ATTI

DELLA

REALE ACCADEMIA DEI LINCEI

ANNO CCLXXXIX.

1892

SERIE QUINTA

RENDICONTI

PUBBLICATI PER CURA DEI SEGRETARI

Classe di scienze fisiche, matematiche e naturali.

VOLUME I.

1° Semestre

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA DEI LINCEI

PROPRIETÀ DEL CAV. V. SALVIUCCI

1892

Matematica. — *Sulla risoluzione della congruenza* $x^z \equiv c \pmod{p^\lambda}$. Nota del prof. A. TONELLI, presentata dal Socio V. CERRUTI.

« È noto che, riconosciuta possibile la congruenza

$$x^z \equiv c \pmod{p^\lambda} \tag{1}$$

non si possiede alcuna espressione atta a rappresentarne le radici per ogni valore di p primo dispari. Infatti quando p è della forma $8h+1$, anche se $\lambda = 1$, è duopo ricorrere al tentativo calcolando i numeri

$$c,\ c+p,\ c+2p,\ \ldots,\ c+rp,\ \ldots$$

fin tanto che non se ne sia trovato uno che è quadrato perfetto. Per $\lambda > 1$ poi si conoscono dei metodi mediante i quali si può risolvere la (1) quando sieno note le radici della congruenza

$$y^z \equiv c \pmod{p} \tag{2}$$

e ciò sia direttamente, sia risolvendo successivamente delle congruenze come la (1), nelle quali $\lambda = 1, 2, 4 \ldots$. In ogni caso però non si assegna mai una formula risolutiva della (1).

« In questa Nota io mi propongo di dare una espressione unica atta a rappresentare le radici della (1) qualunque sia la forma del numero primo dispari p, e qualunque sia il valore di λ. La formula cui io giungo ha certamente un interesse più teorico che pratico; ma, per la sua generalità, può essere utile in qualche ricerca speciale. Infatti servendomi di questa formula io giungo ad ottenere una espressione diretta delle radici della (1) per mezzo di quelle della (2).

« 1. Qualunque sia p primo dispari, potrà sempre porsi sotto la forma

$$p = 2^s \alpha + 1$$

con $s \geq 1$ e α dispari, non avendo nissuna importanza il caso di $p = 1$. Avremo allora

$$q(p^\lambda) = p^{\lambda-1}(p-1) = 2^s \alpha\, p^{\lambda-1} = 2^s \gamma$$

con γ dispari; e, poichè supponiamo che la (1) sia possibile, dovrà essere

$$c^{2^{s-1}\gamma} \equiv 1 \pmod{p^\lambda}.$$

Allora se $s > 1$, ricordando che p è dispari, sarà pure

$$c^{2^{s-2}\gamma} \equiv \pm 1 \pmod{p^\lambda}. \tag{3}$$

Sia g un non residuo di p e quindi di p^λ, e si designi con ε_0 un numero che assumeremo uguale a *zero* se nella (3) si ha il segno superiore $(+)$, uguale ad *uno* se si ha il segno inferiore $(-)$: allora potremo scrivere la congruenza

$$g^{2^{s-1}\gamma\varepsilon_0} \equiv c^{2^{s-2}\gamma} \equiv \pm 1 \pmod{p^\lambda}$$

che combinata colla (3) ci dà

$$c^{2^{s-2}\gamma}\, g^{2^{s-1}\gamma\varepsilon_0} \equiv 1 \pmod{p^\lambda}.$$

Da questa se $s > 2$ trarremo ugualmente

$$c^{2^{s-2}\gamma}\, g^{2^{s-2}\gamma\varepsilon_0} \equiv \pm 1 \pmod{p^\lambda} \tag{4}$$

e quindi, designando ancora con ε_1 un numero che supporremo uguale a zero se nella (4) vale il segno superiore (+), uguale ad uno se vale il segno inferiore (—), potremo scrivere

$$c^{2^{s-3}\gamma}\, g^{2^{s-2}\gamma\left|\varepsilon_0+2\varepsilon_1\right|} \equiv 1 \pmod{p^\lambda}.$$

