varphi([\lambda], [\lambda'], [\lambda''] \text{ etc.})$, poiché i numeri μ, μ', μ'' differiscono da λ, λ', λ'' etc. solo nell'ordine, che in una funzione invariabile non importa.

Di qui si ha infine che W coincide del tutto con W' e che la radice $[q]$ ha in W lo stesso coefficiente di $[p]$. Q.E.D.

Vediamo così che W può essere ridotto alla forma

$$A + a(f, 1) + a'(f, g) + a''(f, g^2) \ldots + a^{\varepsilon}(f, g^{e-1}),$$

in maniera tale che i coefficienti A, $a \ldots a^{\varepsilon}$ sono quantità determinate intere se tutti i coefficienti razionali in F sono interi. Così per esempio se $n = 19$, $f = 6$, $\lambda = 1$ e la funzione φ rappresenta la somma del prodotto delle coppie delle indeterminate, il suo valore si riduce a $3 + (6, 1) + (6, 4)$.

Inoltre si prova facilmente che se sostituiamo t, u, v etc. con le radici di un altro periodo $(f, k\lambda)$, il valore della F diventa

$$A + a(f, k) + a'(f, kg) + a''(f, kg^2) + \text{etc.}$$

348.

Nell'equazione

$$x^f - \alpha x^{f-1} + \beta x^{f-2} - \gamma x^{f-3} \ldots$$

i coefficienti α, β, γ etc. sono funzioni invariabili delle radici, ad esempio α è la somma di tutte esse, β la somma dei prodotti delle radici prese a due a due, γ la somma dei prodotti delle radici prese a tre a tre etc. Dunque in un'equazione le cui radici sono quelle contenute nel periodo (f, λ), il primo coefficiente sarà uguale ad (f, λ) ed ognuno dei rimanenti può essere ridotto alla forma

$$A + a(f, 1) + a'(f, g) \ldots + a^{\varepsilon}(f, g^{e-1}),$$

dove A, a, a' sono interi. Inoltre è evidente che l'equazione le cui radici sono quelle contenute in un qualsiasi altro periodo $(f, k\lambda)$, può essere ottenuta dalla precedente sostituendo nei singoli coefficienti $(f, 1)$ con (f, k), (f, g) con (f, kg) ed in generale (f, p) con (f, kp). In questo modo possiamo assegnare e equazioni $z = 0$, $z' = 0$, $z'' = 0$ etc., le cui radici sono le radici contenute in $(f, 1)$, in (f, g), (f, g^2) etc., non appena sono note le e somme $(f, 1)$, (f, g), (f, g^2) etc., o meglio non appena si trova *una* di esse, poiché per l'articolo 346 da una possono essere ricavate le altre razionalmente. Fatto questo, la funzione X sarà risolta nel prodotto di e fattori di f dimensioni: infatti il prodotto di z, z', z'' etc. è banalmente $= X$.

Esempio. Per $n = 19$ la somma di tutte le radici del periodo $(6, 1)$ è $= (6, 1) = \alpha$; la somma dei prodotti delle coppie sarà $= 3 + (6, 1) + (6, 4) = \beta$; similmente la somma dei prodotti delle terne verrà $= 2 + 2(6, 1) + (6, 2) = \gamma$; la somma del prodotto delle radici prese a quattro a quattro

$= 3 + (6, 1) + (6, 4) = \delta$; la somma dei prodotti delle radici prese a cinque a cinque $= (6, 1) = \varepsilon$; il prodotto di tutte è $= 1$; per cui l'equazione

$$z = x^6 - \alpha x^5 + \beta x^4 - \gamma x^3 + \delta x^2 - \varepsilon x + 1 = 0$$

ammette le radici contenute in $(6, 1)$. Se poi nei coefficienti α, β, γ etc. sostituiamo $(6, 1)$, $(6, 2)$, $(6, 4)$ rispettivamente con $(6, 2)$, $(6, 4)$, $(6, 1)$, si ottiene l'equazione $z' = 0$ che ammette le radici raccolte in $(6, 2)$; se la permutazione è applicata ancora una volta, abbiamo l'equazione $z'' = 0$ che contiene le radici di $(6, 4)$ ed il prodotto $zz'z''$ sarà $= X$.

349.

È spesso molto conveniente, soprattutto quando f è un numero grande, dedurre i coefficienti β, γ etc. dalla somma delle potenze delle radici seguendo il teorema di Newton. Segue infatti che la somma dei quadrati delle radici contenute in (f, λ) è $= (f, 2\lambda)$, la somma dei cubi $= (f, 3\lambda)$ etc. Scrivendo per motivi di brevità q, q', q'' etc. al posto di (f, λ), $(f, 2\lambda)$, $(f, 3\lambda)$ etc. sarà

$$\alpha = q, \quad 2\beta = \alpha q - q', \quad 3\gamma = \beta q - \alpha q' + q'' \quad \text{etc.}$$

dove il prodotto di due periodi per l'articolo 345 deve essere convertito subito nella somma di periodi. Così nel nostro esempio, scrivendo p, p', p'' al posto di $(6, 1)$, $(6, 2)$, $(6, 4)$; q, q', q'', q''', q''''', q'''''' saranno rispettivamente $= p$, p', p', p'', p', p''; quindi

$$\alpha = p, \quad 2\beta = p^2 - p' = 6 + 2p + 2p'$$
$$3\gamma = (3 + p + p'')\, p - pp' + p' = 6 + 6p + 3p'$$

$$4\delta = (2+2p+p')\,p - (3+p+p'') + pp' - p'' = 12+4p+4p'' \text{ etc.}$$

Tuttavia è sufficiente calcolare metà dei coefficienti, infatti non è difficile provare che gli ultimi sono uguali ai primi in ordine inverso; cioè l'ultimo $=1$, il penultimo $=\alpha$, il terzultimo $=\beta$ etc.; oppure in un altro modo gli ultimi possono essere dedotti dai primi sostituendo $(f,1)$, (f,g) etc. con $(f,-1)$, $(f,-g)$ etc. o con $(f,n-1)$, $(f,n-g)$ etc. Il primo caso ha luogo quando f è pari; l'altro quando f è dispari; l'ultimo coefficiente sarà sempre $=1$. La giustificazione di questa affermazione è contenute nel teorema dell'articolo 79, ma per motivi di brevità non ci soffermeremo ulteriormente su questo argomento.

350.

TEOREMA. *Sia* $n-1$ *il prodotto di tre numeri interi positivi* α, β, γ *e sia il periodo* $(\beta\gamma,\lambda)$, *di* $\beta\gamma$ *termini, costituito dai periodi minori di* γ *termini* (γ,λ), (γ,λ'), (γ,λ'') *etc. Supponiamo che in una funzione di* β *indeterminate, simile a quella presa nell'articolo 347, ad esempio* $F=\varphi(t,u,v...)$, *vengano sostituite le indeterminate* t, u, v *etc. con le somme* (γ,λ), (γ,λ'), (γ,λ'') *etc. rispettivamente, il suo valore per i risultati dell'articolo 345.IV si riduce ad*

$$A + a(\gamma,1) + a'(\gamma,g) ... + a^{\zeta}\left(\gamma, g^{\alpha\beta-\alpha}\right) ... + a^{\theta}\left(\gamma, g^{\alpha\beta-1}\right) = W.$$

Allora dico che, se F *è una funzione invariabile, i periodi in* W *che sono contenuti nello stesso periodo di* $\beta\gamma$ *termini (cioè in generale i periodi* $\left(\gamma, g^{\mu}\right)$ *e* $\left(\gamma, g^{\alpha\nu+\mu}\right)$ *dove* ν *è un intero qualsiasi) avranno gli stessi coefficienti.*

Dimostrazione. Poiché il periodo $(\beta\gamma, \lambda g^{\alpha})$ coincide con $(\beta\gamma, \lambda)$, i periodi più piccoli $(\gamma, \lambda g^{\alpha})$, $(\gamma, \lambda' g^{\alpha})$, $(\gamma, \lambda'' g^{\alpha})$ etc., dai quali il primo è costituito, necessariamente coincidono con quelli da cui è formato il secondo sebbene in ordine diverso. Per cui, se sostituite t, u, v etc. ordinatamente con essi, F si trasforma in W', W' coincide con W. Ma per l'articolo 347 sarà

$$\begin{aligned} W' &= A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) \ldots + a^{\zeta}(\gamma, g^{\alpha\beta}) \ldots + a^{\theta}(\gamma, g^{\alpha\beta+\alpha-1}) \\ &= A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) \ldots + a^{\zeta}(\gamma, 1) \ \ldots \ + a^{\theta}(\gamma, g^{\alpha-1}) \end{aligned}$$

e quindi, poiché questa espressione deve coincidere con W, il primo coefficiente, il secondo, il terzo etc. in W (partendo da a), necessariamente coincidono con l'$\alpha+1$-esimo, l'$\alpha+2$-esimo, l'$\alpha+3$-esimo etc. Senza difficoltà possiamo concludere che in generale che i coefficienti dei periodi (γ, g^{μ}), $(\gamma, g^{\alpha+\mu})$, $(\gamma, g^{2\alpha+\mu}) \ldots$ $(\gamma, g^{\nu\alpha+\mu})$, che sono il $\mu+1$-esimo, l'$\alpha+\mu+1$-esimo, il $2\alpha+\mu+1$-esimo … il $\nu\alpha+\mu+1$-esimo, coincideranno tra loro. Q.E.D.

È chiaro allora che W può essere ridotta alla forma

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) \ldots + a^{\varepsilon}(\beta\gamma, g^{\alpha-1})$$

in cui tutti i coefficienti A, a etc. saranno interi, se tutti i coefficienti in F lo sono. È facile convincersi che, se successivamente sostituiamo in F al posto delle indeterminate, β periodi di γ termini contenuti in un altro periodo di $\beta\gamma$ termini, ad esempio $(\beta\gamma, \lambda k)$, che sono $(\gamma, \lambda k)$, $(\gamma, \lambda' k)$, $(\gamma, \lambda'' k)$ etc., allora il valore risultante sarà $A + a(\beta\gamma, k) + a'(\beta\gamma, gk) \ldots + a^{\varepsilon}(\beta\gamma, g^{\alpha-1}k)$. È ovvio che il teorema può essere anche esteso al caso in cui $\alpha\beta = 1$, ovvero $\beta\gamma = n-1$: in tal caso tutti i coefficienti di W saranno uguali e W assumerà la forma $A + a(\beta\gamma, 1)$.

351.

Conservando ora i simboli utilizzati negli articoli precedenti, è chiaro che ogni coefficiente dell'equazione, le cui radici sono le β somme (γ, λ), (γ, λ'), (γ, λ'') etc., può essere ridotto alla forma

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) \ldots + a^{\varepsilon}(\beta\gamma, g^{\alpha-1}),$$

e i numeri A, a etc. saranno tutti interi. Inoltre si può ottenere da quella, l'equazione le cui radici sono i β periodi di γ termini contenuti in un altro periodo $(\beta\gamma, k\lambda)$, sostituendo in ciascun coefficiente un qualsiasi periodo $(\beta\gamma, \mu)$ con $(\beta\gamma, k\mu)$. Se poi $\alpha = 1$, tutti i β periodi di γ termini saranno determinati da un'equazione di grado β, i cui coefficienti saranno della forma $A + a(\beta\gamma, 1)$, *e quindi sono quantità note*, poiché $(\beta\gamma, 1) = (n-1, 1) = -1$. Se invece $\alpha > 1$, i coefficienti dell'equazione le cui radici sono tutti i periodi di γ termini contenuti in un periodo di $\beta\gamma$ termini, saranno quantità note non appena sono noti i valori numerici di tutti gli α periodi di $\beta\gamma$ termini. Il calcolo dei coefficienti di queste equazioni sarà spesso più comodo, soprattutto quando β non è molto piccolo, se prima vengono calcolate le somme delle potenze delle radici e deduciamo da queste i coefficienti, grazie al teorema di Newton, proprio come abbiamo fatto sopra nell'articolo 349.

Esempio I. Sia richiesta, per $n = 19$, l'equazione le cui radici siano le somme $(6, 1)$, $(6, 2)$, $(6, 4)$. Indicando tali radici con p, p', p'' rispettivamente, e l'equazione richiesta con

$$x^3 - Ax^2 + Bx - C = 0$$

sarà

$$A = p + p' + p'', \quad B = pp' + pp'' + p'p'', \quad C = pp'p''.$$

Quindi

$$A = (18, 1) = -1$$

e

$$pp' = p + 2p' + 3p'', \quad pp'' = 2p + 3p' + p'', \quad p'p'' = 3p + p' + 2p''.$$

Da cui

$$B = 6(p + p' + p'') = 6(18, 1) = -6$$

ed infine

$$C = (p + 2p' + 3p'')\, p'' = 3(6, 0) + 11(p + p' + p'') = 18 - 11 = 7$$

quindi l'equazione richiesta sarà

$$x^3 + x^2 - 6x - 7 = 0.$$

Usando un altro metodo abbiamo

$$p + p' + p'' = -1$$

$$p^2 = 6 + 2p + p' + 2p'', \quad p'^2 = 6 + 2p' + p'' + 2p, \quad p''^2 = 6 + 2p'' + p + 2p'$$

da cui

$$p^2 + p'^2 + p''^2 = 18 + 5(p + p' + p'') = 13$$

ed analogamente

$$p^3 + p'^3 + p''^3 = 36 + 34(p + p' + p'') = 2.$$

Così grazie al teorema di Newton la stessa equazione potrà essere ottenuta come prima.

II. Per $n=19$ si chiede l'equazione le cui radici sono le somme $(2,1)$, $(2,7)$, $(2,8)$. Indicando queste ultime rispettivamente con q, q', q'', si trova che

$$q+q'+q''=(6,1),\quad qq'+qq''+q'q''=(6,1)+(6,4),\quad qq'q''=2+(6,2),$$

e, conservando i simboli dell'esempio precedente, l'equazione richiesta sarà

$$x^3-px^2+(p+p'')x-2-p'=0.$$

L'equazione le cui radici sono le somme $(2,2)$, $(2,3)$, $(2,5)$, contenute in $(6,2)$, si ottengono dalla precedente sostituendo p, p', p'' con p', p'', p rispettivamente. Se effettuiamo la stessa sostituzione ancora una volta, otteniamo l'equazione le cui radici sono le somme $(2,4)$, $(2,6)$, $(2,9)$ contenute in $(6,4)$.

352.

I teoremi precedenti, assieme ai loro corollari, contengono i principi fondamentali della teoria intera: il metodo per trovare i valori delle radici di Ω potrà essere esaurito in poche parole.

Anzitutto dobbiamo prendere un numero g, che sia una radice primitiva della congruenza modulo n, e calcolare i minimi residui delle potenze di g fino a g^{n-2} modulo n. Dobbiamo poi decomporre $n-1$ in fattori, e poi in fattori primi se vogliamo ridurre il problema ad equazioni di grado minore possibile. Siano questi (l'ordine è arbitrario) α, β, γ … ζ, e poniamo

$$\frac{n-1}{\alpha}=\beta\gamma\ldots\zeta=a,\quad \frac{n-1}{\alpha\beta}=\gamma\ldots\zeta=b,\quad \text{etc.}$$

Distribuiamo tutte le radici di Ω in α periodi di a termini, ciascuno di questi di nuovo in β periodi di b termini, ciascuno di essi in γ periodi etc. Cerchiamo grazie agli articoli precedenti, un'equazione (A) di grado α, le cui radici sono le α somme di a termini i cui valori possono essere determinati risolvendo questa equazione.

Ma qui si presenta una difficoltà, poiché sembra incerto quale somma si debba porre uguale a quale radice dell'equazione (A); cioè quale radice debba essere denotata con $(a, 1)$, quale con (a, g), etc.: per tale problema possiamo presentare la seguente soluzione. Con $(a, 1)$ può essere designata una qualsiasi radice dell'equazione (A); poiché ogni radice di questa equazione è la somma di a radici di Ω, ed è del tutto indifferente quale radice di Ω si indichi con $[1]$, è lecito allora supporre che $[1]$ rappresenti una qualsiasi delle radici che costituiscono una data radice dell'equazione (A) così che tale radice dell'equazione (A) sarà $(a, 1)$. La radice $[1]$ non è in verità ancora del tutto determinata, ma, anche se essa rimane interamente arbitraria od indefinita, possiamo proporre per $[1]$ una qualsiasi radice tra quelle che realizzano $(a, 1)$. Non appena $(a, 1)$ è determinata, tutte le somme rimanenti di a termini possono essere dedotte razionalmente da essa (articolo 346). Così è chiaro che abbiamo bisogno di trovare solo una radice per mezzo di tale risoluzione. Allo stesso scopo possiamo anche utilizzare il seguente metodo meno diretto. Sia $[1]$ una radice determinata; ad esempio si ponga $[1] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$, con k intero scelto a piacere, non divisibile per n. Fatto questo, $[2]$, $[3]$ etc. indicheranno anch'esse radici determinate, quindi anche le somme $(a, 1)$, (a, g) etc. indicheranno quantità determinate. Ora calcolate queste quantità per mezzo di tavole di seni, con precisione tale da poter decidere quali sono i

maggiori e quali i minori, non ci sarà alcun dubbio su come distinguere ciascuna radice dell'equazione (A).

Quando in tal modo abbiamo trovato tutte le α somme di a termini, cercheremo, servendoci degli articoli precedenti, l'equazione (B) di grado β, le cui radici sono le β somme di b termini contenute in $(a, 1)$. I coefficienti di questa equazione sono tutti delle quantità note. Dunque, poiché è arbitrario quale delle $\alpha = \beta b$ radici contenute in $(a, 1)$ sia denotata con $[1]$, ogni radice data dell'equazione (B) può essere espressa per mezzo di $(b, 1)$, poiché è lecito supporre che una delle b radici, da cui essa è composta sia denotata con $[1]$. Cercheremo allora una qualsiasi radice dell'equazione (B) risolvendo quest'ultima, la porremo $= (b, 1)$, e deriveremo per l'articolo 346 tutti le restanti somme di b termini. Allo questo modo abbiamo allo stesso tempo un modo per confermare il calcolo, poiché quelle somme di b termini, che appartengono allo stesso periodo di a termini, devono risultare delle somme note. In alcuni casi è parimenti semplice costruire altre $\alpha - 1$ equazioni di grado β, le cui radici sono rispettivamente le singole β somme di b termini contenute nei rimanenti periodi di a termini (a, g), (a, g^2) etc., e cercare *tutte* le radici mediante la risoluzione di queste equazioni e dell'equazione B. Allora proprio come sopra con l'aiuto delle tavole dei seni possiamo decidere quali sono i periodi di b termini a cui sono uguali le singole radici trovate in tal modo. In aiuto a tale decisione possono intervenire tanti altri artifici, che non è possibile illustrare qui completamente. Uno di essi tuttavia, quando $\beta = 2$, è molto utile e può essere spiegato più brevemente con gli esempi che non con la teoria. Lo presenteremo nei seguenti esempi.

