ATTI

DELLA

REALE ACCADEMIA DEI LINCEI

ANNO CCXC.

1893

SERIE QUINTA

RENDICONTI

Classe di scienze fisiche, matematiche e naturali.

VOLUME II.

1° Semestre

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA DEI LINCEI

PROPRIETÀ DEL CAV. V. SALVIUCCI

1893

gruppi del gruppo aritmetico Φ. Un sottogruppo del gruppo Φ relativo al gruppo lineare, ossia del gruppo [A], si ottiene, per esempio, ponendo

$$M \equiv m\,,\quad N \equiv n\,,\quad R \equiv r\,,\quad S \equiv s \pmod{a}.$$

Ad esso, perchè non limita l'indipendenza delle m, n, r, s, e perchè queste quantità sono amplificate nelle M, N, R, S (si noti che le precedenti congruenze ammettono come caso particolare le eguaglianze $M = m, N = n, R = r, S = s$), corrisponde un sottogruppo eccezionale del gruppo lineare. Calcolando mediante la [E] i coefficienti d'un tale sottogruppo, risulta che esso si compone di quelle sostituzioni del gruppo lineare che sono congruenti all'identità (mod. a).

« In generale, cognito un sottogruppo del gruppo aritmetico [A], che, non limitando l'indipendenza delle m, n, r, s, le amplifichi nelle M, N, R, S, le sostituzioni

$$\left(z, \frac{m'z + n'}{r'z + s'}\right)$$

del relativo sottogruppo eccezionale del gruppo lineare, si conosceranno facendo uso dell'eguaglianza

$$\left(z, \frac{m'z + n'}{r'z + s'}\right) = S^{-1}S_1 = \left(z, \frac{mz + n}{rz + s}\right)^{-1}\left(z, \frac{Mz + N}{Rz + S}\right),$$

dalla quale si ricava, per i coefficienti m', n', r', s' del sottogruppo eccezionale,

$$\begin{aligned} m' &= Ms - Nr \\ n' &= Nm - Mn \\ r' &= Rs - Sr \\ s' &= Sm - Rn \text{ ».} \end{aligned}$$

Matematica. — *Sulla risoluzione della congruenza* $x^2 \equiv c \pmod{p^\lambda}$. Nota del prof. A. Tonelli, presentata dal Socio V. Cerruti.

« 1. In una Nota inserita in questi Rendiconti (1) studiando la congruenza

$$x^2 \equiv c \pmod{p^\lambda} \tag{1}$$

con p numero primo dispari della forma $2^s\alpha + 1$, dopo aver posto

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

ho dimostrato che le radici della (1) potevano esser rappresentate, in ogni caso, dalla formula

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

dove g è un non residuo di p ed $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{s-2}$ dei numeri i quali possono assumere solamente uno dei due valori 0, 1. Questa formula però, come già

(1) Ser. V, vol. I, 1° semestre 1892.

osservai, può avere una importanza più teorica che pratica, riuscendo utile, a causa della sua generalità, piuttosto come strumento di investigazione che per la determinazione numerica delle radici della (1). Infatti, quando anche sia conosciuto il non residuo g, per ottenere, mediante la (2), il valore di quelle radici, è necessario calcolare successivamente le $\varepsilon_0, \varepsilon_1, .., \varepsilon_{s-2}$ nell'ordine in cui sono scritte, o, per tentativi, la quantità complessiva:

$$\varepsilon_0 + 2\varepsilon_1 + ... + 2^{s-2}\varepsilon_{s-2} .$$

« Pel caso però di $s = 2$, la (2) mi permise di stabilire una vera formula risolutiva della (1) mediante i soli elementi noti; ciò che, per quanto io sappia, non veniva fatto coi metodi fin qui adoperati per lo studio di quella congruenza. Questo risultato io potei ottenerlo perchè, per $s = 2$, si conosce un numero (il 3), il quale gode quella proprietà che aumentato di 1 fornisce un residuo, e diminuito di 1 fornisce un non residuo.

« Ora se anche nel caso di s qualunque, fosse possibile di eliminare dalla (2) le ε, riducendola a contenere, oltre g, solo elementi noti, si sarebbe fatto un passo verso la completa soluzione della congruenza (1). La eliminazione delle ε si potrà effettuare quando anche nel caso generale si conosca un numero k il quale goda della stessa proprietà di cui gode il numero 3 pel caso speciale di $s = 2$.

