# ATTI

DELLA

# REALE ACCADEMIA NAZIONALE

# DEI LINCEI

ANNO CCCXX

1923

---

SERIE QUINTA

---

## RENDICONTI

---

**Classe di scienze fisiche, matematiche e naturali.**

---

**VOLUME XXXII.**

1° SEMESTRE.

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA NAZIONALE DEI LINCEI

PROPRIETÀ DEL DOTT. PIO BEFANI

1923

# RENDICONTI

DELLE SEDUTE

# DELLA REALE ACCADEMIA NAZIONALE DEI LINCEI

## Classe di scienze fisiche, matematiche e naturali.


*Seduta del 21 gennaio 1923.*

Presidenza del Socio anziano, R. LANCIANI.

## MEMORIE E NOTE DI SOCI

**Matematica.** — *Sulle radici primitive per moduli (ideali) composti nei corpi algebrici.* Nota del Socio LUIGI BIANCHI.

**1.** Si sa che per ogni ideale primo P, in qualunque corpo algebrico, $k(\theta)$, esistono radici primitive, appartenenti cioè all'esponente di Fermat $\Phi(P)$. Sembra però che la questione analoga per qualunque ideale A non sia stata fin qui risoluta. Anche nel caso generale, come nell'ordinaria aritmetica razionale, la ricerca si riduce essenzialmente all'esame del comportamento delle *potenze degli ideali primi* P.

Nelle seguenti pagine, imitando il noto procedimento d'aritmetica razionale [1], si risponde in modo esauriente alla questione mediante i quattro teoremi seguenti:

A) *Se un ideale primo* P *è di grado superiore al primo, nessuna potenza superiore di* P *ammette radici primitive.*

B) *Per ogni ideale primo* P *di primo grado tutte le potenze di* P *ammettono radici primitive, salvo nei due casi eccezionali seguenti:*

1°) *quando il numero primo razionale* $p = NP$, *coordinato all'ideale* P, *è dispari e divisibile per* $P^2$ [2],

2°) *quando sia* $p = 2$.

[1] Cfr. Dirichlet-Dedekind, *Zahlentheorie*, Supplemento V (S° 331-339, IV° Auflage) o pag. 326-334 traduzione italiana.

[2] In tal caso $p$ è numero primo *critico* e divide il numero fondamentale D del corpo.

Rispetto al comportamento delle potenze di P nei due casi eccezionali, si hanno questi due teoremi:

C) *Se $p$ è dispari e divisibile per* $P^2$, *ovvero quando è* $p = 2$, *e non divisibile per* $P^2$, *le potenze di* P, *a cominciare dalla* **terza**, *mancano di radici primitive (le hanno* P *e* $P^2$).

D) *Se è* $p = 2$ *ed è* 2 *divisibile per* $P^2$, *le potenze di* P, *a cominciare dalla* **quarta**, *mancano di radici primitive (le hanno* P, $P^2$ *e* $P^3$).

Come si vede, il caso eccezionale $p = 2$ dell'aritmetica razionale rientra nel teorema C); e lo stesso comportamento offrono i numeri primi critici e dispari per gli ideali primi P che vi entrano al quadrato. L'ulteriore eccezione per $p = 2$ (critico) del caso D) non ha riscontro nel campo razionale, ma si presenta subito, ad esempio, nel campo di Gauss per $P = 1 + i$.

**2.** Nel corpo algebrico $k(\theta)$, di grado $m > 1$, sia P un ideale primo, e sia $p$ il suo numero primo razionale coordinato, talchè, per la norma NP di P, si abbia

$$\text{(1)} \qquad NP = p^f,$$

denotando $f$ il grado dell'ideale primo. Cominciamo dal dimostrare il seguente lemma:

$\alpha$) *Se una potenza superiore* $P^{n+1}$ di $P (n \geq 1)$ *possiede una radice primitiva* $g$, *questa è anche radice primitiva di tutte le potenze inferiori*: $P^n, P^{n-1} \ldots P$.

Basterà provare che $g$ è anche radice primitiva di $P^n$, chè allora lo stesso avverrà per le seguenti potenze.