Dopo che in tal modo abbiamo trovato i valori di tutte le $\alpha\beta$ somme di b termini, in maniera simile a questa potranno essere trovate le $\alpha\beta\gamma$ somme di c termini per mezzo di equazioni di grado γ. Cioè possiamo *o da un lato* trovare *una* equazione di grado γ le cui radici, in base all'articolo 350, sono le γ

somme di c termini contenute in $(b, 1)$ e per mezzo della sua risoluzione trovare una qualsiasi radice e porla $=(c, 1)$ così da trovare infine, con i metodi dell'articolo 346, tutte le rimanenti somme simili; *oppure dall'altro* in modo simile possiamo sviluppare le $\alpha\beta$ equazioni di grado γ le cui radici sono rispettivamente le γ somme di c termini contenute nei singoli periodi di b termini. Possiamo poi risolvere tutte queste equazioni per determinare tutte le loro radici e, con l'aiuto di una tavola dei seni, determinare l'ordine di queste. Tuttavia, per $\gamma = 2$ possiamo usare l'artificio che dimostreremo più in basso.

Se continuiamo in questo modo alla fine avremo tutte le $\frac{n-1}{\zeta}$ somme di ζ termini; e se, con il metodo dell'articolo 348, troviamo l'equazione di grado ζ le cui radici sono le ζ radici di Ω contenute in $(\zeta, 1)$, tutti i suoi coefficienti saranno quantità note. Se poi risolviamo l'equazione così da ricavare una delle sue radici, possiamo porre questa $=[1]$ e le sue potenze ci daranno tutte le radici di Ω. Se più piace, possiamo ricavare *tutte* le radici di questa equazione risolvendola; in particolare con la risoluzione di altre $\frac{n-1}{\zeta} - 1$ equazioni di grado ζ, che contengono rispettivamente tutte le ζ radici in ciascuno dei rimanenti periodi di ζ termini, possiamo trovare tutte le radici restanti di Ω.

È chiaro che, non appena viene risolta la prima equazione (A), oppure abbiamo i valori di tutte le α somme di a termini, otteniamo anche la decomposizione della funzione X in α fattori di a dimensioni, per l'articolo 348. Inoltre, dopo aver risolto l'equazione (B) o dopo aver trovato i valori di tutte le $\alpha\beta$ somme di b termini, ciascuno di quei fattori verrà risolto nuovamente in β fattori, cioè X sarà risolto in $\alpha\beta$ fattori di b dimensioni etc.

353.

Primo esempio per $n=19$. Poiché in questo caso si ha $n-1=3\cdot 3\cdot 2$, la ricerca delle radici di Ω si riconduce alla soluzione di due equazioni cubiche e di una quadratica. Questo esempio può essere seguito più facilmente, poiché le operazioni necessarie sono in massima parte contenute negli articoli precedenti. Prendendo come radice primitiva g il numero 2, i minimi residui delle sue potenze saranno questi (gli esponenti delle potenze sono scritti nella prima linea sopra ai residui):

0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17
1.	2.	4.	8.	16.	13.	7.	14.	9.	18.	17.	15.	11.	3.	6.	12.	5.	10

Di qui, grazie agli articoli 344, 345, si deduce facilmente la distribuzione seguente di tutte le radici Ω in tre periodi di sei termini, ciascuno dei quali in tre periodi di due termini:

$$\Omega=(18,1)\left\{\begin{array}{ll}(6,1)\left\{\begin{array}{lll}(2,\ 1) & \ldots & [1],\ [18]\\ (2,\ 8) & \ldots & [8],\ [11]\\ (2,\ 7) & \ldots & [7],\ [12]\end{array}\right.\\ (6,2)\left\{\begin{array}{lll}(2,\ 2) & \ldots & [2],\ [17]\\ (2,16) & \ldots & [3],\ [16]\\ (2,14) & \ldots & [5],\ [14]\end{array}\right.\\ (6,4)\left\{\begin{array}{lll}(2,\ 4) & \ldots & [4],\ [15]\\ (2,13) & \ldots & [6],\ [13]\\ (2,\ 9) & \ldots & [9],\ [10]\end{array}\right.\end{array}\right.$$

L'equazione (A) le cui radici sono le somme $(6,1)$, $(6,2)$, $(6,4)$, è $x^3+x^2-6x-7=0$, ed una delle sue radici è $-1,2218761623$. Indicando questa con $(6,1)$ sarà

$$(6,\ 2) = 4 - (6,\ 1)^2 = 2,5070186441$$

$$(6,\ 4) = -5 - (6,\ 1) + (6,\ 1)^2 = -2,2851424818.$$

Quindi X viene risolta in tre fattori di 6 dimensioni, se questi valori sono sostituiti nell'articolo 348.

L'equazione (B) le cui radici sono le somme $(2,\ 1)$, $(2,\ 7)$, $(2,\ 8)$, restituisce questa

$$x^3 - (6,\ 1)x^2 + \big[(6,\ 1) + (6,\ 4)\big]x - 2 - (6,\ 2) = 0$$

ovvero

$$x^3 + 1,2218761623x^2 - 3,5070186441x - 4,5070186441 = 0\,,$$

di cui una radice è $-1,3545631433$, che chiameremo $(2,\ 1)$. Con i metodi dell'articolo 346 otteniamo le equazioni seguenti, dove per brevità scriveremo q al posto di $(2,\ 1)$:

$$(2,\ 2) = q^2 - 2\,,\quad (2,\ 3) = q^3 - 3q\,,\quad (2,\ 4) = q^4 - 4q^2 + 2\,,\quad (2,\ 5) = q^5 - 5q^3 + 5q$$

$$(2,\ 6) = q^6 - 6q^4 + 9q^2 - 2\,,\qquad (2,\ 7) = q^7 - 7q^5 + 14q^3 - 7q$$

$$(2,\ 8) = q^8 - q^6 + 20q^4 - 16q^2 + 2\quad (2,\ 9) = q^9 - 9q^7 + 27q^5 - 30q^3 + 9q$$

Tali equazioni, in questo caso, possono essere risolte più semplicemente di quanto detto nel metodo dell'articolo 346, in base alle osservazioni seguenti. Supponendo che

$$[1] = \cos\frac{kP}{19} + i\sin\frac{kP}{19}$$

si ottiene

$[18] = \cos\frac{18kP}{19} + i\sin\frac{18kP}{19} = \cos\frac{kP}{19} - i\sin\frac{kP}{19}$ e quindi $(2, 1) = 2\cos\frac{kP}{19}$; più in generale:

$[\lambda] = \cos\frac{\lambda kP}{19} + i\sin\frac{\lambda kP}{19}$ e quindi $(2, \lambda) = [\lambda] + [18\lambda] = [\lambda] + [-\lambda] = 2\cos\frac{\lambda kP}{19}$

Per cui se $\frac{1}{2}q = \cos\omega$, sarà $(2, 2) = 2\cos 2\omega$, $(2, 3) = 2\cos 3\omega$ etc., così grazie alle ben note formule sui coseni degli angoli di angoli multipli si ottengono le stesse formule di sopra. Già da queste formule possiamo derivare i seguenti valori numerici:

$(2, 2) = -0{,}1651586909$	$(2, 6) = \ \ 0{,}4909709743$
$(2, 3) = \ \ 1{,}5782810188$	$(2, 7) = -1{,}7589475024$
$(2, 4) = -1{,}9727226068$	$(2, 8) = \ \ 1{,}8916344834$
$(2, 5) = \ \ 1{,}0938963162$	$(2, 9) = -0{,}8033908493$

I valori degli stessi $(2, 7)$ e $(2, 8)$ possono anche essere ricavati dall'equazione (B), della quale rappresentano le due restanti radici. Il dubbio su *quale* sia $(2, 7)$ e quale $(2, 8)$ può essere eliminato o con dei calcoli approssimati secondo le formule precedenti, oppure per mezzo delle tavole dei seni, che se consultate, mostrano che $(2, 1) = 2\cos\omega$ ponendo $\omega = \frac{7P}{19}$ e così abbiamo

$$(2, 7) = 2\cos\frac{49}{19}P = 2\cos\frac{8}{19}P \quad \text{e} \quad (2, 8) = 2\cos\frac{56}{19}P = 2\cos\frac{1}{19}P\,.$$

Similmente possiamo trovare le somme $(2, 2)$, $(2, 3)$, $(2, 5)$ anche dall'equazione

$$x^3-(6,\,2)x^2+\big[(6,\,1)+(6,\,2)\big]x-2-(6,\,4)=0\,,$$

di cui sono radici, ed il dubbio circa quale radice corrisponda a quale somma può essere rimosso esattamente con lo stesso metodo di prima. Infine le somme $(2,\,4)$, $(2,\,6)$, $(2,\,9)$ possono essere trovate con l'equazione

$$x^3-(6,\,4)x^2+\big[(6,\,2)+(6,\,4)\big]x-2-(6,\,1)=0\,.$$

Ad ultimo $[1]$ e $[18]$ sono le radici dell'equazione $x^2-(2,\,1)x+1=0$, una delle quali sarà $=\frac{1}{2}(2,\,1)+i\sqrt{1-\frac{1}{4}(2,\,1)^2}=\frac{1}{2}(2,\,1)+i\sqrt{\frac{1}{2}-\frac{1}{4}(2,\,2)}$, l'altra $=\frac{1}{2}(2,\,1)-i\sqrt{\frac{1}{2}-\frac{1}{4}(2,\,2)}$.

I valori numerici saranno $=-0,6772815716\pm 0,7357239107\;i$.

Le sedici rimanenti radici possono essere trovate o dalle potenze di una o dell'altra di queste radici oppure risolvendo altre otto equazioni simili. Per decidere quale radice ha il segno positivo nella parte immaginaria e quale quello negativo possiamo usare il metodo seguente o le tavole dei seni oppure ancora il trucco che sarà illustrato nell'esempio seguente. In tal modo troveremo tutti i valori seguenti con il segno superiore corrispondente alla prima radice e quello in basso alla seconda:

$$\begin{aligned}
[1]\ \text{e}\ [18]\ &= -0,6772815716 \pm 0,7357239107\,i\\
[2]\ \text{e}\ [17]\ &= -0,0825793455 \mp 0,9965844930\,i\\
[3]\ \text{e}\ [16]\ &= 0,7891405094 \pm 0,6142127127\,i\\
[4]\ \text{e}\ [15]\ &= -0,9863613034 \pm 0,1645945903\,i\\
[5]\ \text{e}\ [14]\ &= 0,5469481581 \mp 0,8371664783\,i\\
[6]\ \text{e}\ [13]\ &= 0,2454854871 \pm 0,9694002659\,i
\end{aligned}$$

$$[7] \quad \text{e} \quad [12] \quad = -0,8794737512 \mp 0,4759473930\, i$$

$$[8] \quad \text{e} \quad [11] \quad = \quad 0,9458172418 \mp 0,3246994692\, i$$

$$[9] \quad \text{e} \quad [10] \quad = -0,4016954247 \pm 0,9157733267\, i$$

354.

Secondo esempio per $n = 17$. Qui $n-1 = 2\cdot 2\cdot 2\cdot 2$ così il calcolo delle radici di Ω sarà ricondotto alla risoluzione di quattro equazioni quadratiche. Come radice primitiva scegliamo 3. I minimi residui delle sue potenze relative al modulo 17 sono le seguenti:

0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15
1.	3.	9.	10.	13.	5.	15.	11.	16.	14.	8.	7.	4.	12.	2.	6

Da questi deriviamo la seguente distribuzione del complesso Ω in due periodi di otto termini, quattro di quattro termini, due di otto termini:

$$\Omega = (16,1)\begin{cases} (8,1)\begin{cases} (4,1)\begin{cases} (2,1)\ldots[1], & [16] \\ (2,13)\ldots[4], & [13] \end{cases} \\ (4,9)\begin{cases} (2,9)\ldots[8], & [9] \\ (2,15)\ldots[2], & [15] \end{cases} \end{cases} \\ (8,3)\begin{cases} (4,3)\begin{cases} (2,3)\ldots[3], & [14] \\ (2,5)\ldots[5], & [12] \end{cases} \\ (4,10)\begin{cases} (2,10)\ldots[7], & [10] \\ (2,11)\ldots[6], & [11] \end{cases} \end{cases} \end{cases}$$

L'equazione (A) le cui radici sono le somme $(8,1)$, $(8,3)$ si trova essere, in base ai metodi dell'articolo 351, l'equazione $x^2 + x - 4 = 0$. Le sue radici

sono $-\frac{1}{2}+\frac{1}{2}\sqrt{17}=1,5615528128$, e $-\frac{1}{2}-\frac{1}{2}\sqrt{17}=-2,5615528128$. Diciamo la prima $=(8,1)$ cosi l'altra è necessariamente $=(8,3)$.

L'equazione (B), le cui radici sono le somme $(4,1)$ e $(4,9)$, è $x^2-(8,1)x-1=0$, le sue radici sono

$$\frac{1}{2}(8,1)\pm\frac{1}{2}\sqrt{4+(8,1)^2}=\frac{1}{2}(8,1)\pm\frac{1}{2}\sqrt{12+3(8,1)+4(8,3)}.$$

Porremo $(4,1)$ uguale alla quantità che ha il segno positivo davanti al radicale, il suo valore numerico è $2,0494811777$. Così la quantità con il radicale negativo, il cui valore numerico è $-0,4879283649$ sarà espressa da $(4,9)$. Le somme rimanenti di quattro termini, $(4,3)$ e $(4,10)$, possono essere calcolate in due modi. Il *primo* consiste nel metodo dell'articolo 346, che fornisce le formule seguenti quando abbreviamo $(4,1)$ con p:

$$\begin{aligned}(4,3) &= -\frac{3}{2}+3p-\frac{1}{2}p^3 &&= 0,3441507314\\ (4,10) &= \frac{3}{2}+2p-p^2-\frac{1}{2}p^3 &&= -2,9057035442\end{aligned}$$

Lo stesso metodo dà la formula $(4,9)=-1-6p+p^2+p^3$ e da essa otteniamo gli stessi valori trovati prima.

Il *secondo* metodo ci permette di determinare le somme $(4,3)$, $(4,10)$ risolvendo l'equazione di cui sono radici. L'equazione è $x^2-(8,3)x-1=0$, le sue radici sono $\frac{1}{2}(8,3)\pm\sqrt{4+(8,3)^2}$ o $\frac{1}{2}(8,3)+\frac{1}{2}\sqrt{12+4(8,1)+3(8,3)}$ e $\frac{1}{2}(8,3)-\frac{1}{2}\sqrt{12+4(8,1)+3(8,3)}$. Possiamo rimuovere il dubbio su *quale* radice deve rappresentare $(4,3)$ e quale $(4,10)$ secondo il seguente

accorgimento che abbiamo menzionato nell'articolo 352. Calcoliamo il prodotto di $(4,1)-(4,9)$ per $(4,3)-(4,10)$, che è $=2(8,1)-2(8,3)$.*) Chiaramente il valore di questa espressione è positivo ed è $=+2\sqrt{17}$ e, poiché il primo fattore del prodotto, $(4,1)-(4,9)=+\sqrt{12}+3(8,1)+4(8,3)$, è positivo, l'altro fattore, $(4,3)-(4,10)$ deve anch'esso essere positivo. Allora $(4,3)$ è uguale alla *prima* radice che ha il segno positivo davanti al radicale, e $(4,10)$ è uguale alla seconda radice. Da ciò deduciamo gli stessi valori numerici di sopra.

Avendo trovato tutte le somme di quattro termini, passiamo a quelle di due termini. L'equazione (C) le cui radici sono $(2,1)$, $(2,13)$, contenute in $(4,1)$, sarà $x^2-(4,1)x+(4,3)=0$. Le sue radici sono $\frac{1}{2}(4,1)\pm\frac{1}{2}\sqrt{-4(4,3)+(4,1)^2}$ ovvero $\frac{1}{2}(4,1)\pm\frac{1}{2}\sqrt{4+(4,9)-2(4,3)}$: porremo $=(2,1)$ quella in cui la quantità radicale, il cui valore è $=1{,}8649444588$, è positiva, e $(2,13)$ sarà uguale all'altra, il cui valore è $=0{,}1845367189$. Se si preferisce cercare le somme rimanenti di due termini con il metodo dell'articolo 346, possiamo usare le stesse formule per $(2,2)$, $(2,3)$, $(2,4)$, $(2,5)$, $(2,6)$, $(2,7)$, $(2,8)$ come abbiamo fatto nell'esempio precedente per le quantità simili, e cioè, $(2,2)$, (ovvero $(2,15)$) $=(2,1)^2-2$ etc. Sembra tuttavia preferibile trovarle a coppie risolvendo un'equazione quadratica. Per $(2,9)$, $(2,15)$ abbiamo l'equazione $x^2-(4,9)x+(4,10)=0$ le cui radici sono $\frac{1}{2}(4,9)\pm\frac{1}{2}\sqrt{4+(4,1)-2(4,10)}$.

---

*) Il vero motivo di questo artificio sta nel fatto che possiamo prevedere a priori che il prodotto non contiene somme di quattro termini ma solo somme di otto termini. Il motivo di ciò, di facile comprensione per i più esperti, lo omettiamo qui per motivi di brevità.