« Proseguendo con questo medesimo metodo, supponiamo che, essendo $s > k-1$, si sia giunti alla congruenza

$$c^{2^{s-k}\gamma}\, g^{2^{s-k+1}\gamma\left|\varepsilon_0+2\varepsilon_1+\ldots+2^{k-2}\varepsilon_{k-2}\right|} \equiv 1 \pmod{p^\lambda} \tag{5}$$

dove le $\varepsilon_2, \varepsilon_3, \ldots, \varepsilon_{k-2}$ sono ancora uguali a zero o ad uno, e sono state determinate nel medesimo modo tenuto per determinare $\varepsilon_0, \varepsilon_1$. Allora, se $s > k$, avremo ancora

$$c^{2^{s-k-1}\gamma}\, g^{2^{s-k}\gamma\left|\varepsilon_0+2\varepsilon_1+\ldots+2^{k-2}\varepsilon_{k-2}\right|} \equiv \pm 1 \pmod{p^\lambda}$$

e designando con ε_{k-1} un numero che è zero od uno secondo che in questa congruenza vale il segno superiore (+) o il segno inferiore (—), avremo

$$c^{2^{s-k-1}\gamma}\, g^{2^{s-k}\gamma\left|\varepsilon_0+2\varepsilon_1+\ldots+2^{k-2}\varepsilon_{k-2}+2^{k-1}\varepsilon_{k-1}\right|} \equiv 1 \pmod{p^\lambda}$$

e quindi la (5) può considerarsi vera in generale, se $s > k-1$.

« Una circostanza importante a notarsi è che le ε sono indipendenti da λ, per modo che se si fosse seguito il medesimo procedimento partendo dalla congruenza

$$c^{2^{s-1}\alpha} \equiv 1 \pmod{p}$$

si sarebbe ottenuto ancora

$$c^{2^{s-k}\alpha}\, g^{2^{s-k+1}\alpha\left|\varepsilon_0+2\varepsilon_1+\ldots+2^{k-2}\varepsilon_{k-2}\right|} \equiv 1 \pmod{p} \tag{5'}$$

dove le ε hanno i medesimi valori che nella (5).

« Per provar questo basta osservare che avendosi

$$a \equiv \pm 1 \pmod{p}$$

essendo p e $p^{\lambda-1}$ dispari si deve pure avere

$$a^{p^{\lambda-1}} \equiv \pm 1 \pmod{p^\lambda}$$

per cui essendo $\gamma = \alpha \cdot p^{\lambda-1}$ è chiaro che nella (5) le ε non possono avere valori diversi da quelli che si sarebbero ottenuti nel giungere alla (5').

« Ciò posto, facciamo nella (5), $k = s$ e moltiplichiamone i due membri per c, avremo

$$\left\{c^{\frac{\gamma+1}{2}}\, g^{\gamma\left|\varepsilon_0+2\varepsilon_1+\ldots+2^{s-2}\varepsilon_{s-2}\right|}\right\}^2 \equiv c \pmod{p^\lambda}$$

e quindi

$$x \equiv \pm c^{\frac{\gamma+1}{2}} g^{\gamma\left[\varepsilon_0+2\varepsilon_1+\ldots+2^{\lambda-2}\varepsilon_{\lambda-2}\right]} \equiv \pm c^{\frac{p^{\lambda-1}\alpha+1}{2}} g^{p^{\lambda-1}\alpha\left[\varepsilon_0+2\varepsilon_1+\ldots+2^{\lambda-2}\varepsilon_{\lambda-2}\right]} \pmod{p^\lambda}$$

rappresenterà le radici della (1).

Ponendo per brevità

$$\varepsilon_0 + 2\,\varepsilon_1 + \ldots + 2^{\lambda-2}\,\varepsilon_{\lambda-2} = \sigma$$

e ricordando che σ è indipendente da λ, potremo dire che

$$x \equiv \pm c^{\frac{p^{\lambda-1}\alpha+1}{2}} g^{p^{\lambda-1}\alpha\sigma} \pmod{p^\lambda} \tag{6}$$

$$y = \pm c^{\frac{\alpha+1}{2}} g^{\alpha\sigma} \pmod{p} \tag{6'}$$

rappresentano respettivamente le radici della (1) e della (2).