Sia $\delta$ l'esponente a cui appartiene $g$ (mod. $P^n$), onde $\delta$ dividerà $\Phi(P^n)$, e, posto

$$\text{(2)} \qquad g^\delta = 1 + \omega,$$

sarà $\omega$ un intero [di $k(\theta)$] divisibile per $P^n$. Elevando la (2) alla potenza $p$, risulta

$$g^{\delta p} = 1 + p\omega + \binom{p}{2}\omega^2 + \binom{p}{3}\omega^3 + \cdots,$$

e si osserva che a destra tutti i termini, dopo il primo, sono divisibili per $P^{n+1}$. Difatti $\omega^2, \omega^3 \ldots$ sono divisibili per $P^{2n}, P^{3n} \ldots$ ed è già $2n \geq n + 1$; ma anche il secondo termine $p\omega$ è divisibile per $P^{n+1}$, entrando P in $p$, e $P^n$ in $\omega$. Di qui segue la congruenza

$$g^{\delta p} \equiv 1 \ (\text{mod. } P^{n+1});$$

e siccome $g$ è radice primitiva (mod. $P^{n+1}$), dovrà essere $\delta p$ multiplo del numero

$$\Phi(P^{n+1}) = NP \,.\, \Phi(P^n) = p^f \Phi(P^n)$$

e quindi $\delta$ multiplo di $p^{f-1}\Phi(P^n)$. Ma $\delta$ divide $\Phi(P^n)$, come si è detto; e perchè le due cose siano conciliabili, dovremo avere insieme

$$\delta = \Phi(P^n) \quad , \quad f = 1 .$$

La prima di queste eguaglianze dice che $g$ è radice primitiva di $P^n$, e ne resta dimostrato il lemma $\alpha$). La seconda, $f = 1$, insegna che l'ideale P deve essere di *primo grado*: ciò che prova il teorema A) n. 1.

3. Provato così che le potenze superiori di un ideale primo P *possono* avere radici primitive solo quando P è di 1° grado ($NP = p$), passiamo ad esaminare quello che accade effettivamente in questo caso.

Intanto, pel lemma $\alpha$), se $g$ è radice primitiva (mod. $P^{n+1}$), sarà pure radice primitiva (mod. $P^n$), e dotata inoltre della proprietà che la differenza

$$g^{\Phi(P^n)} - 1 ,$$

divisibile per $P^n$, non è però divisibile per $P^{n+1}$ (altrimenti non sarebbe $g$ radice primitiva rispetto a questo modulo).

Il risultato ora osservato si può in certo modo invertire (senza restrizioni) stabilendo questo secondo lemma:

$\beta$) *Se $g$ è una radice primitiva* (mod. $P^n$) ($n \geq 1$), *dotata della proprietà che il numero $g^{\Phi(P^n)} - 1$ non sia divisibile per $P^{n+1}$, sarà anche $g$ radice primitiva* (mod. $P^{n+1}$).

Pongasi infatti nuovamente

$$g^{\Phi(P^n)} = 1 + \omega , \tag{3}$$

e l'intero $\omega$ sarà divisibile per $P^n$, *ma non per* $P^{n+1}$. Ora l'esponente $\delta$, a cui appartiene $g$ (mod. $P^{n+1}$), divide $\Phi(P^{n+1}) = p\,\Phi(P^n)$ e d'altra parte è multiplo di $\Phi(P^n)$, essendo $g^\delta \equiv 1$ (mod. $P^n$) e $g$ radice primitiva di $P^n$. Per conseguenza $\delta$ avrà o il valore $\Phi(P^n)$, o l'altro $\Phi(P^{n+1})$. Ma il primo caso è escluso da che, nella (3), $\omega$ non è divisibile per $P^{n+1}$; e concludiamo quindi che si ha $\delta = \Phi(P^{n+1})$, ossia che $g$ è radice primitiva (mod. $P^{n+1}$), secondo quanto afferma il lemma $\beta$).

Ed ora nelle ipotesi di questo lemma introduciamo la seguente restrizione:

$\gamma$) *Il numero primo razionale $p$, coordinato a* P, *sia dispari e non divisibile per* $P^2$.