Possiamo determinare quale segno usare in modo simile a quanto fatto sopra. Calcolando il prodotto di $(2,1)-(2,13)$ per $(2,9)-(2,15)$ otteniamo $-(4,1)+(4,9)-(4,3)+(4,10)$. Poiché esso è negativo ed il fattore $(2,1)-(2,13)$ è positivo, $(2,9)-(2,15)$ deve necessariamente essere negativo. Così dobbiamo usare il segno positivo per $(2,15)$ e quello negativo per $(2,9)$. Da questo troviamo che $(2,9)=-1,9659461994$, $(2,15)=1,4780178344$. Quindi, poiché calcolando il prodotto di $(2,1)-(2,13)$ per $(2,3)-(2,5)$ otteniamo la quantità positiva $(4,9)-(4,10)$, il fattore $(2,3)-(2,5)$ dev'esser positivo. Poi, per mezzo di un calcolo simile a quello fatto prima, si trova

$$\begin{aligned}(2,3)&=\frac{1}{2}(4,3)-\frac{1}{2}\sqrt{4+(4,10)-2(4,9)}=\ 0,8914767116\\(2,5)&=\frac{1}{2}(4,3)+\frac{1}{2}\sqrt{4+(4,10)-2(4,9)}=-0,5473259801\end{aligned}.$$

Infine con operazioni del tutto analoghe abbiamo

$$\begin{aligned}(2,10)&=\frac{1}{2}(4,10)-\frac{1}{2}\sqrt{4+(4,3)-2(4,1)}=-1,7004342715\\(2,11)&=\frac{1}{2}(4,10)+\frac{1}{2}\sqrt{4+(4,3)-2(4,1)}=-1,2052692728\end{aligned}.$$

Restano ora da trovare le radici stesse di Ω. L'equazione (D), le cui radici sono $[1]$ e $[16]$, diventa $x^2-(2,1)x+1=0$. Le radici di questa sono $\frac{1}{2}(2,1)\pm\frac{1}{2}\sqrt{(2,1)^2-4}$ o meglio $\frac{1}{2}(2,1)\pm\frac{1}{2}i\sqrt{4-(2,1)^2}$ o $\frac{1}{2}(2,1)\pm\frac{1}{2}i\sqrt{2-(2,15)}$. Prenderemo il segno superiore positivo per $[1]$, quello inferiore per $[16]$. Possiamo ottenere le restanti quattordici radici o dalle

potenze di $[1]$ oppure risolvendo sette equazioni quadratiche, ciascuna delle quali ci fornirà due radici, ed il dubbio circa il segno della quantità radicale può essere rimosso proprio come abbiamo fatto prima. Così $[4]$ e $[13]$ sono radici dell'equazione $x^2-(2,13)x+1=0$ e così uguali a $\frac{1}{2}(2,13)\pm\frac{1}{2}i\sqrt{2-(2,9)}$. Calcolando il prodotto di $[1]-[16]$ per $[4]-[13]$ tuttavia troviamo che $(2,5)-(2,3)$ è una quantità reale negativa. Quindi, poiché $[1]-[16]$ è $+i\sqrt{2-(2,15)}$, cioè è il prodotto dell'immaginaria i per un numero reale positivo, anche $[4]-[13]$ deve essere il prodotto di i per una quantità reale positiva giacché $i^2=-1$. Di conseguenza prenderemo il segno superiore per $[4]$ e quello negativo per $[13]$. In maniera simile per le radici $[8]$ e $[9]$ troviamo $\frac{1}{2}(2,9)\pm\frac{1}{2}i\sqrt{2-(2,1)}$; così, visto che il prodotto di $[1]-[16]$ per $[8]-[9]$ è $(2,9)-(2,10)$ ed è negativo, dobbiamo prendere il segno superiore positivo per $[8]$, quello inferiore $[9]$. Se calcoliamo poi le rimanenti radici otterremo i seguenti valori numerici, dove il segno superiore è da assegnare alla prima radice e quello inferiore alla seconda:

$$
\begin{aligned}
[1],\ [16] \quad \ldots \quad &= 0,9324722294 \pm 0,3612416662\,i \\
[2],\ [15] \quad \ldots \quad &= 0,7390089172 \pm 0,6736956436\,i \\
[3],\ [14] \quad \ldots \quad &= 0,4457383558 \pm 0,8951632914\,i \\
[4],\ [13] \quad \ldots \quad &= 0,0922683595 \pm 0,9957341763\,i \\
[5],\ [12] \quad \ldots \quad &= -0,2736629901 \pm 0,9618256432\,i \\
[6],\ [11] \quad \ldots \quad &= -0,6026346364 \pm 0,7980172273\,i \\
[7],\ [10] \quad \ldots \quad &= -0,8502171357 \pm 0,5264321629\,i \\
[8],\ [9] \quad \ldots \quad &= -0,9829730997 \pm 0,1837495178\,i
\end{aligned}
$$

Quanto precede basta a risolvere l'equazione $x^n - 1 = 0$ e così anche a trovare le funzioni trigonometriche corrispondenti agli archi che sono commensurabili con la circonferenza. Ma proprio per la sua importanza, non possiamo porre termine a questa disquisizione, senza prima aver aggiunto alcune osservazioni che illustrano l'argomento, e degli esempi che sono correlati o che dipendono da essa. Tra questi sceglieremo soprattutto quelli che possono essere risolti senza un grande apparato di ricerche secondarie, e considereremo essi solo come *casi particolari* di questa vasta teoria da trattare nei minimi dettagli in un secondo momento.

355.

Poiché supponiamo sempre che n sia dispari, 2 compare tra i fattori di $n-1$, e il complesso Ω sarà composto di $\frac{1}{2}(n-1)$ periodi di due termini. Un periodo di tal tipo $(2, \lambda)$ sarà fatto dalle radici $[\lambda]$ e $\left[\lambda g^{(n-1)/2}\right]$ dove come sopra g rappresenta una qualsiasi radice primitiva per il modulo n. Ma $g^{(n-1)/2} \equiv -1 \,(\mathrm{mod.}\, n)$ e così $\lambda g^{(n-1)/2} \equiv -\lambda$ (vedi l'articolo 62) e $\left[\lambda g^{(n-1)/2}\right] = [-\lambda]$. Quindi se supponiamo che $[\lambda] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$, e $[-\lambda] = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$, avremo che la somma $(2, \lambda) = 2\cos\frac{kP}{n}$. A questo punto possiamo soltanto trarre la conclusione che il valore di una qualsiasi somma di due termini è una quantità reale. Poiché ogni periodo che ha un numero pari di termini $= 2a$ può essere decomposto in a periodi di due termini, è chiaro in generale che il valore di una qualsiasi somma che ha un numero pari di termini è sempre una quantità reale. Quindi se nell'articolo 352 tra i fattori α, β, γ etc. lasciamo il 2 alla fine, tutte le operazioni saranno fatte su quantità

reali finché arriviamo ad una somma di due termini, e gli immaginari saranno introdotti quando passeremo dalle somme alle radici stesse.

356.

Dovremmo porre particolare attenzione alle equazioni ausiliarie per mezzo delle quali determiniamo, per un qualsiasi valore di n, le somme che formano il complesso Ω. Esse sono connesse in maniera sorprendente con le più nascoste proprietà del numero n. Qui ci restringeremo ai due seguenti casi. Nel *primo* caso tratteremo l'equazione quadratica le cui radici sono le somme di $\frac{1}{2}(n-1)$ termini, nel *secondo* caso, in cui $n-1$ ha il fattore 3, considereremo l'equazione cubica le cui radici sono somme di $\frac{1}{3}(n-1)$ termini.

Se per brevità scriviamo m al posto di $\frac{1}{2}(n-1)$ e indichiamo con g una radice primitiva per il modulo n, il complesso Ω consisterà di due periodi $(m, 1)$ e (m, g). Il primo conterrà le radici $[1]$, $[g^2]$, $[g^4]$ … $[g^{n-3}]$, il secondo le radici $[g]$, $[g^3]$, $[g^5]$ … $[g^{n-2}]$. Supponiamo che i minimi residui positivi dei numeri g^2, g^4 … g^{n-3} relativamente al modulo n siano, in ordine arbitrario, R, R', R'' etc. e che i residui di g, g^3, g^5 … g^{n-2} siano N, N', N'' etc. Allora le radici di cui consiste $(m, 1)$ coincidono con $[1]$, $[R]$, $[R']$, $[R'']$ etc. e le radici del periodo (m, g) con $[N]$, $[N']$, $[N'']$ etc. È chiaro che tutti i numeri 1, R, R', R'' etc. sono *residui quadratici* del numero n. Poiché sono tutti diversi e minori di n e poiché il loro numero è $=\frac{1}{2}(n-1)$, e quindi uguale al numero di tutti i residui positivi di *n* che sono più piccoli di *n* (articolo 96, N.d.T.), questi residui coincideranno completamente con quei numeri. Tutti i numeri N, N', N'' etc. sono diversi l'uno dall'altro e dai

numeri 1, R, R' etc. e assieme a questi restituiscono tutti i numeri 1, 2, $3\ldots$ $n-1$. Segue che i numeri N, N', N'' etc. devono coincidere con i *non-residui quadratici* positivi di n che sono più piccoli di n. Ora se supponiamo che l'equazione le cui radici sono le somme $(m, 1)$, (m, g) sia

$$x^2 - Ax + B = 0$$

abbiamo

$$A = (m, 1) + (m, g) = -1, \quad B = (m,1)\cdot(m, g)$$

Il prodotto di $(m, 1)$ per (m, g), per l'articolo 345, è

$$= (m, N+1) + (m, N'+1) + (m, N''+1) + \text{etc.} = W$$

e così sarà ridotto alla forma $\alpha(m, 0) + \beta(m, 1) + \gamma(m, g)$. Per determinare i coefficienti α, β, γ osserviamo *per prima cosa* che $\alpha + \beta + \gamma = m$ (poiché il numero di somme in W è $= m$); *in secondo luogo,* che $\beta = \gamma$ (questo segue dall'articolo 350 poiché il prodotto $(m,1)\cdot(m, g)$ è una funzione invariabile delle somme $(m, 1)$ e (m, g), di cui la somma più grande $(n-1, 1)$ è composta); *terzo* poiché tutti i numeri $N+1$, $N'+1$, $N''+1$ etc. sono contenuti tra i limiti 2 ed $n+1$ esclusi, è chiaro che *o* nessuna somma in W può essere ridotta ad $(m, 0)$, e così $\alpha = 0$ quando il numero $n-1$ non compare tra i numeri N, N', N'' etc.; *oppure* una somma, cioè (m, n), può essere ridotta ad $(m, 0)$, e così $\alpha = 1$ quando $n-1$ compare tra i numeri N, N', N'' etc. Nel primo caso quindi avremo $\alpha = 0$, $\beta = \gamma = \frac{1}{2}m$, nel secondo $\alpha = 1$, $\beta = \gamma = \frac{1}{2}(m-1)$. Segue che, poiché i numeri β e γ devono essere interi, il primo caso ha luogo, e cioè, $n-1$ (o, che è lo stesso, -1), non sarà contenuto

tra i non-residui di n, quando m è pari o n è della forma $4k+1$. Il secondo caso ha luogo, e cioè, $n-1$ o -1 sarà un non-residuo di n, quando m è dispari o n è della forma $4k+3$ *). Ora poiché $(m, 0) = m$, $(m, 1)+(m, g) = -1$ il prodotto che cercavamo sarà $= -\frac{m}{2}$ nel primo caso ed $= \frac{m+1}{2}$ nel secondo. Così l'equazione in quel caso sarà $x^2 + x - \frac{1}{4}(n-1) = 0$ con radici $-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$, in questo $x^2 + x + \frac{1}{4}(n+1) = 0$, le cui radici sono $-\frac{1}{2} \pm \frac{1}{2} i\sqrt{n}$.

Indipendentemente da quale radice di Ω venga scelta per rappresentare $[1]$, la differenza tra le somme $\sum[\mathsf{R}]$ ed $\sum[\mathsf{N}]$, dove al posto di R e di N devono essere sostituiti rispettivamente i residui ed i non-residui quadratici positivi di n che sono più piccoli di n, sarà $= \pm\sqrt{n}$ se $n \equiv 1$ ed $= \pm i\sqrt{n}$ se $n \equiv 3 \pmod 4$. Segue facilmente, denotando con k un qualsiasi intero non divisibile per n, che

$$\sum \cos \frac{k\mathsf{R}P}{n} - \sum \cos \frac{k\mathsf{N}P}{n} = \pm\sqrt{n} \quad \text{e} \quad \sum \sin \frac{k\mathsf{R}P}{n} - \sum \sin \frac{k\mathsf{N}P}{n} = 0$$

se $n \equiv 1 \pmod 4$; viceversa se $n \equiv 3 \pmod 4$ la prima differenza è $= 0$ e la seconda $= \pm\sqrt{n}$. Questi teoremi sono così eleganti che meritano particolare attenzione. Osserviamo che il segno superiore va sempre preso se k è l'unità o più in generale un residuo quadratico dello stesso n e che quello inferiore va preso quando k è un non-residuo. Questi teoremi restano eleganti o addirittura lo diventano ancor di più quando son estesi a valori composti di n.

---

*) In questo modo abbiamo dato una nuova dimostrazione del teorema che dice che -1 è un residuo quadratico di tutti i numeri primi della forma $4k+1$ ed un non-residuo di tutti quelli della forma $4k+3$. Sopra (negli articoli 108, 109, 262) lo abbiamo provato in più modi. Se è preferibile supporre questo teorema non ci sarà bisogno di distinguere i due diversi casi poiché β e γ saranno di per sé interi.

Ma di tali argomenti, che abbisognano di ricerche superiori, non parleremo qui e ci ripromettiamo di farlo in un altro momento.

357.

Sia

$$x^m - ax^{m-1} + bx^{m-2} - \text{etc.} = 0$$

l'equazione di grado m le cui radici sono le m radici contenute nel periodo $(m, 1)$, la indicheremo con $z = 0$. Qui $a = (m, 1)$ e ciascuno dei rimanenti coefficienti b etc. sono della forma $\mathsf{A} + \mathsf{B}(m, 1) + \mathsf{C}(m, 1)$, con A, B, C interi (articolo 348). Denotando con z' la funzione in cui z viene trasformata se sostituiamo $(m, 1)$ con (m, g) ed (m, g) con (m, g^2) o che è lo stesso, con $(m, 1)$, le radici dell'equazione $z' = 0$ saranno contenute in (m, g) ed il prodotto

$$zz' = \frac{x^n - 1}{x - 1} = X\ .$$

Quindi z può essere ridotta alla forma $R + S(m, 1) + T(m, g)$ dove R, S, T sono funzioni intere di x ed a coefficienti tutti interi. Fatto questo avremo

$$z' = R + S(m, g) + T(m, 1).$$

Se per brevità scriviamo p e q al posto di $(m, 1)$ e (m, g) rispettivamente

$$2z = 2R + (S + T)(p + q) - (T - S)(p - q) = 2R - S - T - (T - S)(p - q)$$

ed in maniera simile

$$2z' = 2R - S - T + (T - S)(p - q)$$

e se poniamo

$$2R-S-T=Y,\quad T-S=Z$$

avremo $4X=Y^2-(p-q)^2Z^2$ e poiché $(p-q)^2=\pm n$,

$$4X=Y^2\mp nZ^2.$$

Il segno superiore vale quando n è della forma $4k+1$, quello inferiore quando esso è della forma $4k+3$. Questo è il teorema che sopra (articolo 124) avevamo promesso di dimostrare. È facile vedere che i due termini di grado massimo nella funzione Y saranno sempre $2x^m+x^{m-1}$ ed x^{m-1} sarà il termine di grado massimo nella funzione Z. I coefficienti restanti, che saranno tutti interi, varieranno in accordo alla natura del numero n e non potranno essere espressi da una formula analitica generale.

Esempio. Per $n=17$, con le regole dell'art. 348 l'equazione, le cui radici sono le otto radici contenute in $(8,1)$, sarà

$$x^8-px^7+(4+p+2q)x^6-(4p+3q)x^5+(6+3p+5q)x^4$$
$$-(4p+3q)x^3+(4+p+2q)x^2-px+1=0$$

quindi

$$R=x^8+4x^6+6x^4+4x^2+1$$
$$S=-x^7+x^6-4x^5+3x^4-4x^3+x^2-x$$
$$T=2x^6-3x^5+5x^4-3x^3+2x^2$$

e

$$Y=2x^8+x^7+5x^6+7x^5+4x^4+7x^3+5x^2+x+2$$
$$Z=x^7+x^6+x^5+2x^4+x^3+x^2+x$$

Ecco altri esempi:

n	Y	Z
3	$2x+1$	1
5	$2x^2+x+2$	x
7	$2x^3+x^2-x-2$	x^2+x
11	$2x^5+x^4-2x^3+2x^2-x-2$	x^4+x
13	$2x^6+x^5+4x^4-x^3+4x^2+x+2$	x^5+x^3+x
19	$2x^9+x^8-4x^7+3x^6+5x^5-5x^4$ $-3x^3+4x^2-x-2$	$x^8-x^6+x^5+x^4-x^3+x$
23	$2x^{11}+x^{10}-5x^9-8x^8-7x^7-4x^6$ $+4x^5+7x^4+8x^3+5x^2-x-2$	$x^{10}+x^9-x^7-2x^6-2x^5$ $-x^4+x^2+x$

358.

Procediamo ora a considerazioni sull'equazione cubica, per la quale, nel caso in cui n è della forma $3k+1$, dobbiamo determinare le tre somme di $\frac{1}{3}(n-1)$ termini che compongono il complesso Ω. Sia g una radice primitiva per il modulo n, e $\frac{1}{3}(n-1)=m$, che sarà un intero pari. Allora le tre somme dei quali Ω è fatto, saranno $(m,1)$, (m,g), (m,g^2), al posto dei quali scriveremo rispettivamente p, p', p''. È chiaro che il primo contiene le radici $[1]$, $[g^3]$, $[g^6]$ … $[g^{n-4}]$, il secondo $[g]$, $[g^4]$ … $[g^{n-3}]$, il terzo ha le radici $[g^2]$, $[g^5]$ … $[g^{n-2}]$. Supponiamo che l'equazione cercata sia

$$x^3-Ax^2+Bx-C=0$$

Avremo

$$A=p+p'+p'',\quad B=pp'+p'p''+pp'',\quad C=pp'p''$$

ed $A=-1$. Siano A, B, C etc., i minimi residui positivi dei numeri g^3, g^6 … g^{n-4} relativamente al modulo n senza dare importanza all'ordine. Chiameremo R il loro complesso con aggiunto il numero 1. Allo stesso modo siano A', B', C' etc. i minimi residui dei numeri g, g^4, g^7 … g^{n-4} ed R' il loro complesso; infine siano A'', B'', C'' etc. i minimi residui dei numeri g^2, g^5, g^8 … g^{n-2} ed R'' il loro insieme. Così tutti i numeri di R, R', R'' saranno diversi e coincideranno con 1, 2, 3 … $n-1$. Prima di tutto dobbiamo osservare che il numero $n-1$ deve essere in R, poiché è facile convincersi che è un residuo di $g^{\frac{3m}{2}}$. Da ciò segue anche che i due numeri h ed $n-h$ saranno sempre nello *stesso* dei tre complessi R, R', R''; infatti se uno di essi è un residuo della potenza g^λ, l'altro sarà un residuo della potenza $g^{\lambda+\frac{3m}{2}}$ o $g^{\lambda-\frac{3m}{2}}$ se $\lambda > \frac{3m}{2}$. Denoteremo con (RR) il numero dei numeri della serie 1, 2, 3 … $n-1$ che appartengono ad R e che vi rimangono se aumentati dell'unità; (RR') sarà il numero dei numeri nella stessa serie, che sono contenuti in R ed i successivi dei quali cadono in R'. Segue immediatamente il significato dei simboli (RR''), $(\mathsf{R}'\mathsf{R})$, $(\mathsf{R}'\mathsf{R}')$, $(\mathsf{R}'\mathsf{R}'')$ $(\mathsf{R}''\mathsf{R})$, $(\mathsf{R}''\mathsf{R}')$, $(\mathsf{R}''\mathsf{R}'')$. Fatto questo, dico che *per prima cosa* $(\mathsf{RR}')=(\mathsf{R}'\mathsf{R})$. Supponiamo infatti che h, h', h'' etc. siano tutti i numeri della serie 1, 2, 3 … $n-1$ che sono in R e tali che i più vicini $h+1$, $h'+1$, $h''+1$ etc. cadono in R': il loro numero è (RR'). È chiaro che tutti i numeri $n-h-1$, $n-h'-1$, $n-h''-1$ etc. sono contenuti in R' ed i loro successivi $n-h$, $n-h'$, $n-h''$ etc. in R. Ora poiché ci sono in tutto $(\mathsf{R}'\mathsf{R})$ numeri di tal fatta, non possiamo di certo avere $(\mathsf{R}'\mathsf{R})<(\mathsf{RR}')$; allo stesso modo non può essere $(\mathsf{RR}')<(\mathsf{R}'\mathsf{R})$ e quindi questi due numeri sono uguali. Esattamente allo stesso modo si prova che $(\mathsf{RR}'')=(\mathsf{R}''\mathsf{R})$, $(\mathsf{R}'\mathsf{R}'')=(\mathsf{R}''\mathsf{R}')$ etc. In secondo luogo, poiché ogni numero di R, tranne il

più grande $n-1$, è seguito dal suo successivo in R, o in R' o in R'', la somma $(\mathsf{RR})+(\mathsf{RR}')+(\mathsf{RR}'')$ deve essere uguale al numero di tutti i numeri di R diminuito di un'unità, cioè $=m-1$. Per una simile ragione

$$(\mathsf{R}'\mathsf{R})+(\mathsf{R}'\mathsf{R}')+(\mathsf{R}'\mathsf{R}'')=(\mathsf{R}''\mathsf{R})+(\mathsf{R}''\mathsf{R}')+(\mathsf{R}''\mathsf{R}'')=m\,.$$