Osserviamo che la (6) può scriversi

$$x \equiv \pm \left\{ c^{\frac{\alpha+1}{2}} g^{\alpha\sigma} \right\}^{p^{\lambda-1}} c^{\frac{p^\lambda - 2p^{\lambda-1}+1}{2}} \pmod{p^\lambda}$$

ed allora, poichè la (2) non ha che due radici rappresentate dalla (6'), ne seguirà che, se y rappresenta una radice qualunque della (2), avendosi

$$y \equiv \pm c^{\frac{\alpha+1}{2}} g^{\alpha\sigma} \pmod{p}$$

e quindi

$$y^{p^{\lambda-1}} \equiv \pm \left\{ c^{\frac{\alpha+1}{2}} g^{\alpha\sigma} \right\}^{p^{\lambda-1}} \pmod{p^\lambda}$$

potremo porre

$$x \equiv \pm y^{p^{\lambda-1}} c^{\frac{p^\lambda - 2p^{\lambda-1}+1}{2}} \pmod{p^\lambda}$$

ovvero le radici della (1) vengono così immediatamente espresse per quelle della (2) [1].

3. Determinate le radici della (1) o della (2), colla conoscenza di un non residuo, si ottengono subito le radici dell'altra

$$z^2 \equiv -c \pmod{p^\lambda}.$$

Infatti, poichè questa e la (1) non possono contemporaneamente aver luogo se non si ha $s \geq 2$, avremo

$$\left(x\, g^{2^{s-1}\alpha p^{\lambda-1}}\right)^2 \equiv -c \pmod{p^\lambda}$$

[1] Questa formula, da me comunicata senza dimostrazione all'illustre professore E. Schering, è riportata in una mia Nota *Sulla soluzione della congruenza* $x^2 \equiv c \pmod{p}$, che il medesimo professore ebbe la gentilezza di presentare all'Accademia di Gottinga. La dimostrazione colà accennata dal prof. Schering non è quella che ho dato qui come applicazione delle formule precedentemente ottenute.

e quindi:

$$z \equiv \pm x\, g^{2^{s-2}\alpha p^{\lambda-1}}$$

$$\equiv \pm y^{p^{\lambda-1}} g^{2^{s-2}\alpha p^{2\lambda-1}} c^{\frac{p^{\lambda}-2p^{\lambda-1}+1}{2}} \pmod{p^{\lambda}}.$$

« 4. Consideriamo qualche caso particolare. Se $s=1$ si ha subito per le radici della (1), poichè $\sigma=0$, l'espressione

$$x \equiv \pm c^{\frac{\alpha p^{\lambda-1}+1}{2}} \equiv \pm c^{\frac{p^{\lambda}-p^{\lambda-1}+2}{4}} \pmod{p^{\lambda}}.$$

Questo risultato è noto per $\lambda=1$, sapendosi che le radici della (2) quando $p=2\alpha+1=4k+3$ sono date da

$$y \equiv \pm c^{k+1} \equiv \pm c^{\frac{p+1}{4}} \pmod{p}.$$

Se $s=2$ ovvero $p=4\alpha+1=8k+5$, si ha

$$x \equiv \pm c^{\frac{p^{\lambda-1}\alpha+1}{2}} g^{\alpha p^{\lambda-1}\varepsilon_0} \pmod{p^{\lambda}}$$

dove sarà

$$\varepsilon_0 = 0 \quad \text{se} \quad c^{\alpha p^{\lambda-1}} \equiv 1 \pmod{p^{\lambda}}$$
$$\varepsilon = 1 \quad \text{se} \quad c^{\alpha p^{\lambda-1}} \equiv -1 \pmod{p^{\lambda}}.$$

La formula corrispondente al caso di $\varepsilon_0=0$ è pure conosciuta per $\lambda=1$.