In tal caso possiamo vieppiù precisare il lemma $\beta$) nell'altro:

$\beta'$) *Sotto la restrizione $\gamma$), la radice primitiva $g$* (mod. $P^{n+1}$) *sarà dotata dell'analoga proprietà: che il numero $g^{\Phi(P^{n+1})} - 1$, divisibile per $P^{n+1}$, non è però divisibile per $P^{n+2}$.*

Per dimostrarlo eleviamo nuovamente la (3) alla potenza $p$ ed avremo:

$$g^{\Phi(P^{n+1})} = 1 + p\omega + \frac{p-1}{2} p\omega^2 + \binom{p}{3}\omega^3 + \cdots \tag{4}$$

Qui i termini a destra, da $\omega^3$ in poi, sono divisibili per $P^{3n}$, indi per $P^{n+2}$ a causa di $3n \geq n+2$; ma lo stesso avviene del termine precedente $\frac{p-1}{2} p\omega^2$, perchè $\frac{p-1}{2}$ è intero, $p$ è divisibile per P e $\omega^2$ per $P^{2n}$, indi $p\omega^2$ per $P^{2n+1}$, mentre $2n+1 \geq n+2$. Invece nel secondo termine $p\omega$ a destra, nella (4), come più alta potenza di P entra la $P^{n+1}$, entrando P in $p$ solo alla prima potenza per la restrizione $\gamma$), ed in $\omega$ esattamente alla potenza $P^n$. Se ne deduce dunque in effetto che la differenza $g^{\Phi(P^{n+1})} - 1$, divisibile per $P^{n+1}$, non è però divisibile per $P^{n+2}$, ed anche il lemma $\beta'$) è dimostrato.

È ora evidente come dalla ripetuta applicazione dei lemmi $\beta$) $\beta'$), nelle ammesse ipotesi e con la restrizione $\gamma$), risulta:

*La radice primitiva $g$* (mod. $P^n$) *è anche radice primitiva di tutte le potenze superiori di* P.

**4.** Siamo ora in grado di dimostrare il teorema B) del n. 1, nel cui enunciato è già ammessa la restrizione $\gamma$) del numero precedente.

Pei risultati sopra esposti basterà accertare l'esistenza di radici primitive $g$ del modulo P, tali che la differenza

$$g^{\Phi(P)} - 1 = g^{p-1} - 1,$$

o, ciò che è lo stesso, l'altra $g^p - g$, certamente divisibile per P, non sia però divisibile per $P^2$. Una tale $g$ sarà infatti, per quanto precede, radice primitiva di tutte le potenze superiori di P.

Allo scopo prendiamo una qualunque radice primitiva $\gamma$ (mod. P), e poniamo

$$g = \gamma + \omega, \tag{5}$$

con $\omega$, intero in $k(\theta)$, divisibile per P *e, del resto, arbitrario.* Sarà sempre $g$ radice primitiva (mod. P) e, disponendo di $\omega$, potremo facilmente conseguire che la differenza $g^p - g$ non sia divisibile per $P^2$, che è quanto occorre. Dalla (5), elevata a $p$, si trae infatti

$$g^p = \gamma^p + p\omega\gamma^{p-1} + \binom{p}{2}\omega^2\gamma^{p-2} + \cdots;$$

e poichè tutti i termini a destra, dopo il primo, sono divisibili per $P^2$, ne segue la congruenza

$$g^p \equiv \gamma^p \pmod{P^2},$$

dalla quale, sottraendo la (5), si ha l'altra

$$g^p - g \equiv (\gamma^p - \gamma) - \omega \pmod{P^2}. \tag{6}$$

Ora, se la differenza $\gamma^p - \gamma$ non è divisibile per $P^2$, abbiamo già in $\gamma$ una radice primitiva (mod. P) dotata della proprietà richiesta [si farà allora $\omega = 0$ ovvero $\omega \equiv 0$ (mod. $P^2$)].

Se invece $\gamma^p - \gamma \equiv 0$ (mod. $P^2$), si prenda nella (6) il numero $\omega$ divisibile bensì per P *ma non per* $P^2$, e la radice primitiva $g$ (mod. P), data dalla (5), avrà la proprietà voluta. Così il teorema B) del n. 1 è completamente dimostrato.

Si osservi ancora che, in questa dimostrazione dell'esistenza di radici primitive $g$ (mod. P), con la proprietà che $g^{p-1} - 1$ non sia divisibile per $P^2$, *non è occorsa la restrizione* $\gamma$); e allora, pel lemma $\beta$) n. 3, una tale $g$ è anche radice primitiva (mod. $P^2$). Vale dunque in ogni caso il teorema:

E) *La seconda potenza di un qualunque ideale primo di primo grado ammette sempre radici primitive.*

**5.** Venendo ai casi eccezionali, per provare il teorema C) del n. 1 dimostriamo successivamente:

1°) *Se $p$ è dispari e divisibile per* $P^2$, *già la terza potenza* $P^3$ *non ha radici primitive.* Allora, pel lemma $\alpha$) n. 2, è certo che anche tutte le potenze superiori di P mancano di radici primitive, ed hanno invece, pel teorema E), radici primitive $P^2$ e P. Così sarà provato il teorema C) per $p$ dispari.