Con questi preliminari, con le regole dell'articolo 345 sviluppiamo il prodotto pp' in $(m,\mathsf{A}'+1)+(m,\mathsf{B}'+1)+(m,\mathsf{C}'+1)+\text{etc.}$, la quale espressione è facilmente riducibile alla forma $(\mathsf{R}'\mathsf{R})\,p+(\mathsf{R}'\mathsf{R}')\,p'+(\mathsf{R}'\mathsf{R}'')\,p''$. Grazie all'articolo 345.I possiamo calcolare a partire da questo, il prodotto $p'p''$ sostituendo $(m,1)$, (m,g), (m,g^2) rispettivamente con (m,g), (m,g^2), (m,g^3) e cioè p, p', p'' rispettivamente con p', p'', p. Così abbiamo $p'p''=(\mathsf{R}'\mathsf{R})\,p'+(\mathsf{R}'\mathsf{R}')\,p''+(\mathsf{R}'\mathsf{R}'')\,p$. Allo stesso modo si ha $p''p=(\mathsf{R}'\mathsf{R})\,p''+(\mathsf{R}'\mathsf{R}')\,p+(\mathsf{R}'\mathsf{R}'')\,p'$. Da ciò otteniamo *in primo luogo* che

$$B=m(p+p'+p'')=-m\,,$$

e, *in secondo luogo*, in maniera del tutto analoga a quando abbiamo calcolato pp', possiamo ridurre anche pp'' a $(\mathsf{R}''\mathsf{R})\,p+(\mathsf{R}''\mathsf{R}')\,p'+(\mathsf{R}''\mathsf{R}'')\,p''$. Poiché questa espressione è identica alle precedenti, avremo necessariamente $(\mathsf{R}''\mathsf{R})=(\mathsf{R}'\mathsf{R}')$ e $(\mathsf{R}''\mathsf{R}'')=(\mathsf{R}'\mathsf{R})$. Ora se poniamo

$$(\mathsf{R}'\mathsf{R}'')=(\mathsf{R}''\mathsf{R}')=a\,,\quad(\mathsf{R}''\mathsf{R}'')=(\mathsf{R}'\mathsf{R})=(\mathsf{R}\mathsf{R}')=b\,,$$

$$(\mathsf{R}'\mathsf{R}')=(\mathsf{R}''\mathsf{R})=(\mathsf{R}\mathsf{R}'')=c$$

avremo $m-1=(\mathsf{RR})+(\mathsf{RR}')+(\mathsf{RR}'')=(\mathsf{RR})+b+c$, ed essendo $a+b+c=m$, $(\mathsf{RR})=a-1$. Così le nove quantità incognite si riducono alle tre a, b, c, o meglio due, poiché $a+b+c=m$. Infine è chiaro che il quadrato p^2

diventa $(m, 1+1)+(m, \mathsf{A}+1)+(m, \mathsf{B}+1)+(m, \mathsf{C}+1)+\text{etc.}$ Tra i termini di questa espressione abbiamo (m, n), che si riduce ad $(m, 0)$, ovvero ad m, ed i termini rimanenti si riducono a $(\mathsf{RR})p+(\mathsf{RR}')p'+(\mathsf{RR}'')p''$, così abbiamo $p^2 = m+(a-1)p+bp'+cp''$.

Come risultato di tutte le ricerche precedenti abbiamo le seguenti quattro riduzioni:

$$\begin{aligned} p^2 &= m+(a-1)p+bp'+cp'' \\ pp' &= bp+cp'+ap'' \\ pp'' &= cp+ap'+bp'' \\ p'p'' &= ap+bp'+cp'' \end{aligned}$$

dove le tre incognite a, b, c soddisfano l'equazione condizionale

$$a+b+c=m \ldots\ldots\ldots\ldots\ldots\ldots (\mathrm{I})$$

ed inoltre sappiamo che questi numeri sono interi. Di qui abbiamo

$$\begin{aligned} C = p\cdot p'p'' &= ap^2+bpp'+cpp'' \\ &= am+(a^2+b^2+c^2-a)p+(ab+bc+ac)p'+(ab+bc+ac)p'' \end{aligned}$$

Ma essendo $pp'p''$ una funzione invariabile di p, p', p'', i coefficienti, per cui essi vengono moltiplicati nell'espressione precedente, sono necessariamente uguali (articolo 350), abbiamo allora la nuova equazione

$$a^2+b^2+c^2-a = ab+bc+ac \ldots (\mathrm{II})$$

e da questo otteniamo $C = am+(ab+bc+ac)(p+p'+p'')$ o (grazie ad I e per il fatto che $p+p'+p''=-1$)

$$C = a^2-bc \ldots\ldots\ldots\ldots\ldots\ldots (\mathrm{III})$$

Ora sebbene C dipenda da tre incognite, legate tra loro soltanto da due equazioni, tuttavia con l'aiuto della condizione che a, b, c sono interi, queste sono sufficienti a determinare completamente C. Per mostrare ciò esprimiamo l'equazione II come

$$\begin{aligned} 12a+12b+12c+4 = 36a^2+36b^2+36c^2-36ab-36ac-36bc \\ -24a+12b+12c+4 \end{aligned}$$

Grazie ad I, il membro sinistro diventa $=12m+4=4n$. La parte destra si riduce a

$$(6a-3b-3c-2)^2+27(b-c)^2$$

o, se scriviamo k al posto di $2a-b-c$, a $(3k-2)^2+27(b-c)^2$. Così il numero $4n$ (ovvero in generale il quadruplo di un qualsiasi primo della forma $3m+1$) può essere rappresentato dalla forma x^2+27y^2. Tutto ciò può essere dedotto senza difficoltà dalla teoria generale delle forme binarie, ma è importante che una tale decomposizione possa essere realizzata con i valori di a, b, c. Inoltre il numero $4n$ può essere decomposto in maniera unica come somma di un quadrato e di un quadrato moltipicato per 27. Lo mostriamo nel seguente modo.*) Se supponiamo che

$$4n = t^2+27u^2 = t'^2+27u'^2$$

abbiamo, *primo,* che

$$(tt'-27uu')^2+27(tu'+t'u)^2 = 16n^2;$$

secondo, che

$$(tt'+27uu')^2+27(tu'-t'u)^2 = 16n^2;$$

---

*) Questa proposizione può essere provata in maniera più diretta con i principi della Sezione V.

terzo, che

$$(tu'+t'u)(tu'-t'u)=4n(u'^2-u^2).$$

Dalla terza equazione segue che n, poiché è un numero primo, divide uno dei numeri $tu'+t'u$, $tu'-t'u$. Dalla prima e dalla seconda invece, è chiaro che entrambi questi numeri sono minori di n; per cui, quello diviso da n deve essere $=0$ necessariamente. Così anche $u'^2-u^2=0$, per cui $u'^2=u^2$ e $t'^2=t^2$, cioè le due decomposizioni sono uguali. Supponiamo ora che la decomposizione di $4n$ nella somma di un quadrato e di un quadrato moltiplicato per 27 sia data (questo può essere fatto o con il metodo diretto della Sezione V oppure per la via indiretta illustrata negli articoli 323, 324); avremo allora $4n=M^2+27N^2$, e i quadrati $(3k-2)^2$, $(b-c)^2$ potranno essere determinati e così avremo due equazioni al posto della (II).

Ma chiaramente non sarà determinato solo il quadrato $(3k-2)^2$, ma anche la sua radice $3k-2$. Poiché essa deve essere $=+M$ o $=-M$, l'ambiguità si rimuove facilmente. Infatti poiché k deve essere un intero, avremo che $3k-2=+M$ o $=-M$ a seconda che M sia della forma $3z+1$ oppure

$3z+2$.*) Ora poiché $k=2a-b-c=3a-m$, avremo $a=\frac{1}{3}(m+k)$, $b+c=m-a=\frac{1}{3}(2m-k)$ da cui

---

*) Chiaramente M non può essere della forma $3z$ poiché altrimenti $4n$ sarebbe divisibile per tre. Per quanto riguarda il dubbio se $b-c$ debba essere $=N$ o $=-N$, non è necessario considerare la questione qui, e per la natura della cosa, non può essere determinato in alcun modo, perché dipende dalla scelta della radice primitiva g. Per alcune radici primitive la differenza $b-c$ sarà positiva, per altre negativa.

$$C = a^2 - bc = a^2 - \frac{1}{4}(b+c)^2 + \frac{1}{4}(b-c)^2$$
$$= \frac{1}{9}(m+k)^2 - \frac{1}{36}(2m-k)^2 + \frac{1}{4}N^2 = \frac{1}{12}k^2 + \frac{1}{3}km + \frac{1}{4}N^2$$

e così abbiamo trovato che tutti i coefficienti dell'equazione. Q.E.F. Questa formula apparirà più semplice se sostituiamo N^2 con il suo valore nell'equazione $(3k-2)^2 + 27N^2 = 4n = 12m + 4$. Dopo il calcolo si trova

$$C = \frac{1}{9}(m + k + 3km) = \frac{1}{9}(m + kn).$$

Lo stesso valore può essere ridotto a $(3k-2)N^2 + k^3 - 2k^2 + k - km + m$. E sebbene questa espressione sia meno pratica, essa mostra immediatamente che di sicuro C deve essere un intero, poiché è pari.

Esempio. Per $n = 19$ abbiamo $4n = 49 + 27$, così $3k - 2 = +7$, $k = 3$, $C = \frac{1}{9}(6 + 57) = 7$ e l'equazione che vogliamo è $x^3 + x^2 - 6x - 7 = 0$, come abbiamo visto sopra (articolo 351). Allo stesso modo, per $n = 7, 13, 31, 37, 43, 61, 67$ i valori corrispondenti di k sono $1, -1, 2, -3, -2, 1, -1$ e $C = 1, -1, 8, -11, -8, 9, -5$.

Sebbene il problema che abbiamo risolto in questo articolo sia piuttosto complicato, volutamente non lo abbiamo omesso per l'eleganza della soluzione e perché ci ha dato occasione di usare vari artifici che potranno essere usati fruttuosamente in altre ricerche.*)

---

*) Corollario. Sia ε una radice dell'equazione $x^3 - 1 = 0$ e si avrà $\left(p + \varepsilon p' + \varepsilon^2\right)^3 = \frac{n}{2}\left(M + N\sqrt{-27}\right)$. Sia $\frac{M}{\sqrt{4n}} = \cos\varphi$, $\frac{N\sqrt{27}}{\sqrt{4n}} = \sin\varphi$ e sarà

$$p = -\frac{1}{3} + \frac{2}{3}\cos\frac{1}{3}\varphi\sqrt{n}; \quad M \equiv +1 \pmod 3; \quad 1 \equiv M\,(1\cdot 2\cdot 3 \ldots m)^3 \pmod n$$

Se poniamo $3x + 1 = y$, allora abbiamo $y^3 - 3ny - Mn = 0$.

359.

Le ricerche precedenti hanno a che fare con la *ricerca* delle equazioni ausiliarie: ora spiegheremo una proprietà molto importante concernente la loro *soluzione*. Tutti sappiamo che i più grandi geometri hanno cercato senza successo la risoluzione generale delle equazioni di grado maggiore del quarto, o (per definire la ricerca più accuratamente) la RIDUZIONE DI EQUAZIONI MISTE AD EQUAZIONI PURE, e rimane ancora il dubbio che questo problema sia non tanto superiore ai moderni metodi dell'analisi, quanto piuttosto, come dicono alcuni, impossibile (vedi quanto abbiamo detto circa questo argomento nella *Demonstratio nova*, articolo 9). È certo ciononostante che ci sono moltissime equazioni miste di ogni grado che ammettono una riduzione ad equazioni pure, e speriamo che i geometri ci saranno grati se mostriamo che le nostre equazioni sono sempre di questo tipo. Ma a causa della lunghezza della discussione, presenteremo qui solo i più importanti principi necessari a mostrare i nostri intenti e ci rimandiamo ad un altro momento una più completa trattazione di questo argomento. Presenteremo prima alcune osservazioni generali circa le radici dell'equazione $x^e - 1 = 0$, che comprende anche il caso in cui e è un numero composto.

I. Queste radici sono date (come è noto dai testi elementari) da $\cos\frac{kP}{e} + i\sin\frac{kP}{e}$ dove k è uno degli e numeri 0, 1, 2, 3 … $e-1$ od un qualsiasi altro numero congruo ad uno di questi secondo il modulo e. Una radice, per $k = 0$, o per un qualsiasi altro valore di k divisibile per e, sarà $= 1$; ad un qualsiasi altro valore di k corrisponde una radice diversa da 1.

II. Poiché $\left(\cos\frac{kP}{e} + i\sin\frac{kP}{e}\right)^{\lambda} = \cos\frac{\lambda kP}{e} + i\sin\frac{\lambda kP}{e}$, è chiaro che se R è una radice di questo tipo corrispondente ad un valore di k coprimo con e, allora nella successione R, R^2, R^3 etc. l'e-simo termine sarà $= 1$, ed i valori antecedenti saranno tutti diversi da 1. Segue immediatamente che tutti i valori

delle e quantità 1, R, R^2, R^3 … R^{e-1} sono diversi e, poiché tutti soddisfano all'equazione $x^e - 1 = 0$, essi ci forniranno tutte le radici dell'equazione.

III. Sotto le stesse supposizioni la somma

$$1 + R^{\lambda} + R^{2\lambda} \ldots + R^{\lambda(e-1)} = 0$$

per un qualsiasi valore intero di λ, non divisibile per e; infatti è $= \frac{1 - R^{\lambda e}}{1 - R^{\lambda}}$ ed il numeratore di questa frazione è $= 0$ ed il denominatore non è $= 0$. Quando λ è divisibile per e, la somma è ovviamente $= e$.

360.

Sia n, come sempre finora, un numero primo e g una radice primitiva per il modulo n, ed $n-1$ sia il prodotto di tre numeri interi positivi α, β, γ. Per brevità considereremo insieme i casi in cui α o $\gamma = 1$. Quando $\gamma = 1$, possiamo sostituire le somme $(\gamma, 1)$, (γ, g) etc. con le radici $[1]$, $[g]$ etc. Supponiamo dunque che da tutte le α somme di $\beta\gamma$ termini, $(\beta\gamma, 1)$, $(\beta\gamma, g)$, $(\beta\gamma, g^2)$ $\ldots(\beta\gamma, g^{\alpha-1})$, che sono note, vogliamo trovare le somme di γ termini. Abbiamo ricondotto tale compito ad equazioni miste di grado β, ora mostreremo però come risolverle per mezzo di equazioni pure dello stesso grado. Per brevità, al posto delle somme

$$(\gamma, 1), (\gamma, g^{\alpha}), (\gamma, g^{2\alpha}) \ldots (\gamma, g^{\alpha\beta-\alpha})$$

che sono contenute in $(\beta\gamma, 1)$, scriveremo a, b, $c \ldots m$ rispettivamente; al posto di

$$(\gamma, g), (\gamma, g^{\alpha+1}) \ldots (\gamma, g^{\alpha\beta-\alpha+1})$$

contenute in $(\beta\gamma,\ g)$, scriveremo a', b' . . . m'; al posto di

$$(\gamma,\ g^2),\ (\gamma,\ g^{\alpha+2}) \ldots (\gamma,\ g^{\alpha\beta-\alpha+2})$$

scriveremo a'', b'' . . . m'', etc. fino a quelle che sono contenute in $(\beta\gamma,\ g^{\alpha-1})$.

Sia R una radice indefinita dell'equazione $x^\beta - 1 = 0$, e supponiamo che lo sviluppo della β-esima potenza della funzione

$$t = a + Rb + R^2c \ldots + R^{\beta-1}m$$

sia, in accordo con le regole dell'articolo 345,

$$\begin{aligned} N &+ Aa + Bb + Cc \ldots + Mm \\ &+ A'a' + B'b' + C'c' \ldots + M'm' \\ &+ A''a'' + B''b'' + C''c'' \ldots + M''m'' \\ &+ \text{etc.} \qquad\qquad\qquad\qquad = T \end{aligned}$$

dove tutti i coefficienti N, A, B, A' etc. sono funzioni razionali intere di R. Supponiamo inoltre che le β-esime potenze delle altre due funzioni

$$u = R^\beta a + Rb + R^2c \ldots + R^{\beta-1}m, \quad u' = b + Rc + R^2d \ldots + R^{\beta-2}m + R^{\beta-1}a$$

diventino rispettivamente U ed U'. Grazie all'articolo 350 è facile convincersi, siccome u' risulta dalla permutazione delle somme a, b, c . . . m in b, c, d . . . a, che

$$\begin{aligned} U' = N &+ Aa + Bb + Cc \ldots + Mm \\ &+ A'a' + B'b' + C'c' \ldots + M'm' \\ &+ A''a'' + B''b'' + C''c'' \ldots + M''m'' \\ &+ \text{etc.} \end{aligned}$$

È chiaro inoltre che, essendo $u = Ru'$, avremo $U = R^\beta U'$; per cui essendo $R^\beta = 1$, i corrispondenti coefficienti in U ed U' saranno uguali. Infine, poiché

t ed u differiscono soltanto nel fatto che a in t viene moltiplicata per l'unità ed in u per R^{β}, tutti i coefficienti corrispondenti (cioè quelli che moltiplicano le stesse somme) in T ed U saranno uguali, e così anche i coefficienti corrispondenti di T ed U'. Quindi $A = B = C$ etc. $= M$; $A' = B' = C'$ etc.; $A'' = B'' = C''$ etc.; etc. così T si riduce ad una forma del tipo

$$N + A(\beta\gamma, 1) + A'(\beta\gamma, g) + A''(\beta\gamma, g^2) + \text{etc.}$$

dove i singoli coefficienti N, A, A' etc. sono riducibili alla forma

$$pR^{\beta-1} + p'R^{\beta-2} + p''R^{\beta-3} + \text{etc.}$$

in maniera tale che p, p', p'' etc. siano degli interi noti.

II. Se prendiamo al posto di R una radice determinata dell'equazione $x^{\beta} - 1 = 0$ (della quale supponiamo già di avere la soluzione) ed in maniera tale che nessuna potenza più piccola della β-esima sia uguale all'unità, anche T sarà una quantità nota, e da questa potremo determinare t per mezzo dell'equazione pura $t^{\beta} - T = 0$. Ma avendo tale equazione β radici, che sono t, Rt, R^2 … $R^{\beta-1}t$, ci può essere un dubbio su quale radice debba essere scelta. Ciò tuttavia è arbitrario, come apparirà facilmente. Bisogna ricordare che dopo che sono state determinate tutte le somme di $\beta\gamma$ termini, la radice $[1]$ è definita in maniera tale che una qualsiasi delle $\beta\gamma$ radici contenute in $(\beta\gamma, 1)$ possa essere denotata con quel segno. Così è del tutto arbitrario con quale delle β somme che costituiscono lo stesso $(\beta\gamma, 1)$, scegliamo di rappresentare a. Se poi esprimiamo una di tali somme con a e supponiamo che sia $t = \mathsf{T}$, è facile vedere che quella somma che prima indicavamo con b può essere trasformata in a, e ciò che prima erano c, d … a, b ora diventano b, c … m, a ed il valore di t è ora $= \dfrac{\mathsf{T}}{R} = \mathsf{T}R^{\beta-1}$. Allo stesso modo se vogliamo trasformare a in quella somma che prima rappresentava c, il valore di t diventa $\mathsf{T}R^{\beta-2}$, così t

può essere posto uguale ad una qualsiasi delle quantità T, $\mathsf{T}R^{\beta-1}$, $\mathsf{T}R^{\beta-2}$ etc. cioè ad una qualsiasi delle radici dell'equazione $x^{\beta}-1=0$ a seconda di quale somma di $(\beta\gamma, 1)$ rappresenta $(\gamma, 1)$. Q.E.D.