« Supponendo $s \geq 2$ (perchè per $s = 1$ la (1) si risolve immediatamente) il numero k sarà noto quando si conosca un numero h della serie:

$$1 , 2 , .. , p - 1 \tag{3}$$

che sia compreso tra un residuo ed un non residuo: infatti uno dei due numeri:

$$\pm h$$

sarà certo tale che aumentato di 1 fornisce un residuo e diminuito di 1 fornisce un non residuo.

« L'esistenza di un tal numero h è evidente nella serie (3), perchè in essa i residui ed i non residui non possono presentarsi sempre alternati, come è noto [1] e come si capisce subito osservando che 1, 4 sono ambedue residui. Nella serie (3) dovrà quindi presentarsi una successione almeno di due o più residui ed una successione almeno di due o più non residui. Se $s = 2$ abbiamo già osservato che per k può assumersi il numero 3, appunto perchè il 3 o termina una successione di non residui (2, 3) o inizia una successione di residui (3, 4) secondo che 3 è non residuo o residuo di p.

« Ma si potrebbe anche prendere $k = p - 2$ se 3 e quindi $p - 3$ è non residuo, o $k = p - s + 1$ se $p - s$ è il primo non residuo della serie decrescente:

$$p - 3 , p - 4 , p - 5 , ...$$

[1] Cf. p. e., Serret, *Cours d'Algèbre*. Vol. II, pag. 95.

« Se $s \geq 3$, essendo il 2 residuo, abbiamo fin da principio una serie di residui e se l'ultimo della successione dei residui è r basterà prendere:

$$k = p - r \equiv -r \pmod{p}$$

« Ma nella serie (3) vi dovrà essere pure una successione di non residui e se t è l'ultimo di quella successione, poichè non può essere $t = p - 1$, potremo anche prendere:

$$k = t$$

« Si vede dunque che, per $s \geq 2$, non uno solo ma almeno due numeri esistono nella serie (3) che soddisfano le condizioni volute pel numero k [1]; e quei due numeri sono certo distinti perchè uno di essi è residuo e l'altro non residuo.

« 2. Stabilita così l'esistenza del numero k, vediamo qual profitto si possa trarre dalla sua conoscenza per la soluzione della (1).

« Osserviamo che si ha:

$$(k-1)^{2\alpha^{-1}} \equiv \pm 1 \pmod{p}$$

$$(k-1)^{2\gamma^{s-1}} \equiv \pm 1 \pmod{p^\lambda}$$

dove i segni $\pm$ si corrispondono nella stessa formula e nelle due formule. Si ha ancora, colla stessa corrispondenza nei segni:

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

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

e quindi:

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

da cui:

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

e se poniamo, per brevità:

$$v_{s-2} \equiv c^{2\alpha^{s-2}} + k \pmod{p}$$

potremo scrivere:

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

« A questa poi corrisponderà l'altra:

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

[1] Fa eccezione il solo caso di $p = 5$, nel quale la (1) si risolve subito.

e poichè da esse si deducono le congruenze:

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

$$v_{s-2}^{2\alpha^{s-2}} c^{2\alpha^{s-3}} \equiv \pm 1 \pmod{p}$$

colla solita corrispondenza nei segni, ne concluderemo facilmente che si ha pure:

$$\left\{v_{s-2}^{2\alpha^{s-2}} c^{2\alpha^{s-3}} + k\right\}^{2\gamma^{s-1}} v_{s-2}^{2\gamma^{s-2}} c^{2\gamma^{s-3}} \equiv 1 \pmod{p^\lambda}$$

e dopo aver posto per brevità:

$$v_{s-3} \equiv v_{s-2}^{2\alpha^{s-2}} c^{2\alpha^{s-3}} + k$$

sarà:

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

« Proseguendo con questo medesimo metodo e determinando successivamente le quantità $v_{s-2}, v_{s-3}, \ldots, v_{s-h}$, mediante le formule ricorrenti:

$$(4)\quad \left.\begin{aligned} v_{s-2} &\equiv c^{2\alpha^{s-2}} + k \\ v_{s-3} &\equiv c^{2\alpha^{s-3}} v_{s-2}^{2\alpha^{s-2}} + k \\ v_{s-4} &\equiv c^{2\alpha^{s-4}} v_{s-2}^{2\alpha^{s-3}} v_{s-3}^{2\alpha^{s-2}} + k \\ &\ldots\ldots\ldots\ldots \\ v_{s-h} &\equiv c^{2\alpha^{s-h}} v_{s-2}^{2\alpha^{s-h+1}} \ldots\ldots v_{s-h+1}^{2\alpha^{s-2}} + k \end{aligned}\right\} \pmod{p}$$

giungeremo alla congruenza:

$$v_{s-h}^{2\gamma^{s-1}} v_{s-h+1}^{2\gamma^{s-2}} \ldots\ldots v_{s-2}^{2\gamma^{s-h+1}} c^{2\gamma^{s-h}} \equiv 1 \pmod{p^\lambda}$$

come si potrebbe facilmente dimostrare col metodo induttivo.