Suppongasi, al contrario, $g$ radice primitiva (mod. $P^3$), e per ciò anche di $P^2$, P. Posto

$$g^{\Phi(P)} = 1 + \omega ,$$

sarà $\omega$ divisibile per P (non per $P^2$), ed, elevando a $p$, avremo

$$g^{\Phi(P^2)} = 1 + p\omega + \frac{p-1}{2} p\omega^2 + \cdots$$

Qui i termini a destra, dal terzo in poi, sono divisibili per $P^3$, ed anche il secondo $p\omega$ è divisibile per $P^3$, entrando $P^2$ in $p$ e P in $\omega$; ne segue la congruenza

$$g^{\Phi(P^2)} \equiv 1 \text{ (mod. } P^3).$$

Dunque l'esponente a cui appartiene $g$ (mod. $P^3$) è un divisore di $\Phi(P^2)$, in contraddizione coll'ipotesi che $g$ sia radice primitiva (mod. $P^3$). Similmente, per la seconda ipotesi nel teorema C), dimostriamo:

2°) *Se $p = 2$, e non è divisibile per* $P^2$, *manca già di radici primitive la terza potenza* $P^3$.

Si ammetta al solito, invece, l'esistenza di una tale radice primitiva $g$. Siccome $\Phi(P^2) = 2$, e i numeri 1, 3 sono primi con $P^2$ ed incongrui perchè $3 - 1 = 2$ non è divisibile per $P^2$, nè può essere $g \equiv 1$ (mod. $P^2$), sarà $g \equiv 3$ (mod. $P^2$), ossia

$$g = 3 + \omega \quad , \quad \omega \equiv 0 \text{ (mod. } P^2).$$

Elevando al quadrato, risulta

$$g^2 - 1 = g^{\Phi(P^2)} - 1 = 8 + 6\omega + \omega^2,$$

e i tre termini a destra $8, 6\omega, \omega^2$ sono tutti divisibili per $P^3$.

Si ha dunque, come sopra,

$$g^{\Phi(P^2)} \equiv 1 \pmod{P^3},$$

congruenza inconciliabile coll'ipotesi di $g$ radice primitiva (mod. $P^3$).

Così è dimostrato il teorema C).

**6.** Da ultimo dimostriamo il teorema D) provando che:

*Se $p = 2$ ed è 2 divisibile per $P^2$, già la quarta potenza di P manca di radici primitive, che esistono invece per $P^3$ (e per $P^2$, P).*

Per la prima parte si osservi che, se $g$ è un qualunque numero non divisibile per P, si ha

$$g^{\Phi(P^2)} = 1 + \omega \quad , \quad \text{con } \omega \equiv 0 \pmod{P^2},$$

e, elevando al quadrato,

$$g^{\Phi(P^3)} = 1 + 2\omega + \omega^2.$$

Per le nostre ipotesi, $2\omega$ e $\omega^2$ sono divisibili per $P^4$ e vale dunque, *per qualunque $g$*, la congruenza

$$g^{\Phi(P^3)} \equiv 1 \pmod{P^4},$$

ciò che esclude l'esistenza di radici primitive (mod. $P^4$).

Invece, per la terza potenza $P^3$ riconosciamo l'esistenza di radici primitive come segue: Poniamo

$$g = 1 + \omega$$

con $\omega$ divisibile per P, ma non per $P^2$, e sarà $g$ radice primitiva (mod. $P^2$). Ma si ha

$$g^2 - 1 = g^{\Phi(P^2)} - 1 = 2\omega + \omega^2,$$

ed è $2\omega$ divisibile per $P^3$, ed $\omega^2$ per $P^2$ soltanto, onde $g^{\Phi(P^2)} - 1$ non è divisibile per $P^3$. E allora questa $g$, pel lemma $\beta$) n. 3, è anche radice primitiva (mod. $P^3$), c. d. d.

Osserviamo in fine che il problema qui risolto riguarda i casi in cui il gruppo Abeliano formato dalle sostituzioni lineari

$$x' \equiv ax \pmod{P^n},$$

dove $a$ percorre i $\Phi(P^n)$ moltiplicatori primi con $P^n$, è un gruppo ciclico. La questione si può generalizzare alla ricerca della *base* del gruppo Abeliano

$$x' \equiv ax \pmod{A}$$

per un ideale A, comunque composto.