III. Dopo aver determinato la quantità t in questo modo, dobbiamo cercare le altre $\beta-1$ che si originano da t sostituendo nella sua espressione ad R, successivamente, R^2, R^3, R^4 … R^{β} e cioè

$$t'=a+R^2b+R^4c\ldots+R^{2\beta-2}m,\quad t''=a+R^3b+R^6c\ldots+R^{3\beta-3}m \quad \text{etc.}$$

Di queste abbiamo già l'ultima, che è banalmente $=a+b+c\ldots+m=(\beta\gamma, 1)$; le altre possono essere calcolate nel modo seguente. Usiamo i metodi dell'articolo 345 per trovare il prodotto $t^{\beta-2}t'$ proprio come abbiamo trovato t^{β} in I. Allora proveremo con un metodo del tutto analogo al precedente, che quel prodotto si riduce alla forma

$$\mathsf{N}+\mathsf{A}(\beta\gamma, 1)+\mathsf{A}'(\beta\gamma, g)+\mathsf{A}''(\beta\gamma, g^2)\ \text{etc.}=T'$$

in maniera tale che N, A, A' etc. siano funzioni razionali intere di R, e così T' è una quantità nota e $t'=\frac{T't^2}{T}$. Esattamente nello stesso modo possiamo trovare T'' calcolando il prodotto $t^{\beta-3}t''$. Questa espressione avrà una forma simile e poiché il suo valore è noto possiamo derivare t'' dall'equazione $t''=\frac{T''t^3}{T}$. Allora può essere trovato t''' dall'equazione $t'''=\frac{T'''t^4}{T}$ dove T''' è una quantità nota etc.

Questo metodo non sarebbe applicabile se fosse $t=0$ da cui discenderebbe $T=T'=T''$ etc. $=0$. Ma si può dimostrare che ciò è impossibile, nonostante la dimostrazione sia troppo lunga e noi qui la omettiamo. Ci sono degli altri speciali artifici per convertire le frazioni $\frac{T'}{T}$, $\frac{T''}{T}$ etc. in funzioni

razionali *intere* di R ed altri metodi più brevi nel caso in cui $\alpha = 1$, per trovare i valori di t', t'' etc., ma non li considereremo qui.

IV. Infine, dopo aver trovato t, t', t'' etc., per l'osservazione III dell'articolo precedente, abbiamo immediatamente che $t + t' + t'' + etc. = \beta a$, per cui il valore di a stesso sarà noto e da questo, per l'articolo 346, possono essere ricavati i valori di tutte le restanti somme di γ termini. Possono essere ricavati anche i valori di b, c, d etc. grazie alle equazioni seguenti, la cui validità può essere facilmente provata:

$$\begin{aligned}
\beta b &= R^{\beta-1}t + R^{\beta-2}t' + R^{\beta-3}t'' + \text{etc.} \\
\beta c &= R^{2\beta-2}t + R^{2\beta-4}t' + R^{2\beta-6}t'' + \text{etc.} \\
\beta d &= R^{3\beta-3}t + R^{3\beta-6}t' + R^{3\beta-9}t'' + \text{etc.} \quad \text{etc.}
\end{aligned}$$

Del gran numero di osservazioni che potremmo fare circa le proprietà precedenti, ci soffermeremo soltanto su di una. Riguardo alla soluzione dell'equazione pura $x^{\beta} - T = 0$, è chiaro che T ha in molti casi il valore immaginario $P + iQ$, così che la soluzione dipende in parte dalla divisione di un angolo (la cui tangente è $= \frac{Q}{P}$), in parte dalla divisione di un segmento (dell'unità su $\sqrt{P^2 + Q^2}$) in β parti. È altresì importante (non tratteremo qui questo argomento) che il valore di $\sqrt[\beta]{P^2 + Q^2}$ può essere sempre espresso *razionalmente* per mezzo di quantità note, in modo che, eccettuata l'estrazione di una radice quadrata, bisogna effettuare per la soluzione *soltanto* la divisione di un angolo, per esempio, se $\beta = 3$, solo la trisezione di un angolo, mentre per molte equazioni cubiche, le cui radici sono tutte reali, non è possibile evitare contemporaneamente la trisezione dell'angolo e quella del segmento.

Quindi, poiché nulla ci vieta di supporre $\alpha = 1$, $\gamma = 1$ e quindi $\beta = n - 1$, è chiaro che la soluzione dell'equazione $x^n - 1 = 0$ può essere immediatamente ricondotta alla soluzione dell'equazione pura $x^{n-1} - T = 0$ di grado $n - 1$, dove T è determinata grazie alle radici di $x^{n-1} - 1 = 0$. Dall'osservazione ora fatta

segue che la divisione dell'intera circonferenza in n parti richiede 1° la suddivisione dell'intero circolo in $n-1$ parti, 2° la divisione, di un altro arco, che può essere costruito una volta fatta la prima divisione in $n-1$ parti, 3° l'estrazione di una sola radice quadrata, e si può dimostrare che questa è sempre $\sqrt{n}$.

361.

Non ci resta che esaminare più da vicino il legame tra le radici di Ω e le funzioni trigonometriche degli angoli $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$ … $\frac{(n-1)P}{n}$. Il metodo che abbiamo usato per trovare le radici di Ω (a meno che non consultiamo le tavole dei seni come s'è detto sopra, il che sarebbe meno diretto) lascia un dubbio *su quale* radice corrisponda ad ogni *singolo* angolo, cioè quale radice sia $=\cos\frac{P}{n}+i\sin\frac{P}{n}$, quale $=\cos\frac{2P}{n}+i\sin\frac{2P}{n}$, etc. Questa incertezza si rimuove facilmente osservando che i coseni degli angoli $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$ … $\frac{(n-1)P}{2n}$ diminuiscono continuamente (facendo attenzione ai segni) e che i seni sono tutti positivi. D'altro canto gli angoli $\frac{(n-1)P}{n}$, $\frac{(n-2)P}{n}$, $\frac{(n-3)P}{n}$ … $\frac{(n+1)P}{2n}$ hanno gli stessi coseni degli angoli precedenti, ed i seni sono negativi, sebbene abbiano lo stesso valore assoluto. Quindi delle radici di Ω, le due che hanno le più grandi parti reali (che sono tra loro uguali), corrispondono agli angoli $\frac{P}{n}$ $\frac{(n-1)P}{n}$ e nella prima di esse la quantità immaginaria i è moltiplicata per una quantità positiva nella seconda, per una negativa. Delle rimanenti $n-3$ radici quelle che hanno parte reale più grande corrispondono agli angoli $\frac{2P}{n}$,

$\frac{(n-2)P}{n}$ e così via. Non appena è nota la radice che corrisponde all'angolo $\frac{P}{n}$, quelle che corrispondono agli angoli rimanenti possono essere determinate a partire da questa, poiché se supponiamo che essa sia $=[\lambda]$, le radici $[2\lambda]$, $[3\lambda]$, $[4\lambda]$ etc. corrispondono agli angoli $\frac{2P}{n}$, $\frac{3P}{n}$, $\frac{4P}{n}$ etc. Così nell'esempio nell'articolo 353 vediamo che la radice corrispondente all'angolo $\frac{1}{19}P$ non può essere nessuna radice che non sia $[11]$, e all'angolo $\frac{18}{19}P$ corrisponde la radice $[8]$. In maniera simile agli angoli $\frac{2}{19}P$, $\frac{17}{19}P$, $\frac{3}{19}P$, $\frac{16}{19}P$ etc. corrispondono le radici $[3]$, $[16]$, $[14]$, $[5]$ etc. Nell'esempio dell'articolo 354 all'angolo $\frac{1}{17}P$ chiaramente corrisponde la radice $[1]$, all'angolo $\frac{2}{17}P$ la radice $[2]$ etc. Così i seni ed i coseni degli angoli $\frac{P}{n}$, $\frac{2P}{n}$ etc. saranno completamente determinati.

362.

Riguardo alle funzioni trigonometriche rimanenti di questi angoli, ci sono quelle che possono essere derivate dai corrispondenti seni e coseni per mezzo di formule ben note. In questo modo le secanti e le tangenti possono essere trovate dividendo l'unità ed il seno per il coseno; le cosecanti e le cotangenti dividendo l'unità ed il seno per il coseno. Ma sarà più spesso utile ottenere le stesse quantità con l'aiuto delle seguenti formule con sole addizioni e nessuna divisione. Sia ω uno qualsiasi degli angoli $\frac{P}{n}$, $\frac{2P}{n}$ … $\frac{(n-1)P}{n}$ e sia $\cos\omega + i\sin\omega = R$ in modo tale che R sia una radice di Ω, allora

$$\cos\omega = \frac{1}{2}\left(R + \frac{1}{R}\right) = \frac{1+R^2}{2R}$$

$$\sin\omega = \frac{1}{2i}\left(R - \frac{1}{R}\right) = \frac{i\left(1-R^2\right)}{2R}$$

E da questa

$$\sec\omega = \frac{2R}{1+R^2},\ \text{tang}\,\omega = \frac{i\left(1-R^2\right)}{1+R^2},\ \text{cosec}\,\omega = \frac{2Ri}{R^2-1},\ \text{cotang}\,\omega = \frac{i\left(R^2+1\right)}{R^2-1}$$

Ora mostreremo come trasformare i numeratori di queste quattro funzioni in modo tale che siano divisibili per i denominatori.

I. Poiché $R = R^{n+1} = R^{2n+1}$ abbiamo che $2R = R + R^{2n+1}$. Questa espressione è divisibile per $1+R^2$, poiché n è un numero dispari. Così abbiamo che

$$\sec\omega = R - R^3 + R^5 - R^7 \ \ldots + R^{2n-1}$$

e quindi (poiché $\sin\omega = -\sin\left(2n-1\right)\omega$, $\sin 3\omega = -\sin\left(2n-3\right)\omega$ etc. abbiamo che $\sin\omega - \sin 3\omega + \sin 5\omega \ldots + \sin\left(2n-1\right)\omega = 0$)

$$\sec\omega = \cos\omega - \cos 3\omega + \cos 5\omega \ldots + \cos\left(2n-1\right)\omega$$

od infine (poiché $\cos\omega = \cos\left(2n-1\right)\omega$, $\cos 3\omega = \cos\left(2n-3\right)\omega$, etc.)

$$= 2\left(\cos\omega - \cos 3\omega + \cos 5\omega \ldots \mp \cos\left(n-2\right)\omega\right) \pm \cos n\omega,$$

dove si deve scegliere il segno superiore od inferiore a seconda che n sia della forma $4k+1$ o $4k+3$. Ovviamente questa formula può essere anche espressa come

$$\sec\omega = \pm\left[1 - 2\cos 2\omega + 2\cos 4\omega \ldots \pm 2\cos\left(n-1\right)\omega\right]$$

II. In maniera simile sostituendo $1-R^2$ con $1-R^{2n+2}$ abbiamo

$$\text{tang}\,\omega = i\left(1-R^2+R^4-R^6\ \ldots -R^{2n}\right)$$

oppure (poiché $1-R^{2n}=0$, $R^2-R^{2n-2}=2i\sin 2\omega$, $R^4-R^{2n-4}=2i\sin 4\omega$ etc.)

$$\text{tang}\,\omega = 2\left[\sin 2\omega-\sin 4\omega+\sin 6\omega\ \ldots \mp\sin\left(n-1\right)\omega\right]$$

III. Poiché $1+R^2+R^4\ \ldots +R^{2n-2}=0$, sarà

$$n = n-1-R^2-R^4\ \ldots R^{2n-2} = \left(1-1\right)+\left(1-R^2\right)+\left(1-R^4\right)\ldots+\left(1-R^{2n-2}\right)$$

i cui addendi sono divisibili per $1-R^2$. Di qui segue

$$\begin{aligned}\frac{n}{1-R^2} &= 1+\left(1+R^2\right)+\left(1+R^2+R^4\right)\ldots+\left(1+R^2+R^4\ \ldots+R^{2n-4}\right)\\ &= \left(n-1\right)+\left(n-2\right)R^2+\left(n-3\right)R^4\ \ldots+R^{2n-4}\end{aligned}$$

Moltiplicando per 2 e sottraendo la quantità

$$0 = \left(n-1\right)\left(1+R^2+R^4\ \ldots+R^{2n-2}\right)$$

e moltiplicando ancora per R, abbiamo

$$\frac{2nR}{1-R^2} = \left(n-1\right)R+\left(n-3\right)R^3+\left(n-5\right)R^5\ \ldots-\left(n-3\right)R^{2n-3}-\left(n-1\right)R^{2n-1}$$

e da questo otteniamo immediatamente che

$$\begin{aligned}\text{cosec}\,\omega &= \frac{1}{n}\left[\left(n-1\right)\sin\omega+\left(n-3\right)\sin 3\omega\ \ldots-\left(n-1\right)\sin\left(2n-1\right)\omega\right]\\ &= \frac{2}{n}\left[\left(n-1\right)\sin\omega+\left(n-3\right)\sin 3\omega+\text{etc.}+2\sin\left(n-2\right)\omega\right]\end{aligned}$$

che può anche essere riscritta come

$$\operatorname{cosec}\omega = -\frac{2}{n}\left[2\sin 2\omega + 4\sin 4\omega + 6\sin 6\omega \ldots + (n-1)\sin(n-1)\omega\right]$$

IV. Moltiplicando il valore dato prima di $\frac{n}{1-R^2}$ per $1+R^2$ e sottraendo

$$0 = (n-1)\left(1 + R^2 + R^4 \ldots + R^{2n-2}\right)$$

abbiamo

$$\frac{n\left(1+R^2\right)}{1-R^2} = (n-2)R^2 + (n-4)R^4 + (n-6)R^6 \ldots - (n-2)R^{2n-2}$$

e da questo segue immediatamente che

$$\begin{aligned}\operatorname{cotang}\omega &= \frac{1}{n}\left[(n-2)\sin 2\omega + (n-4)\sin 4\omega + (n-6)\sin 6\omega \ldots - (n-2)\sin(n-2)\omega\right] \\ &= \frac{2}{n}\left[(n-2)\sin 2\omega + (n-4)\sin 4\omega \ldots + 3\sin(n-3)\omega + \sin(n-1)\omega\right]\end{aligned}$$

e questa formula può essere anche espressa come

$$\operatorname{cotang}\omega = -\frac{2}{n}\left[\sin\omega + 3\sin 3\omega \ldots + (n-2)\sin(n-2)\omega\right].$$

363.

Quando $n-1 = ef$, la funzione X può essere risolta in e fattori di f dimensioni non appena troviamo il valore di tutte le e somme di f termini (articolo 348). Nello stesso modo, se supponiamo che $Z = 0$ sia un'equazione di ordine $n-1$ le cui radici sono i seni o qualsiasi altra funzione trigonometrica

degli angoli $\frac{P}{n}$, $\frac{2P}{n}$ … $\frac{(n-1)P}{n}$, la funzione Z può essere risolta in e fattori di f dimensioni effettuando i seguenti passi.

Supponiamo che Ω consista di e periodi di f termini, $(f,1)=P$, P', P'' etc.; il periodo P consista delle radici $[1]$, $[a]$, $[b]$, $[c]$ etc.; P' delle radici $[a']$, $[b']$, $[c']$ etc.; P'' delle radici $[a'']$, $[b'']$, $[c'']$ etc. etc. Sia ω l'angolo corrispondente alla radice $[1]$, e così gli angoli $a\omega$, $b\omega$ etc. corrispondono alle radici $[a]$, $[b]$ etc., gli angoli $a'\omega$, $b'\omega$ etc. corrispondono alle radici $[a']$, $[b']$ etc., gli angoli $a''\omega$, $b''\omega$ etc. corrispondono alle radici $[a'']$, $[b'']$ etc. È facile vedere che le funzioni trigonometriche *) di tutti questi angoli presi assieme coincidono con quelle degli angoli $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$ … $\frac{(n-1)P}{n}$. Ora se denotiamo le funzioni che stiamo considerando con la lettera φ, seguita dall'angolo, e se poniamo $=Y$ il prodotto degli e fattori

$$x-\varphi\omega,\quad x-\varphi a\omega,\quad x-\varphi b\omega \quad \text{etc.}$$

ed il prodotto dei fattori $x-\varphi a'\omega, x-\varphi b'\omega$ etc. $=Y'$, il prodotto di $x-\varphi a''\omega$, $x-\varphi b''\omega$ etc. $=Y''$ etc.: allora il prodotto $YY'Y''\ldots=Z$. Resta adesso da provare che tutti i coefficienti nelle funzioni Y, Y', Y'' etc. possono essere ridotti alla forma

$$A+B(f,1)+C(f,g)+D(f,g^2)\ldots+L(f,g^{e-1}).$$

Dopo aver fatto ciò, chiaramente tutti questi saranno noti non appena conosciamo i valori di tutte le somme di f termini. Proveremo ciò nel modo seguente.

---

*) Due angoli coincidono a questo riguardo se la loro differenza è uguale alla circonferenza ad un suo multiplo. Possiamo dire che sono *congruenti modulo la circonferenza* se vogliamo usare il termine congruenza in senso esteso.

Come $\cos\omega = \frac{1}{2}[1] + \frac{1}{2}[1]^{n-1}$, $\sin\omega = -\frac{1}{2}i[1] + \frac{1}{2}i[1]^{n-1}$, così per il precedente articolo, tutte le restanti funzioni trigonometriche dell'angolo ω possono essere ridotte alla forma $\mathsf{A} + \mathsf{B}[1] + \mathsf{C}[1]^2 + \mathsf{D}[1]^3 + \text{etc.}$ e, come è facile provare, le funzioni dell'angolo $k\omega$ diventano allora $\mathsf{A} + \mathsf{B}[k] + \mathsf{C}[k]^2 + \mathsf{D}[k]^3 + \text{etc.}$, dove k è un intero. Ora poiché i singoli coefficienti di Y sono funzioni razionali intere invariabili di $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$ etc. se sostituiamo queste quantità con i loro valori quantità i singoli coefficienti diventeranno funzioni razionali intere invariabili di $[1]$, $[a]$, $[b]$, etc. che per l'articolo 347 possono essere ridotte alla forma $A + B(f, 1) + C(f, g) + \text{etc.}$ Analogamente i coefficienti di Y', Y'' etc. possono essere ridotti a forme simili. Q.E.D.

364.

Aggiungiamo alcune informazioni riguardo i problemi dei precedenti articoli.

I. I singoli coefficienti di Y' sono le stesse funzioni delle radici contenute nel periodo P' (possiamo porlo $=(f, a')$) che le funzioni che esprimono i corrispondenti coefficienti in Y a partire dalle radici contenute in P. È chiaro dall'articolo 347 che possiamo ricavare Y' da Y, sostituendo ovunque in Y le quantità $(f, 1)$, (f, g), (f, g^2) etc. rispettivamente con (f, a'), $(f, a'g)$, $(f, a'g^2)$ etc. Quindi Y'' si può ricavare da Y, sostituendo ovunque in Y le quantità $(f, 1)$, (f, g), (f, g^2) etc. rispettivamente con (f, a''), $(f, a''g)$, $(f, a''g^2)$ etc. etc. Quindi appena abbiamo la funzione Y, le restanti Y', Y'' etc. seguono facilmente.