« Supponendo allora in questa conguenza $h = s$, e dopo averla moltiplicata per c, avremo:

$$\left\{v_0^{2\gamma^{s-2}} v_1^{2\gamma^{s-3}} \ldots\ldots v_{s-4}^{2\gamma^{2}} v_{s-3}^{2\gamma} v_{s-2}^{\gamma} c^{\frac{\gamma+1}{2}}\right\}^2 \equiv c \pmod{p^\lambda}$$

per cui le radici della (1) saranno rappresentate da:

$$x \equiv \pm v_0^{2\gamma} v_1^{2^2\gamma} \dots v_{s-3}^{2^{s-3}\gamma} v_{s-2}^{2^{s-2}\gamma} c^{\frac{\gamma+1}{2}} \pmod{p^\lambda}. \tag{5}$$

« In questo modo, salvo la complicazione della formula, la (1) può ritenersi completamente risoluta quando sia noto il numero k, perchè se, per brevità, abbiamo introdotto i simboli $v_0, v_1, \dots, v_{s-2}$, ad essi possono sostituirsi le loro espressioni mediante gli elementi noti della congruenza, considerando le (4) come uguaglianze.

« Le (4) considerate come congruenze possono piuttosto essere utili pel calcolo numerico delle radici della (1).

« 3. Per $\lambda = 1$ si trae dalla (5) la formula:

$$x_1 \equiv \pm v_0^{2^{s-2}\alpha} v_1^{2^{s-3}\alpha} \dots v_{s-2}^{\alpha} c^{\frac{\alpha+1}{2}} \pmod{p}$$

che serve ad esprimere le radici della congruenza:

$$x_1^2 \equiv c \pmod{p} \tag{1'}$$

poichè le $v_0, v_1, \dots v_{s-2}$ sono indipendenti da λ.

« Osservando allora che la (5) può scriversi:

$$x \equiv \left\{ \pm v_0^{2^{s-2}\alpha} v_1^{2^{s-3}\alpha} \dots v_{s-2}^{\alpha} c^{\frac{\alpha+1}{2}} \right\}^{p^{\lambda-1}} c^{\frac{p^{\lambda-2}p^{\lambda-1}+1}{2}} \pmod{p}$$

si trae di nuovo la formula già da me dimostrata nella nota ricordata in principio:

$$x \equiv x_1^{p^{\lambda-1}} c^{\frac{p^{\lambda-2}p^{\lambda-1}+1}{2}} \pmod{p^\lambda}$$

che serve ad esprimere le radici della (1) per mezzo di quelle della (1').

« 4. La formula (5) è affatto generale, e vale per qualunque forma del numero primo dispari p.

« Per $s = 1$ si trova subito:

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

come già si sapeva dalla (2).

« Per $s = 2$ essendo $p = 4\alpha + 1 = 8h + 5$ si può prendere $k = 3$ e quindi:

$$x \equiv \pm v_0^{\gamma} c^{\frac{\gamma+1}{2}} \equiv \pm (\varrho^\alpha + 3)^{\gamma} c^{\frac{\gamma+1}{2}} \equiv$$
$$\equiv \pm (c^{\frac{p-1}{4}} + 3)^{\frac{p^\lambda - p^{\lambda-1}}{4}} c^{\frac{p^\lambda - p^{\lambda-1}+4}{8}} \pmod{p^\lambda}$$

come già si era trovato nella nota sopra ricordata.

« Finalmente se $s = 3$ si avrà:

$$x \equiv \pm (c^{2\alpha} + k)^{\gamma} \left\{ (c^{2\alpha} + k)^{2\alpha} c^{\alpha} + k \right\}^{2\gamma} c^{\frac{\gamma+1}{2}} \equiv$$

$$\equiv \pm (c^{\frac{p-1}{4}} + k) \left\{ (c^{\frac{p-1}{4}} + k)^{\frac{p-1}{4}} c^{\frac{p-1}{8}} - k \right\} c^{\frac{p^{\lambda} - p^{\lambda-1} + 8}{16}} \pmod{p^{\lambda}}$$

e se, essendo $p = 2^3 \alpha + 1$, la α non è divisibile per 3 si potrà prendere $k = -2$, e se α è divisibile per 3, ma nè α nè $4\alpha + 1$ sono divisibili per 5, potremo prendere $k = -4$.