« Si può però giungere ad una espressione che non contiene ε_0 ed è quindi atta a rappresentare le radici della (1) sempre che sia $p=8k+5$.

« Infatti si sa che può prendersi $g=2$ e che alla congruenza

$$c^{\alpha p^{\lambda-1}} \equiv \pm 1 \pmod{p^{\lambda}}$$

deve necessariamente corrispondere l'altra

$$c^{\alpha} \equiv \pm 1 \pmod{p}$$

e viceversa.

« Allora se si ha

$$c^{\alpha} \equiv 1 \pmod{p}$$

avremo

$$c^{\alpha} + 3 \equiv 2^2 \pmod{p}$$

e

$$(c^{\alpha}+3)^{p^{\lambda-1}\alpha} \equiv 2^{2p^{\lambda-1}\alpha} \equiv -1 \pmod{p^{\lambda}}$$

e se si ha

$$c^{\alpha} \equiv -1 \pmod{p}$$

avremo

$$c^{\alpha} + 3 \equiv 2 \pmod{p}$$

e

$$(c^{\alpha}+3)^{p^{\lambda-1}\alpha} \equiv 2^{p^{\lambda-1}\alpha} \equiv g^{p^{\lambda-1}\alpha} \pmod{p^{\lambda}}$$

per cui

$$x \equiv \pm c^{\frac{p^{\lambda-1}\alpha+1}{2}} (c^\alpha + 3)^{p^{\lambda-1}\alpha} \equiv \pm c^{\frac{p^\lambda - p^{\lambda-1}+4}{8}} \left(\frac{p-1}{c^4}+3\right)^{\frac{p^\lambda - p^{\lambda-1}}{4}} \pmod{p^\lambda}$$

rappresenterà le radici della (1) quando $p = 4\alpha + 1 = 8k + 5$.

« 5. Riprendendo la formula generale

$$x \equiv \pm c^{\frac{p^{\lambda-1}\alpha+1}{2}} g^{p^{\lambda-1}\alpha\sigma} \pmod{p^\lambda}$$

vediamo se essa non possa esser di qualche utilità anche quando per la soluzione della (1) sia necessario ricorrere ai tentativi. Il massimo valore che possa assumere σ è $2^{\varepsilon-1} - 1$, per cui il massimo numero delle prove che dovrebbero eseguirsi per trovare il valore di σ corrispondente alle radici della (1) sarebbe $2^{\varepsilon-1} - 1 = \frac{p-2\alpha-1}{2\alpha}$. Questo numero, quando $\alpha > 1$, è più piccolo del numero possibile delle prove da farsi quando per risolvere la (2) si dovessero calcolare i numeri

$$c,\ c+p,\ c+2p,\ \ldots$$

o per risolvere la (1) si dovessero calcolare i numeri

$$c,\ c+p^\lambda,\ c+2p^\lambda,\ \ldots$$

per verificare quale di essi è un quadrato perfetto.

« Si vede che il numero delle prove possibili per determinare σ dipende solo da p, ed è indipendente quindi da c e da λ. Così per $p = 8\alpha + 1$ ed α dispari il numero delle prove per determinare σ non può mai superare 3.

« Inoltre, poichè σ non dipende da λ, per determinarne il valore basterà vedere quando si ha

$$c^{\alpha+1} g^{2\alpha\sigma} \equiv c \pmod{p}$$

ovvero

$$c^\alpha g^{2\alpha\sigma} \equiv 1 \pmod{p}.$$

Si calcolino allora i residui

$$c^\alpha \equiv a \pmod{p}$$
$$g^{2\alpha} \equiv b \pmod{p}$$

in seguito basterà vedere quale dei numeri

$$a,\ ab,\ ab^2,\ \ldots$$

abbia per residuo uno rispetto al modulo p, e trovato

$$ab^k \equiv 1 \pmod{p}$$

sarà determinato σ che può prendersi uguale a k. Si vede che in questo modo le operazioni da farsi, dopo calcolati a e b, sono uniformi e più semplici che non delle estrazioni di radici ».