II. Supponiamo che

$$Y = x^f - \alpha x^{f-1} + \beta x^{f-2} - \text{etc.},$$

dove i coefficienti α, β etc. sono rispettivamente la somma delle radici dell'equazione $Y = 0$, cioè delle quantità $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$ etc., la somma dei loro prodotti prese a due a due, etc. Ma questi coefficienti saranno trovati più facilmente con un metodo simile a quello dell'articolo 349, e cioè calcolando la somma delle radici $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$ etc., la somma dei loro quadrati, cubi, etc. e ricavando da questi, per mezzo del teorema di Newton, i coefficienti cercati. Se poi φ rappresenta la tangente, la secante, la cotangente o la cosecante abbiamo altri metodi per abbreviare il procedimento, ma non li considereremo.

III. Il caso in cui f è un numero pari merita un'attenzione particolare perché ciascuno dei periodi P, P', P'' sarà composto di $\frac{f}{2}$ periodi di due termini. Supponiamo che P sia composto dai numeri $(2, 1)$, $(2, \mathfrak{a})$, $(2, \mathfrak{b})$, $(2, \mathfrak{c})$ etc. I numeri 1, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ etc. ed $n-1$, $n-\mathfrak{a}$, $n-\mathfrak{b}$, $n-\mathfrak{c}$ etc. presi assieme coincideranno con i numeri 1, a, b, c etc. o (che è la stessa cosa) almeno saranno congruenti a questi modulo n. Ma $\varphi(n-1)\omega = \pm\varphi\omega$, $\varphi(n-\mathfrak{a})\omega = \pm\varphi\mathfrak{a}\omega$ etc., dove il segno superiore deve essere preso quando φ rappresenta il coseno o la secante, quello inferiore quando φ rappresenta il seno, la tangente, la cotangente o la cosecante. Segue da ciò che nei due precedenti casi i fattori di cui Y è composto, saranno uguali a due a due, e così Y è un quadrato, ad esempio $Y = y^2$ se supponiamo che y sia il prodotto di

$$x - \varphi\omega, \quad x - \varphi\mathfrak{a}\omega, \quad x - \varphi\mathfrak{b}\omega \quad \text{etc.}$$

Nello stesso caso le funzioni restanti Y', Y'' etc. saranno quadrati e se supponiamo che P' sia composto da $(2, \mathfrak{a}')$, $(2, \mathfrak{b}')$, $(2, \mathfrak{c}')$ etc.; P'' da $(2, \mathfrak{a}'')$, $(2, \mathfrak{b}'')$, $(2, \mathfrak{c}'')$ etc. etc., il prodotto di $x - \varphi\mathfrak{a}'\omega$, $x - \varphi\mathfrak{b}'\omega$, $x - \varphi\mathfrak{c}'\omega$ etc. $= y'$, il prodotto di $x - \varphi\mathfrak{a}''\omega$, $x - \varphi\mathfrak{b}''\omega = y''$, etc., allora $Y' = y'^2$, $Y'' = y''^2$

etc. La funzione Z sarà ancora un quadrato (vedi sopra, articolo 337) e la sua radice sarà uguale al prodotto di y, y', y'' etc. Ma chiaramente y', y'' etc. possono essere derivate da y, proprio come abbiamo detto prima che Y', Y'' etc. possono essere dedotte da Y (vedi I). Inoltre i singoli coefficienti in y possono essere ridotti alla forma

$$A+B(f,1)+C(f,g)+\text{etc.}$$

poiché le somme delle singole potenze delle radici dell'equazione $y=0$ sono uguali a metà delle somme delle potenze delle radici dell'equazione $Y=0$ e quindi sono riducibili ad una forma di quel tipo. Nei seguenti quattro casi Y sarà invece il prodotto dei fattori

$$x^2-(\varphi\omega)^2,\quad x^2-(\varphi a\omega)^2,\quad x^2-(\varphi b\omega)^2,\quad \text{etc.}$$

e quindi sarà della forma

$$x^f-\lambda x^{f-2}+\mu x^{f-4}-\text{etc.}$$

È chiaro che i coefficienti λ, μ etc. possono essere dedotti dalle somme dei quadrati, delle quarte potenze, etc. delle radici $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$ etc. La stessa cosa è vera per Y', Y'' etc.

Esempio I. Sia $n=17$, $f=8$ e φ rappresenti il coseno. Allora avremo

$$Z=\left(x^8+\frac{1}{2}x^7-\frac{7}{4}x^6-\frac{3}{4}x^5+\frac{15}{16}x^4+\frac{5}{16}x^3-\frac{5}{32}x^2-\frac{1}{32}x+\frac{1}{256}\right)^2$$

e quindi $\sqrt{Z}$ sarà spezzata nel prodotto di due fattori di grado quattro, y ed y'. Il periodo $P=(8,1)$ consiste in $(2,1)$, $(2,9)$, $(2,13)$, $(2,15)$, così y sarà il prodotto dei fattori

$$x-\varphi\omega,\quad x-\varphi 9\omega,\quad x-\varphi 13\omega,\quad x-\varphi 15\omega.$$

Sostituendo $\varphi k\omega$ con $\frac{1}{2}[k]+\frac{1}{2}[n-k]$, si trova

$$\varphi\omega+\varphi 9\omega+\varphi 13\omega+\varphi 15\omega=\frac{1}{2}(8,1),$$

$$(\varphi\omega)^2+(\varphi 9\omega)^2+(\varphi 13\omega)^2+(\varphi 15\omega)^2=2+\frac{1}{4}(8,1)$$

inoltre la somma dei cubi è $=\frac{3}{8}(8,1)+\frac{1}{8}(8,3)$, la somma delle quarte potenze vale $\frac{1}{2}+\frac{5}{16}(8,1)$. Grazie al teorema di Newton, una volta determinati i coefficienti di y, si ottiene

$$y=x^4-\frac{1}{2}(8,1)x^3+\frac{1}{4}\big[(8,1)+2(8,3)\big]x^2-\frac{1}{8}\big[(8,1)+3(8,3)\big]x+\frac{1}{16}\big[(8,1)+(8,3)\big],$$

ed y' si ottiene da y scambiando $(8,1)$ con $(8,3)$. Sostituendo dunque ad $(8,1)$ ed $(8,3)$ i valori $-\frac{1}{2}+\frac{1}{2}\sqrt{17}$, $-\frac{1}{2}-\frac{1}{2}\sqrt{17}$, si ha

$$y=x^4+\left(\frac{1}{4}-\frac{1}{4}\sqrt{17}\right)x^3-\left(\frac{3}{8}+\frac{1}{8}\sqrt{17}\right)x^2+\left(\frac{1}{4}+\frac{1}{8}\sqrt{17}\right)x-\frac{1}{16}$$

$$y'=x^4+\left(\frac{1}{4}+\frac{1}{4}\sqrt{17}\right)x^3-\left(\frac{3}{8}-\frac{1}{8}\sqrt{17}\right)x^2+\left(\frac{1}{4}-\frac{1}{8}\sqrt{17}\right)x-\frac{1}{16}$$

Allo stesso modo $\sqrt{Z}$ può essere spezzata in quattro fattori di due dimensioni, dei quali il primo è $(x-\varphi\omega)(x-\varphi 13\omega)$, il secondo $(x-\varphi 9\omega)(x-\varphi 15\omega)$, il terzo $(x-\varphi 3\omega)(x-\varphi 5\omega)$, il quarto $(x-\varphi 10\omega)(x-\varphi 11\omega)$ e tutti i coefficienti di questi fattori si possono esprimere per mezzo delle quattro somme $(4,1)$, $(4,9)$, $(4,3)$, $(4,10)$. Chiaramente il prodotto del primo fattore per il secondo è y, il prodotto del terzo per il quarto è y'.

Esempio II. Lasciando tutto il resto immutato, se supponiamo che φ rappresenti il seno, in modo tale che

$$Z=\left(x^{16}-\frac{17}{4}x^{14}+\frac{119}{16}x^{12}-\frac{221}{32}x^{10}+\frac{935}{256}x^{8}-\frac{561}{512}x^{6}+\frac{357}{2084}x^{4}-\frac{51}{4096}x^{2}+\frac{17}{65536}\right)^{2}$$

deve essere risolta in due fattori di 8 dimensioni, y ed y', allora y sarà il prodotto di quattro fattori doppi

$$x^2-(\varphi\omega)^2,\quad x^2-(\varphi 9\omega)^2,\quad x^2-(\varphi 13\omega)^2,\quad x^2-(\varphi 15\omega)^2$$

Ora, poiché

$$\varphi k\omega=-\frac{1}{2}i[k]+\frac{1}{2}i[n-k]$$

abbiamo

$$(\varphi k\omega)^2=-\frac{1}{4}[2k]+\frac{1}{2}[n]-\frac{1}{4}[2n-2k]=\frac{1}{2}-\frac{1}{4}[2k]-\frac{1}{4}[2n-2k]$$

In questo modo la somma dei quadrati delle radici $\varphi\omega$, $\varphi 9\omega$, $\varphi 13\omega$, $\varphi 15\omega$ sarà $2-\frac{1}{4}(8,1)$, la somma delle loro quarte potenze $=\frac{3}{2}-\frac{3}{16}(8,1)$, la somma delle seste potenze $=\frac{5}{4}-\frac{9}{64}(8,1)-\frac{1}{64}(8,3)$, la somma delle ottave potenze $\frac{35}{32}-\frac{25}{256}(8,1)-\frac{1}{32}(8,3)$. Da ciò segue

$$\begin{aligned}y=x^8&-\left[2-\frac{1}{4}(8,1)\right]x^6+\left[\frac{3}{2}-\frac{5}{16}(8,1)+\frac{1}{8}(8,3)\right]x^4\\&-\left[\frac{1}{2}-\frac{9}{64}(8,1)+\frac{5}{64}(8,3)\right]x^2+\frac{1}{16}-\frac{2}{256}(8,1)+\frac{3}{256}(8,3)\end{aligned}$$

ed y' si ottiene da y scambiando $(8, 1)$, $(8, 3)$, così che, sostituendo i valori di queste somme, si ha

$$y = x^8 - \left(\frac{17}{8} - \frac{1}{8}\sqrt{17}\right)x^6 + \left(\frac{51}{32} - \frac{7}{32}\sqrt{17}\right)x^4 - \left(\frac{17}{32} - \frac{7}{64}\sqrt{17}\right)x^2 + \frac{17}{256} - \frac{1}{64}\sqrt{17}$$

$$y' = x^8 - \left(\frac{17}{8} + \frac{1}{8}\sqrt{17}\right)x^6 + \left(\frac{51}{32} + \frac{7}{32}\sqrt{17}\right)x^4 - \left(\frac{17}{32} + \frac{7}{64}\sqrt{17}\right)x^2 + \frac{17}{256} + \frac{1}{64}\sqrt{17}$$

Successivamente Z può essere risolta in quattro fattori, i coefficienti dei quali possono essere espressi mediante gli aggregati di quattro termini, ed il prodotto di due di essi sarà y, il prodotto dei due rimanenti sarà y'.

365.

In tal modo, grazie alle precedenti ricerche, abbiamo ricondotto il problema della divisione del circolo in n parti, se n è un numero primo, alla soluzione di tante equazioni quanti sono i fattori del numero $n-1$ ed i loro gradi dipendono dalla grandezza di tali fattori. Ogniqualvolta $n-1$ è una potenza del numero 2, cosa che accade quando il valore di n è uguale a 3, 5, 17, 257, 65537 etc. la suddivisione della circonferenza si riduce alla soluzione di sole equazioni quadratiche e le funzioni trigonometriche degli angoli $\frac{P}{n}$, $\frac{2P}{n}$ etc. potranno essere calcolate per mezzo di radici quadrate più o meno complicate (a seconda della grandezza del numero n). Dunque in questi casi la divisione del cerchio in n parti o l'inscrizione di un poligono regolare di n lati può essere effettuata per mezzo di costruzioni geometriche. Così, per esempio, per $n = 17$ dagli articoli 354, 361 abbiamo la seguente espressione per il coseno dell'angolo $\frac{P}{17}$:

$$-\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}\ .$$

I coseni dei multipli di questi angoli avranno una forma simile, ma i seni avranno più radicali. Fa meraviglia sapere che, sebbene la divisibilità geometrica del cerchio in tre e cinque parti fosse già nota ai tempi di Euclide, non è stato aggiunto nulla a queste scoperte per 2000 anni. E tutti i geometri hanno detto che, eccetto quelle divisioni che si possono ottenere direttamente da queste, (cioè la divisione in 15, $3\cdot 2^{\mu}$, $5\cdot 2^{\mu}$, e 2^{μ} parti), non ce ne sono altre che possono essere effettuate per mezzo di costruzioni geometriche. Invece è facile provare che se il numero primo n è $=2^{m}+1$, l'esponente m non può avere altri fattori primi diversi da 2, e quindi è $=1$ o $=2$ od è uguale ad una qualsiasi altra potenza di 2. Se infatti m fosse divisibile per un numero dispari ζ (maggiore dell'unità) e $m=\zeta\eta$, $2^{m}+1$ sarebbe divisibile per $2^{\eta}+1$ e quindi necessariamente un numero composto. Tutti i valori di n, quindi, che ci conducono ad equazioni quadratiche, sono di tipo $2^{2^{\nu}}+1$; Si ottengono così i cinque numeri 3, 5, 17, 257, 65537 ponendo $\nu=0$, 1, 2, 3, 4 ovvero $m=1$, 2, 4, 8, 16. In verità la sezione del cerchio non è possibile per *tutti* i numeri di quella forma, ma soltanto per quelli primi. Fermat, ingannato dalla sua induzione, affermava che tutti i numeri in quella forma fossero necessariamente primi, ma l'illustre Euler ha trovato che tale regola è errata per $\nu=5$, ovvero per $m=32$: si accorse per primo che $2^{32}+1=4294967297$ contiene il fattore 641.

Tutte le volte che il numero $n-1$ contiene fattori primi diversi da 2, siamo condotti sempre ad equazioni di grado superiore e precisamente ad una o più equazioni cubiche quando 3 appare una o più volte tra i fattori di $n-1$; ad equazioni di quinto grado quando $n-1$ è divisibile per 5 etc. E POSSIAMO PROVARE CON TUTTO IL RIGORE CHE QUESTE EQUAZIONI DI GRADO PIÙ ALTO NON POSSONO IN NESSUN MODO ESSERE EVITATE NÉ ESSERE RIDOTTE AD EQUAZIONI DI GRADO PIÙ

BASSO. I limiti del presente lavoro escludono questa dimostrazione, ma ciò che abbiamo fatto deve persuadere a non tentare le costruzioni geometriche delle sezioni diverse da quelle che la nostra teoria ha suggerito, cioè la suddivisione in 7, 11, 13, 19 etc. parti, per non perdere tempo inutilmente.

366.

Se si deve dividere il cerchio in a^α parti dove a è un numero primo, ovviamente questo può essere fatto geometricamente quando $a = 2$, ma non per tutti i valori di a se $\alpha > 1$, perché oltre alle equazioni richieste per la divisione in a parti, devono essere necessariamente risolte altre $\alpha - 1$ equazioni di grado a; queste non possono essere in nessun modo evitate od abbassate di grado. In generale il grado delle equazioni necessarie per questo scopo può essere ricavato dai fattori primi del numero $(a-1)a^{\alpha-1}$ (includendo anche il caso in cui $\alpha = 1$).

Infine se il cerchio deve essere suddiviso in $N = a^\alpha b^\beta c^\gamma \ldots$ parti, dove a, b, c etc. sono primi distinti, è sufficiente effettuare la suddivisione in a^α, b^β, c^γ etc. parti (articolo 336). Così per conoscere il grado delle equazioni necessarie per lo scopo, dobbiamo considerare i fattori primi dei numeri

$$(a-1)a^{\alpha-1}, \quad (b-1)b^{\beta-1}, \quad (c-1)c^{\gamma-1}, \quad \text{etc.}$$

o che è lo stesso, i fattori del loro prodotto. Sottolineiamo il fatto che questo prodotto indica il numero dei numeri coprimi con N e minori di esso (articolo 38). Geometricamente questa divisione può essere effettuata solo quando questo numero è una potenza di 2, ma quando i fattori includono fattori diversi da 2, ad esempio p, p' etc. allora le equazioni di grado p, p' etc. non possono essere evitate. In generale dunque per poter dividere geometricamente il cerchio in N parti, N deve essere 2 od una potenza più alta di 2, *od* un numero primo

della forma 2^m+1, *od* il prodotto di più numeri primi di questo tipo, *oppure ancora* il prodotto di uno o più numeri di questo tipo per 2 od una potenza più alta di 2. In breve è richiesto che N non ammetta fattori primi dispari che non siano della forma 2^m+1 né fattori primi della forma 2^m+1 ripetuti più d'una volta. I valori di N ammessi fino a 300 sono i seguenti 38:

2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.

Osservazioni.

Ci proponiamo ora di fare alcune osservazioni sul testo appena letto. A questo proposito avvisiamo che si ritiene che il modo migliore di procedere sia commentare singolarmente gli articoli della sezione VII. In particolare riscriveremo questi articoli in un linguaggio più accessibile che tenga conto dei recenti sviluppi dell'algebra moderna e che, quindi, ne faciliti la comprensione.

► **335.** Questo primo articolo ha carattere puramente introduttivo. Qui Gauss presenta, in maniera molto generale, il contenuto della sezione VII, dicendo che tratterà della teoria delle funzioni trigonometriche ed in particolare della teoria dei poligoni regolari, che fin dai tempi di Euclide, non aveva compiuto sostanziali passi in avanti. Il Maestro avvisa inoltre che avrà modo di chiarire le perplessità del lettore che vede trattati argomenti di carattere geometrico in un lavoro di Aritmetica superiore.

A causa degli elevati costi tipografici, Gauss dice che non gli è stato possibile presentare ulteriori applicazioni dell'argomento. Si riferisce in particolare alle funzioni trascendenti che dipendono dall'integrale $\int \frac{dx}{\sqrt{1-x^4}}$, che oggi chiamiamo integrale *lemniscatico*. Servendoci delle note appuntate nel suo diario personale, il *Tagebuch,* contenuto in *Werke,* Gauss, vol. VIII, veniamo a sapere che grazie all'aiuto di questi studi ed alle sue ricerche sulla *media aritmetico-geometrica*, è riuscito a calcolare la lunghezza della lemniscata di Bernoulli. Questa è una curva algebrica del piano di equazione cartesiana $\left(x^2+y^2\right)^2 = x^2 - y^2$, definita come il luogo geometrico dei punti del piano per cui è costante il prodotto delle distanze da due punti fissi detti fuochi. Jacob Bernoulli, il suo scopritore, aveva dimostrato che l'integrale $\int \frac{dx}{\sqrt{1-x^4}}$ ne calcola la lunghezza, ma aveva constatato con amarezza che non è possibile

esprimerlo mediante funzioni elementari note, ovvero aveva provato che è una grandezza trascendente. L'importanza del risultato raggiunto da Gauss sta nel fatto di aver trovato, mediante passaggi puramente algebrici (e *razionali*), una formula per il calcolo del suddetto integrale. Si trova infatti che tale lunghezza è uguale a $\frac{2\pi|OO'|}{M\left(1,\sqrt{2}\right)}$, dove $|OO'|$ rappresenta la distanza tra i due fuochi O ed O' della curva e $M\left(1,\sqrt{2}\right)$ è la media aritmetico-geometrica dei numeri 1 e $\sqrt{2}$.