« Troppo complicata riescirebbe a scriversi la formula se $s > 3$: però quando in $p = 2^{s}\alpha + 1$ la α non sia divisibile per 3, o non sia divisibile per 5 nè α nè $2^{s-3}\alpha + 1$, la (1) può ritenersi completamente risoluta mediante la (5), potendosi prendere in un caso $k = -2$ e nell'altro $k = -4$. In questo modo potremo ritenere come risolute infinite congruenze della forma (1) quando sia $p = 2^{s}\alpha + 1$ e $s \geq 3$.

« 5. La soluzione della (1) in ogni caso è così ricondotta alla ricerca di un numero che goda della proprietà di quello da noi accennato con k, ovvero alla ricerca del primo non residuo di p contenuto nella serie (3); per cui questa condizione non è, in fondo, più restrittiva di quella che ponemmo per istabilire la formula (2): infatti ove per ispeciali condizioni della proposta congruenza (1) non sia conosciuto il non residuo g, e quindi lo si debba in qualche modo cercare, è logico, andando per tentativi, di incominciare le prove dai più piccoli numeri della serie (3). Inoltre abbiamo il mezzo di limitare assai i tentativi da farsi, perchè il primo non residuo deve essere necessariamente un numero assolutamente primo: e supponendo α divisibile per 3 dovremo considerare successivamente i numeri:

$$5 , 7 , 11 , 13 , 17 , \ldots$$

per arrestarci indubbiamente al numero assolutamente primo che precede $\frac{p-1}{4} = 2^{s-2}\alpha$. Ma si può anche far vedere che un non residuo di p deve trovarsi nella serie più ristretta dei numeri primi non superiori a:

$$\frac{p-1}{8} = 2^{s-3}\alpha .$$

« Infatti si vede molto facilmente che non possono essere residui tutti i numeri della serie:

$$1 , 2 , 3 , \ldots , 2^{s-2}\alpha = \frac{p-1}{4}$$

e poichè l'ultimo residuo della successione deve esser pari supponiamo che questa successione sia formata dai numeri:

$$1 , 2 , \ldots , 2\alpha^{s-2} - 2H$$

« Voglio dimostrare che deve essere $2H \geq 2\alpha^{s-3}$.

« Consideriamo infatti gli altri numeri successivi a $2\alpha^{s-2} - 2H$ fino a $2\alpha^{s-1} = \frac{p-1}{2}$, e cioè:

$$2\alpha^{s-2} - 2H + 1 , 2\alpha^{s-2} - 2H + 2 , \ldots , 2\alpha^{s-1} - 4H , 2\alpha^{s-1} - 4H + 1 , \ldots , 2\alpha^{s-1}$$

e si vedrà facilmente che quelli pari sino a $2\alpha^{s-1} - 4H$ sono pure residui perchè risultano del prodotto di 2 per uno dei numeri che formano la supposta successione di residui. Ora il numero di questi residui da aggiungersi a quelli che si presentano in principio della serie (3) è:

$$\frac{1}{2}\left\{2\alpha^{s-1} - 4H - 2\alpha^{s-2} + 2H\right\} = 2\alpha^{s-3} - H .$$

« Ma i 4H numeri che succedono a $2\alpha^{s-1} - 4H$ sino a $2\alpha^{s-1}$ comprenderanno ancora H residui certamente ove già non si supponga ciò che si vuol dimostrare e cioè $2H \geq 2\alpha^{s-3}$; e questi residui saranno rappresentati dai multipli di 4.

« Così avremo certo in tutto, nella serie:

$$1 , 2 , 3 , \ldots , 2\alpha^{s-1} = \frac{p-1}{2} ,$$

un numero di residui espresso da:

$$2\alpha^{s-2} - 2H + 2\alpha^{s-3} - H + H = 2\alpha^{s-2} + 2\alpha^{s-3} - 2H$$

e quindi dovrà essere:

$$2H \geq 2\alpha^{s-3}$$

per cui la successione dei residui non potrà mai proseguirsi al di là della serie:

$$1 , 2 , 3 , \ldots , 2\alpha^{s-3} = \frac{p-1}{8} .$$

« Questa serie potrà ancora maggiormente restringersi quando si considerino i numeri dispari non superiori a $2\alpha^{-1}$ che risultano residui in conseguenza dell'ipotesi fatta circa la successione iniziale, e quando si supponga α divisibile per 3; ma su questo argomento non intendo per ora di trattenermi più oltre ».