► **336.** Negli articoli seguenti Gauss illustra i punti salienti della sua idea. Anzitutto fa osservare che è sufficiente saper dividere il circolo in un numero di parti che è una potenza di un numero primo. In maniera più semplice possiamo giustificare questo come segue. Supponiamo di voler costruire il poligono regolare di n lati, o, che è lo stesso, l'angolo $\alpha=\frac{2\pi}{n}$. Per semplicità, supponiamo che $n=n_1\cdot n_2$, con $MCD\left(n_1,n_2\right)=1$, e che il problema sia risolubile per $n=n_1$ e per $n=n_2$. Posto $\alpha_1=\frac{2\pi}{n_1}$ e $\alpha_2=\frac{2\pi}{n_2}$, per il lemma di Bézout esistono due interi r_1 ed r_2 tali che $r_1n_1+r_2n_2=1$. Di qui, moltiplicando per $\frac{2\pi}{n}$, si ottiene che $r_1\alpha_2+r_2\alpha_1=r_1\frac{2\pi}{n_2}+r_2\frac{2\pi}{n_1}=\frac{2\pi}{n_1n_2}$, ovvero che il problema è anche risolubile per n. Di qui segue che possiamo considerare solo il caso in cui n è una potenza di un primo.

► **339.** In linguaggio moderno possiamo riassumere quanto detto in questo articolo come segue. Sia n un numero primo e sia Ω l'insieme di tutte le radici dell'equazione $x^{n-1}+x^{n-2}+\text{etc.}+x+1=0\quad(\text{I})$. Ci proponiamo di provare che l'insieme $\Omega\cup\{1\}$, che oggi indichiamo con $\mathbb{U}_n$, è un gruppo ciclico di ordine n, i cui elementi non banali sono tutti generatori.

Per provare ciò, poniamo $\Omega \cup \{1\} = A$. Sia r un elemento di Ω, cioè una radice dell'equazione (I). È ovvio che $r^n = 1$. Inoltre, per le proprietà delle potenze, si ha che ogni potenza di r ad esponente intero ed il prodotto di due radici di Ω sono ancora delle soluzioni di (I). A è quindi un gruppo moltiplicativo.

In maniera molto elegante, possiamo rivedere il metodo usato da Gauss per provare che questo insieme ha esattamente n elementi, servendoci di un omomorfismo tra gli insiemi $\mathbb{Z}_n$ ed A:

$$\gamma : [k]_n \in \mathbb{Z}_n \mapsto r^k \in A$$

Non ci sono dubbi che γ è un omomorfismo dal gruppo additivo $\mathbb{Z}_n$ all'insieme A. Inoltre Gauss, lavorando con le proprietà delle congruenze, prova che γ è ben definito ed ingettivo. Da questo segue che $n = |\mathbb{Z}_n| \leq |A|$. Inoltre, per un teorema ben noto all'epoca, un'equazione di grado n non può avere più di n radici distinte, per cui è anche $n \geq |A|$. Di conseguenza γ è un isomorfismo e l'insieme A ha esattamente n elementi. Per ottenere questi, basta prendere un elemento non banale r di Ω e calcolare tutte le sue potenze con esponenti che variano in un sistema completo di rappresentanti per la relazione di congruenza modulo n.

Dalle parole dell'Autore si evince altresì che tutti gli elementi di Ω hanno periodo n. Più semplicemente giustifichiamo ciò sottolineando che n è un numero primo, e quindi gli ordini degli elementi di Ω coincidono con n stesso, per il teorema di Lagrange. Per cui, fissata una qualsiasi radice r diversa da 1, si ha che $\Omega = \{1, r, r^2 \ldots r^{n-1}\}$ ovvero $\Omega \cup \{1\} = \langle r \rangle$ ovvero il più familiare $\mathbb{Z}_n$.

► **340.** Chiariamo soltanto il concetto di *funzione algebrica razionale intera* nelle indeterminate t, u, v etc. Queste funzioni altro non sono che polinomi

(*funzioni algebriche intere*) a coefficienti razionali nelle indeterminate t, u, v etc. L'aggettivo *intero* è usato per indicare che le funzioni non contengono indeterminate ai denominatori. Esse quindi sono gli elementi di $\mathbb{Q}[t, u, v \ldots]$. Questo ci fa capire che nel XVIII secolo, la teoria dei polinomi e quella degli anelli non erano ancora state formalizzate, e ciò portava gli studiosi ad utilizzare un linguaggio per noi molto complicato e spesso di difficile comprensione.

► **341.** Dal punto di vista storico, questo articolo rappresenta una pagina molto importante per lo sviluppo dell'algebra moderna. Si intravede qui infatti il celebre teorema di irriducibilità in $\mathbb{Q}[x]$ dei polinomi ciclotomici, che il Maestro dimostra solo nel caso di un ordine primo. Non riprenderemo la lunga dimostrazione, che ha un carattere prettamente aritmetico, ma invitiamo il Lettore a leggere la dimostrazione del caso generale (si può ad esempio far riferimento a *Field and Galois theory* di P. Morandi). Quest'ultima infatti è molto distante da quella data nell'articolo 341, perché usa degli strumenti algebrici molto moderni, sconosciuti ai tempi di Gauss, senza però, a nostro avviso, elevarne di molto la difficoltà. Si pensi, infatti, che gli strumenti più complicati che vengono utilizzati, sono l'omomorfismo di valutazione ed il piccolo teorema di Fermat.

Nella dimostrazione Gauss richiama più volte l'articolo 42. Data la sua importanza lo abbiamo richiamato nell'introduzione. Questo altro non è che il *Lemma di Gauss*, uno dei più potenti strumenti di cui si servono oggi gli algebristi per decidere dell'irriducibilità dei polinomi a coefficienti interi o razionali.

► **342.** Dopo aver presentato il da farsi, per comodità di scrittura Gauss introduce il simbolo $[\lambda]$ che indicherà la quantità r^{λ}, una volta che è stata fissata una radice r di Ω. Per lavorare con questo oggetto più

disinvoltamente, sottolineiamo che le proprietà di cui gode sono simili a quelle dei logaritmi.

► **343.** In questo articolo il Maestro anticipa alcune delle idee fondamentali della moderna teoria dei gruppi.

Come abbiamo detto nell'introduzione, Gauss prova nella sezione III che $U(\square_n)$ ammette un generatore, una *radice primitiva*. Qui ne scegliamo una e la chiamiamo g. Poiché $U(\square_n)=\langle g\rangle$, gli $n-1$ numeri 1, g, g^2, … g^{n-2} saranno congruenti ai numeri 1, 2, 3, … $n-1$ modulo n (senza dare importanza all'ordine). Quindi

$$U(\square_n)=\{1,\ g,\ g^2\ \ldots\ g^{n-2}\}\quad\text{e}\quad \square_n=\{1,[g],[g^2]\ldots[g^{n-2}]\},$$

non appena si fissa una radice $r\in\Omega$. Scegliendo un'altra radice primitiva G in $U(\square_n)$, chiaramente il discorso non cambia, poiché si ottengono gli stessi insiemi indicati sopra, con gli elementi al più in ordine diverso.

Più in generale se $n-1=ef$, $g^e=h$ e $G^e=H$, gli f numeri 1, h, h^2 … h^{f-1} saranno congruenti ad 1, H, H^2 … H^{f-1} modulo n (non ordinatamente). Questo perché, come ci insegna la moderna teoria dei gruppi, il teorema di Lagrange può essere invertito nei gruppi ciclici. Infatti se g è un generatore di un gruppo ciclico di ordine $n-1$, ed f è un divisore di $n-1$, il sottogruppo $\left\langle g^{\frac{n-1}{f}}\right\rangle=\langle g^e\rangle=\langle h\rangle$ è ciclico di ordine f. Lo stesso vale per il gruppo ciclico $\langle H\rangle$, anch'esso di ordine f. Per un teorema ben noto (vedi ad esempio *Elementi di algebra*, Franciosi-de Giovanni, Teorema 4.10.12), dato un gruppo ciclico A di ordine finito m ed un divisore positivo d di m, esiste un unico sottogruppo di A, (necessariamente ciclico) di ordine d (che può essere costruito come abbiamo illustrato). Di qui segue che $\langle h\rangle=\langle H\rangle$. Passando alle corrispondenti radici di Ω che hanno gli elementi di questi sottogruppi come

esponenti, è chiaro che le f radici $[1], [h], \left[h^2\right] \ldots \left[h^{f-1}\right]$ saranno uguali alle radici $[1], [H], \left[H^2\right] \ldots \left[H^{f-1}\right]$.

Se poi prendiamo λ coprimo con n, il Maestro aggiunge che coincidono le più generali serie

$$[\lambda], [\lambda h], \left[\lambda h^2\right] \ldots \left[\lambda h^{f-1}\right] \quad \text{e} \quad [\lambda], [\lambda H], \left[\lambda H^2\right] \ldots \left[\lambda H^{f-1}\right].$$

Questo segue banalmente dall'uguaglianza $\langle h \rangle = \langle H \rangle$; di conseguenza è del tutto arbitrario se si sceglie di lavorare rispetto ad h od H, cioè rispetto alla radice primitiva g oppure G.

Spendiamo ancora alcune parole su questo fatto. Ricordiamo anzitutto che $U(\mathbb{Z}_m)$ è costituito da tutti gli elementi $[a]_m$ tali che $MCD(a, m) = 1$. Quindi $U(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \{[0]_n\}$ se n è un numero primo. Inoltre, sempre nelle ipotesi che n sia primo, $\mathbb{Z}_n$ è un dominio integro. Consideriamo l'applicazione:

$$\ell_\lambda : [a]_n \in U(\mathbb{Z}_n) \to [\lambda a]_n \in U(\mathbb{Z}_n).$$

Essa è ben definita perché moltiplicando tra loro due elementi primi con n, si ottiene un elemento dello stesso tipo, per cui nelle nostre ipotesi $[\lambda a]_n \in U(\mathbb{Z}_n)$, grazie alla compatibilità della congruenza modulo n con il prodotto tra interi. Inoltre ℓ_λ è iniettiva; scegliendo infatti due classi $[a]_n$ e $[b]_n$, se supponiamo che $[\lambda a]_n = [\lambda b]_n$ questo vuol dire che $\lambda a \equiv \lambda b \pmod{n}$, che, essendo per ipotesi λ coprimo con n, si riduce a $a \equiv b \pmod{n}$. Come volevamo, sarà $[a]_n = [b]_n$. Più sotto sfrutteremo questa iniettività per ottenere uno dei più importanti risultati della teoria dei gruppi.

L'indipendenza dei periodi su definiti dalla radice primitiva scelta, è fondamentale nella definizione seguente, che è la chiave di tutta la teoria

innovativa dell'Autore. Diciamo subito però che Gauss non è molto chiaro nel definire l'oggetto (f, λ). Per noi, d'ora in poi,

$$(f, \lambda) = [\lambda] + [\lambda h] + \text{etc.} + \left[\lambda h^{f-1}\right],$$

cioè una somma di numeri complessi, mentre il *periodo* (f, λ) è il seguente sottoinsieme di $\mathbb{C}_n$:

$$\left\{ [\lambda], [\lambda h], \left[\lambda h^2\right] \ldots \left[\lambda h^{f-1}\right] \right\}.$$

La nota posta a piè di pagina crea una piccola confusione tra la somma (*il valore numerico del periodo*) ed il periodo stesso, che non presuppone alcun tipo di operazione tra le radici. Ciò non deve fare meraviglia, né creare dubbi circa la chiarezza del linguaggio del Maestro: negli articoli seguenti sarà chiarito perché si può lavorare disinvoltamente sulle radici dei periodi con o senza le somme. È pleonastico, a questo punto, provare che entrambe le definizioni date sopra sono ben poste. Ci interessa invece soffermarci sugli esempi che vengono fatti e, soprattutto, sul motivo per cui è stato scelto il nome, tanto emblematico, di periodo.

Per $n = 19$, si trova che $U(\mathbb{C}_{19}) = \langle [2]_{19} \rangle$. Per determinare il periodo $(6, 1)$ procediamo così. Abbiamo che $n - 1 = 18 = 6 \cdot 3$. Quindi le radici cercate sono $[1]$, $\left[1 \cdot 2^3\right] = [8]$, $\left[1 \cdot 8^2\right] = [64]$, $\left[1 \cdot 8^3\right] = [512]$, $\left[1 \cdot 8^4\right] = [4096]$, $\left[1 \cdot 8^5\right] = [32768]$. Per quanto detto sopra è sufficiente considerare esponenti che variano tra 1 e 18, così riducendo modulo 19 si ottiene: $[1]$, $[7]$, $[8]$, $[11]$, $[12]$, $[18]$. Per semplificare la notazione lavoreremo con questi numeri, che in realtà indicano quantità complesse, privandoli delle parentesi e trattandoli come elementi di $\mathbb{C}_{19}$ (la qual cosa è lecita formalmente per l'isomorfismo trovato nell'articolo ►339). Avremo

$$(6, 1) = \{1, 7, 8, 11, 12, 18\},$$

che a ben vedere coincide con $\langle 8\rangle < U(\mathbb{Z}_{19})$, *l'unico* sottogruppo di $U(\mathbb{Z}_{19})$ di ordine 6. Allo stesso modo i periodi

$$(6, 2) = (6, 3) = \{2, 3, 5, 14, 16, 17\} \text{ e } (6, 4) = \{4, 6, 9, 10, 13, 15\}$$

sono altri *sottoinsiemi* di $U(\mathbb{Z}_{19})$.

Alla luce di questo esempio, è facile convincersi che, scelti un divisore f di $n-1$ e g, generatore di $U(\mathbb{Z}_n)$, il periodo $(f, 1)$ rappresenta il gruppo ciclico $\left\langle g^{\frac{n-1}{f}} \right\rangle = \langle h\rangle$, che indicheremo con K: esso è l'unico sottogruppo di $U(\mathbb{Z}_n)$ di ordine f. Quanto segue chiarirà il significato degli altri periodi.

► **344.** Negli articoli successivi di questa sezione sono contenute delle importantissime osservazioni che ci permetteranno di presentare ulteriori risultati della teoria dei gruppi ciclici finiti.

L'osservazione II dice che, fissate come sopra, una radice primitiva g ed una radice r dell'equazione (I), Ω sarà composto dai periodi $(f, 1)$, (f, g), (f, g^2) … (f, g^{e-1}), ovvero richiamando l'isomorfismo γ e le osservazioni precedenti:

$$U(\mathbb{Z}_n) = (f, 1) \cup (f, g) \cup (f, g^2) \ldots \cup (f, g^{e-1}).$$

Per l'osservazione I tale riunione è disgiunta, infatti non appena un elemento di (f, λ) cade in (f, λ'), i due periodi coincidono del tutto.

Quindi, ritornando all'esempio fatto per $n = 19$, $U(\mathbb{Z}_{19})$ è l'unione disgiunta dei tre periodi $(6, 1)$, $(6, 2)$, $(6, 4)$ di 6 elementi ciascuno. Sia come sopra K l'insieme $(6, 1)$, che coincide col sottogruppo ciclico $\langle 8\rangle$. Diciamo

che questi tre insiemi rappresentano le classi laterali di $U(\square_{19})$ rispetto alla congruenza modulo K.

Questo è vero in generale come assicura l'osservazione I. Infatti se λ e λ' sono due elementi dello stesso periodo di f termini, $\lambda'\lambda^{-1}$ è congruo ad una qualche potenza di $h = g^e$, sarà dunque un elemento di K. Questa altro non è che la definizione di congruenza modulo un sottogruppo. Inoltre la partizione di $U(\square_n)$ in insiemi di f elementi, così ottenuta, è unica, poiché tale è il sottogruppo K di ordine f.

Vogliamo aggiungere infine, per sottolinearne l'importanza, che così facendo Gauss effettua una dimostrazione a posteriori del teorema di Lagrange per i gruppi finiti. Infatti, come lui stesso indica, il numero delle classi laterali (quelle che lui chiama *periodi*), è esattamente e; poiché $n-1 = e \cdot f$, l'ordine di K, che è f, è un divisore di $n-1$, cioè l'ordine del gruppo in cui stiamo lavorando.

Spendiamo ancora alcune parole sulle classi laterali $(f, 1)$, (f, g), (f, g^2) … (f, g^{e-1}) e sull'applicazione ℓ_λ. La ciclicità dell'insieme K non era sfuggita nemmeno a Gauss: il Maestro aveva infatti notato, che questa particolare proprietà di $(f, 1)$ si trasmette anche agli altri periodi, che *ciclicamente* assumono gli stessi valori al crescere delle potenze di h. Abbiamo trovato sopra che ℓ_λ è iniettiva, e la prova che abbiamo dato ricalca la moderna dimostrazione del teorema di Lagrange. Questo teorema serve, tra le altre cose, per provare che tutte le classi laterali modulo il sottogruppo K sono equipotenti. Allora tutti gli insiemi di tipo (f, λ) hanno lo stesso numero di elementi, che è pari ad f. Inoltre, per l'iniettività di ℓ_λ, per determinare completamente quei periodi, basta prendere in considerazione le prime f potenze di h, a partire da quella con esponente 0.

Nell'osservazione III Gauss procede ad un'ulteriore partizione in classi laterali degli insiemi $U(\mathbb{Z}_n)$ e K. Si parte col supporre che $n-1=a\cdot b\cdot c$, con a, b, c fattori interi. Si asserisce che ogni periodo di bc termini è composto da b periodi di c termini, che, nel nostro linguaggio, significa suddividere una classe laterale modulo K di bc termini, in b classi laterali di c elementi. Nel testo è anche illustrato come procedere. Si ha infatti che

$$(bc,\lambda)=(c,\lambda)\cup(c,\lambda g^{a})\cup(c,\lambda g^{2a})\ldots\cup(c,\lambda g^{ab-a})$$

Ritornando all'esempio per $n=19$, risulta che K è unione di tre classi di 2 elementi. Posto $a=3$, $b=3$, $c=2$ e fissata la radice primitiva 2 in $U(\mathbb{Z}_{19})$, si ha

$$h=2^{\frac{n-1}{c}}=2^{\frac{18}{2}}=2^{9}\equiv 18\ (\mathrm{mod.}\ 19).$$

Da qui segue $(2,1)=\{1,18\}=\{1,-1\}=\langle -1\rangle$, che è l'unico sottogruppo ciclico di $U(\mathbb{Z}_{19})$ di ordine 2; lo indicheremo con L. Le altre due classi laterali $(2,2^{a})=(2,8)$ e $(2,2^{2a})=(2,2^{6})=(2,7)$, si ottengono più semplicemente a partire da $(2,1)$ moltiplicando i suoi elementi rispettivamente per 8 e per 7, e riducendo modulo 19. Si ottiene così che

$$(6,1)=L\cup(2,7)\cup(2,8)=L\cup 7L\cup 8L\,.$$

Preferiamo per ora lasciare in forma implicita gli insiemi $7L$ e $8L$ ripromettendoci di calcolare i loro elementi, in maniera più elegante, alla luce delle seguenti osservazioni.

In fin dei conti, non abbiamo fatto altro che determinare le 9 classi laterali in $U(\mathbb{Z}_{19})$ modulo il sottogruppo L, e selezionare quelle che ricoprono K. Analogamente si possono ripartire i periodi $(6,2)$ e $(6,4)$ in classi di due

elementi, ma non ci addentriamo in laboriosi calcoli, rinviando la questione ad un secondo momento.

È facile convincersi che tutto questo discorso può essere generalizzato non appena si fissa un divisore c di f (che a sua volta divide $n-1$). Come noto esiste un unico sottogruppo di $U(\mathbb{Z}_n)$ di ordine c, e questo è, come indica Gauss stesso, il periodo $(c, 1)$; indichiamolo con L. Ovviamente dalla definizione data sopra segue che $(c, 1) = \left\langle g^{\frac{n-1}{c}} \right\rangle$ ed è chiaro inoltre che $L < K$.

Infatti $u = g^{\frac{n-1}{c}}$, generatore di L, è un elemento del gruppo K, che è generato da $v = g^{\frac{n-1}{f}}$. Sia infatti $f = c \cdot c'$. Allora chiaramente $c' < f$ e $v^{c'} = g^{\frac{n-1}{f} \cdot c'} = g^{\frac{n-1}{c}} = u$. Otteniamo così una nuova verifica del teorema di Lagrange, poiché $L < K$, $|L| = c$, $|K| = f$ e per ipotesi $c \mid f$.

Veniamo ora all'artificio che, in maniera elegante, ci permette di determinare le partizioni di $(6, 1)$, $(6, 2)$, $(6, 4)$ in classi di 2 elementi, senza svolgere calcoli. Se si pone $c = 2$, ovviamente $(2, 1) = L = \langle -1 \rangle$. Gli elementi di questo gruppo sono 1 e $-1 = 18 \pmod{19}$, due quantità la cui somma è $0 \equiv 19 \pmod{19}$. Il laterale $7L$ può essere ottenuto moltiplicando gli elementi di L per 7, e quindi $7L = \{7, -7\} = \{7, 12\}$.

Lo stesso per $8L = \{8, -8\} = \{8, 11\}$, per cui

$$(6, 1) = \{1, 18\} \cup \{7, 12\} \cup \{8, 11\}.$$

Allo stesso modo vanno ripartiti gli elementi di $(6, 2)$ e $(6, 4)$ accoppiando gli opposti:

$$(6, 2) = \{2, 17\} \cup \{3, 16\} \cup \{5, 14\} \quad \text{e} \quad (6, 4) = \{4, 15\} \cup \{6, 13\} \cup \{9, 10\}.$$

Osserviamo che nel caso generale, 2 è sempre un fattore di $n-1$, poiché si sceglie di lavorare con n primo *dispari*; sarà quindi sempre possibile una partizione come quella indicata nell' esempio. Data l'evidenza della cosa non riteniamo necessario formalizzare il procedimento.

► **345., 346.** Gli articoli che seguono illustrano alcune proprietà dei periodi e ci insegnano ad operare con essi. In particolare, l'articolo 345 dice che il prodotto di periodi *simili*, oggi diremmo equipotenti, è un periodo simile; l'articolo 346 invece, stabilisce che fissato un periodo (f, λ), tutti i periodi simili sono espressioni polinomiali di questo a coefficienti razionali. Come corollario, deduciamo che la valutazione di un polinomio di $\mathbb{Q}[t, u, v \ldots]$ in periodi di tipo (f, λ), si può ridurre alla forma

$$A + B(f, 1) + B'(f, g) + B''(f, g^2) + \ldots + B^{\varepsilon}(f, g^{e-1})$$

visto che i periodi $(f, 1)$, (f, g), (f, g^2) … (f, g^{e-1}) costituiscono un sistema completo di rappresentanti per la congruenza modulo il sottogruppo K. Nel coefficiente A è stato conglobato il periodo $(f, 0) = (f, kn)$, che vale f, come è facile calcolare.

► **347.** Da questo articolo si evince perché la definizione di periodo data Gauss non è strettamente univoca. Anzitutto una *funzione algebrica razionale intera invariabile* è, in linguaggio moderno, un polinomio simmetrico di $\mathbb{Q}[t, u, v \ldots]$.Ora preso un polinomio di questo tipo, si dimostra che, valutandolo nelle radici di un periodo (f, λ), si ottiene una forma di tipo $A + A'[1] + A''[2] + \text{etc.} = W$, in cui le radici che appartengono allo stesso periodo hanno lo stesso coefficiente. Di conseguenza, in una combinazione lineare di questo tipo se compare una radice di un periodo, compaiono automaticamente tutte le altre che, *sommate,* moltiplicano il medesimo

coefficiente. Di qui segue l'arbitrarietà nell'utilizzare o meno il simbolo di somma tra le radici di un periodo giacché, nelle espressioni con cui lavoreremo le loro radici compaiono comunque legate dalla somma.

► **349.** In questo articolo vengono richiamate brevemente le celebri formule di Viète che servono per trovare i coefficienti di un polinomio come funzioni polinomiali simmetriche delle sue radici. Al Maestro interessa in particolare costruire dei polinomi in $\mathbb{Q}[x]$ le cui radici siano quelle contenute nei periodi su definiti.

► **350.** In questo articolo si riprendono i risultati dell'articolo 347, e si applicano al caso di un periodo di tipo (bc, λ). Un'applicazione di questo fatto sta nella costruzione della successione di equazioni, di cui parlavamo nell'introduzione, che ci servirà per determinare completamente l'insieme $\mathbb{Q}_n$.

► **351.** Seguono applicazioni delle proprietà che abbiamo dimostrato. Nel primo esempio, per $n=19$, troviamo l'equazione le cui radici sono le somme $(6,1)$, $(6,2)$, $(6,4)$, che indichiamo rispettivamente con p, p', p''. Con il metodo di Viète o con quello di Newton si ottiene $x^3+x^2-6x-7=0$.

Nel secondo esempio poi, si cerca l'equazione le cui radici sono le somme $(2,1)$, $(2,7)$, $(2,8)$, contenute in p. Questa è

$$x^3-px^2+(p+p'')x-2-p'=0 \qquad (1).$$

Tralasciamo i dettagli, perché riteniamo più che chiare le parole del Maestro; sottolineiamo piuttosto, l'osservazione conclusiva che stabilisce come ottenere le equazioni le cui radici sono le somme $(2,2)$, $(2,3)$, $(2,5)$, contenute in p', e le somme $(2,4)$, $(2,6)$, $(2,9)$, contenute in p''. Il Maestro osserva che, per ottenere queste ultime, basta sostituire nella (1) p, p', p'' rispettivamente

con p', p'', p e con p'', p, p'. Bisogna dunque effettuare una permutazione delle radici. Ed è proprio su questa permutazione che torneremo più tardi.

► **352.** Viene qui presentato il metodo che Gauss usa per determinare le radici che formano l'insieme Ω_n, un metodo che è alternativo a quello delle formule di Cotes-De Moivre.

► **353., 354.** Seguono alcune applicazioni del metodo di Gauss per la determinazione di Ω_n nei casi $n=19$ ed $n=17$. In realtà potrebbe fare meraviglia che, in un trattato di Aritmetica Superiore come le *Disquisitiones*, vengano effettuate delle valutazioni numeriche. Questo urta un po' con la nostra concezione, tutta moderna, dell'Algebra, che consideriamo pura e lontana da ogni tipo di approssimazione o calcolo. Si ha così modo di capire come lavoravano i grandi del passato: essi non facevano differenza tra la teoria pura e le sue applicazioni, scegliendo di effettuare ricerche solo nell'uno o solo nell'altro campo, bensì studiavano delle teorie innovative che, pur essendo astratte, avevano comunque un'utilità pratica. Del resto, la storia ci insegna che anche le più geniali ed eleganti idee sono ben presto destinate a perire se non trovano un'utile applicazione nei problemi contemporanei. Avremo successivamente occasione di capire quanto ai contemporanei furono utili le osservazioni del Maestro per gli studi di trigonometria.

► **355. … 358.** Questi articoli trattano alcuni casi particolari e suggeriscono come lavorare quando 2 e 3 rispettivamente, compaiono tra i fattori di $n-1$. Come corollari Gauss ottiene degli importantissimi risultati della teoria algebrica dei numeri, che potrebbero essere dimostrati usando la teoria delle forme quadratiche, ma che qui egli dimostra sfruttando la teoria dei periodi. Viene dimostrato nuovamente che -1 è un residuo quadratico dei numeri primi della forma $4k+1$ ed un non-residuo di tutti quelli della forma $4k+3$. Il

secondo risultato stabilisce invece che se n è un numero primo della forma $3k+1$, allora esistono due interi a e b tali che $4n = a^2 + 27b^2$.

► **359.** Questo articolo, come altri all'interno dell'opera, ha un'elevata importanza storica. Infatti, nelle Disquisitiones, si fa spesso riferimento ad alcuni dei problemi matematici di fine Settecento. Qui vengono affrontati in particolare i problemi relativi alla teoria dei polinomi. Negli articoli precedenti Gauss dimostra che è possibile calcolare le radici di Φ_n, con n numero primo, servendosi di una successione di equazioni i cui gradi sono essenzialmente i fattori primi di $n-1$. Il maestro ha inoltre determinato un metodo semplice per calcolarle. Un problema ben più complesso è quello della loro risolubilità algebrica. Fino a quando i primi compresi tra i fattori di $n-1$ sono 2 e 3, basta applicare le ben note formule risolutive. Ma potrebbero comparire fattori primi ben più grandi. Ad esempio se $n=71$, allora $n-1=2\cdot5\cdot7$ e ci troviamo di fronte alla necessità di risolvere un'equazione di grado 5 ed una di grado 7 ma, come ben sappiamo per il teorema di Ruffini-Abel-Galois, non esiste una formula risolutiva per l'equazione di grado maggiore od uguale a 5. Osserviamo che Gauss era a conoscenza di questo enunciato; infatti dice: "*Tutti sappiamo che i più grandi geometri hanno cercato senza successo la risoluzione generale delle equazioni di grado maggiore del quarto, o (per definire la ricerca più accuratamente) la RIDUZIONE DI EQUAZIONI MISTE AD EQUAZIONI PURE, e rimane ancora il dubbio che questo problema sia non tanto superiore ai moderni metodi dell'analisi, quanto piuttosto, come dicono alcuni, impossibile".* Ciononostante Gauss dimostra che le equazioni che noi otteniamo col suo metodo sono sempre risolubili algebricamente, ovvero riducibili ad equazioni di grado inferiore. Quando riuscì a costruire con riga e compasso il poligono regolare di 17 lati, appena diciottenne, risolse altresì un equazione di grado diciassettesimo.

Circa questo fatto viene raccontato un aneddoto in *Storia del pensiero matematico* di Morris Kline: ci sembra importante raccontarlo. Un giorno Gauss si avvicinò a Kästner, il suo professore all'Università di Göttingen, con

la dimostrazione della costruibilità del 17-gono regolare. Kästner era incredulo e cercò di sbarazzarsi di Gauss a torto, proprio come farebbero oggi i professori universitari con i trisettori dell'angolo. Piuttosto che perdere tempo ad esaminare la dimostrazione per trovarvi il supposto errore, Kastner gli disse che la costruzione era scarsamente importante poiché esistevano delle costruzioni pratiche. Egli sapeva bene, però, che l'esistenza di metodi approssimati di costruzione era del tutto irrilevante. Gauss osservò allora che aveva risolto un'equazione di grado diciassettesimo. Kästner replicò che la soluzione era impossibile, ma Gauss aggiunse che aveva ricondotto il problema ad una equazione di grado inferiore. "Oh bella," lo schernì Kästner, "questo l'ho già fatto io!". Ci consola sapere che persino l'illustre Gauss ha avuto problemi ad affermarsi durante i suoi studi universitari, (le Disquisitiones lo portarono subitò dopo all'immortalità) ma sentiamo il dovere di far sapere che non abbiamo mai incontrato insegnanti di un'ottusità tanto scandalosa e paragonabile a quella di Kästner, anzi abbiamo sempre avuto a che fare con professionisti incredibilmente preparati e sempre disponibili.

► **361.** In questo articolo si torna a trattare argomenti di trigonometria. Come abbiamo anticipato al punto ►353, ai tempi del Maestro, non esistendo calcolatori elettronici, le computazioni venivano fatte con al più l'ausilio di tavole logaritmiche e trigonometriche. Il metodo illustrato in questo articolo permette di determinare con buona precisione le funzioni trigonometriche degli archi ottenuti mediante la ciclotomia.

► **364.** Sempre riferendosi alle equazioni che permettono di determinare le funzioni trigonometriche degli archi ciclotomici, si parla di permutazioni tra radici come quelle usate al punto ►351. Mentre Lagrange effettuava le sue permutazioni sulle espressioni algebriche delle radici permutando direttamente le radici, nel senso moderno Gauss moltiplica semplicemente un'espressione di questo tipo con una delle radici o con una somma di esse. Questo prodotto produce una permutazione poiché, lo ribadiamo, l'insieme Ω_n è un gruppo

ciclico di ordine primo e perché le espressioni che utilizziamo sono combinazioni *lineari* delle radici.

► **365., 366.** Nella parte finale, che contiene a nostro avviso il risultato storicmente più importante di tutta l'opera, il discorso letteralmente precipita. Gauss, dopo aver presentato brevemente il problema millenario della ciclotomia, propone la sua brillante soluzione mostrando come questo problema geometrico sia connesso all'Aritmetica. Grazie alle ricerche precedenti abbiamo provato che dividere il cerchio in n parti uguali equivale a risolvere un certo numero di equazioni i cui gradi sono i divisori primi, anche ripetuti, del numero $n-1$.

Le costruzioni geometriche con riga e compasso nel piano, corrispondono, dal punto di vista algebrico, alla risoluzione di equazioni di grado 1 oppure 2. Infatti l'equazione di una retta nel piano è di tipo

$$ax+by+c=0, \qquad (a,\,b)\neq(0,\,0),$$

basata quindi su di un polinomio lineare, mentre quella di una circonferenza è di secondo grado ed è di tipo:

$$x^2+y^2+2Ax+2By+C=0 \qquad A^2+B^2-C>0\,.$$

L'intersezione di rette porta alla soluzione di un sistema lineare, che grazie ai teoremi dell'algebra lineare sappiamo risolvere completamente; l'intersezione di una retta e di una circonferenza ci conduce ad una sistema di secondo grado con un'equazione risolvente, di secondo grado anch'essa, che si può risolvere con le formule ben note. L'intersezione di due circoli conduce apparentemente ad un sistema di quarto grado, ma come è facile provare, l'equazione risolvente anche in questo caso è al più di secondo grado (la cosa è ancora più evidente se si affronta il problema da un punto di vista geometrico). Per cui gli unici poligoni regolari con un numero primo n di lati, che possiamo costruire, sono quelli per cui $n-1$ è una potenza di 2, giacché altri fattori primi diversi da 2

richiederebbero operazioni non effettuabili con riga e compasso. I numeri primi di questo tipo sono i cosiddetti *primi di Fermat* e finora se ne conoscono solo cinque, e precisamente: 3, 5, 17, 257, 65537. Se si vuole costruire il poligono regolare di a^{α} lati, con a primo, la costruzione è banale se $a=2$ (si devono effettuare delle bisecazioni successive), è invece impossibile se $a\neq 2$ ed $\alpha>1$ poiché dovremmo risolvere, come abbiamo provato negli articoli precedenti,un'equazione di grado $a-1$, ed $\alpha-1$ equazioni di grado a che non possono essere né ridotte né abbassate di grado. La funzione totiente di Euler calcolata in a^{α} indica i gradi delle equazioni necessarie allo scopo; infatti si ha

$$\phi\left(a^{\alpha}\right)=(a-1)a^{\alpha-1}.$$

Generalizzando, per poter costruire il poligono regolare di $N=a^{\alpha}b^{\beta}\ldots$ lati, con a, b … numeri primi, si ha che

$$\phi(N)=(a-1)a^{\alpha-1}(b-1)b^{\beta-1}\ \ldots$$

deve essere una potenza di due. Questo accade se $a=b=\ldots=2$ oppure se $a-1$, $b-1$ … sono potenze di 2 e gli esponenti α, β … sono $=1$. In questo secondo caso quindi siamo di fronte a dei primi di Fermat. È facile convincersi che possono essere presenti nella fattorizzazione di N sia una potenze di 2 che primi di Fermat tutti distinti.

A titolo d'informazione sottolineiamo quanto dice Gauss nell'articolo 365 a proposito dei primi di Fermat.

"Ogniqualvolta $n-1$ è una potenza del numero 2, cosa che accade quando il valore di n è uguale a 3, 5, 17, 257, 65537 etc. la suddivisione della circonferenza si riduce alla soluzione di sole equazioni quadratiche".

E successivamente:

"Tutti i valori di n*, quindi, che ci conducono ad equazioni quadratiche, sono di tipo* $2^{2^\nu}+1$*; Si ottengono così i cinque numeri 3, 5, 17, 257, 65537.* […]
In verità la sezione del cerchio non è possibile per tutti i numeri di quella forma, ma soltanto per quelli primi. Fermat, ingannato dalla sua induzione, affermava che tutti i numeri in quella forma fossero necessarimente primi, ma l'illustre Euler ha trovato che tale regola è errata per $\nu = 5$*: si accorse per primo che* $2^{32}+1 = 4294967297$ *contiene il fattore 641".*

Abbiamo estratto queste frasi per ricordare al Lettore che, sebbene siano passati più di duecento anni dalla data di pubblicazione delle Disquisitiones, e sebbene siano stati utilizzati metodi di ricerca potentissimi e raffinatissimi dei più svariati campi, fino ad oggi (22 Novembre 2006) i cinque primi elencati da Gauss sono i soli conosciuti. Ci domandiamo allora se l'espressione "*etc.*" posta dopo 65537, manifesti la convinzione del Maestro dell'esistenza di altri numeri primi di Fermat, oppure se sia semplicemente una forma di prudente pignoleria. Lasciamo al Lettore *l'ardua sentenza.*

Come ultima cosa, dando uno sguardo complessivo a tutto il testo, anche alla luce delle osservazioni fatte, ci piace evidenziare il carattere fortemente aritmetico con cui Gauss tratta la teoria algebrica dei numeri. In verità, questo modo di lavorare non è dissimile dall'impostazione che viene data nei corsi elementari di Algebra, alla teoria dei gruppi. Anche oggi infatti, siamo abituati a risolvere i problemi relativi ai gruppi finiti (ciclici in particolare), sfruttando delle semplicissime relazioni aritmetiche tra numeri interi che rappresentano gli ordini di gruppi e sottogruppi, piuttosto che lavorare in modo più complicato con i singoli elementi.

Bibliografia.

- **E. T. Bell,** *I grandi matematici,* Sansoni Firenze, 1950;
- **W. Dunnington,** *Gauss, titan of science,* The Math. Assoc. of America, 2004;
- **S. Franciosi e F. De Giovanni,** *Elementi di Algebra,* Aracne Editrice, 1992;
- **C. F. Gauss,** *Werke,* voll. I ed VIII;
- **B. M. Kiernan,** *The Development of Galois Theory from Lagrange to Artin,* Archive for History of Exact Science 8, 1971;
- **M. Kline,** *Storia del pensiero matematico,* vol. II, Biblioteca Einaudi Torino, 1991;
- **A. Scimone,** *I primi 200 anni delle Disquisitiones Arithmeticae, 1801-2001,* Lettera pristem 41-42, 2001.