ATTI

DELLA

REALE ACCADEMIA DEI LINCEI

ANNO CCCIV.

1907

SERIE QUINTA

RENDICONTI

Classe di scienze fisiche, matematiche e naturali.

VOLUME XVI.

1° Semestre.

ROMA
TIPOGRAFIA DELLA R. ACCADEMIA DEI LINCEI

PROPRIETÀ DEL CAV. V. SALVIUCCI

1907

omografia sopra una superficie di quarto ordine birazionalmente identica alla detta superficie di Kummer.

Un'ultima osservazione:

Le relazioni (11) sono due *relazioni singolari*, perchè rientrano nel tipo:

$$D(h^2 - gg') + Ag + Bh + Cg' + E = 0,$$

con A, ..., E numeri interi, che serve di definizione a tali relazioni.

È noto che, affinchè la superficie iperellittica relativa ad una tabella del tipo (10) possegga integrali di 1ª specie *ellittici*, è necessario e sufficiente che esista una relazione singolare il cui *invariante*, che per la relazione generale scritta avanti è:

$$B^2 - 4AC - 4DE,$$

sia un numero quadrato (1).

Ora, nel nostro caso, ogni relazione singolare tra i periodi (10) è fatta così:

$$\lambda(h^2 - gg' - 3) + \mu(g' - 2g) = 0,$$

con λ, μ interi, e l'invariante è:

$$8\mu^2 + 12\lambda^2.$$

Ma si vede facilmente che questa forma non può rappresentare un quadrato; e quindi il caso in esame è un caso iperellittico *puro* nel senso che non esistono integrali ellittici di 1ª specie, o, ciò che vale lo stesso, la nostra superficie iperellittica non possiede fasci di curve ellittiche.

Matematica. — *Sulla risoluzione apiristica delle congruenze binomie.* Nota I di MICHELE CIPOLLA, presentata dal Corrispondente A. VENTURI.

Noi abbiamo già risoluto, quando il modulo p è un numero primo, la questione di determinare una soluzione *apiristica* della congruenza binomia

$$x^n \equiv a \pmod{p},$$

cioè un polinomio in a, che fornisca una soluzione della congruenza per ogni a residuo n-ico di p (2).

Il problema generale relativo ad un modulo qualunque si riconduce, com'è noto, alla risoluzione di congruenze binomie i cui moduli sono potenze

(1) Humbert, loc. cit.

(2) *Sulla risoluzione apiristica delle congruenze binomie*, Mathematische Annalen, 1906, LXIII Band., pp. 54-61.

di numeri primi, onde noi ci limiteremo alla considerazione delle congruenze della forma

$$x^n \equiv a \pmod{p^m}.$$

È pur noto che il grado n può supporsi divisore di $\varphi(p^m) = p^{m-1}(p-1)$, ma in questa prima nota noi supporremo che n sia una potenza del medesimo numero primo p, rimandando ad una nota successiva la trattazione del caso generale.

Consideriamo dunque la congruenza

$$x^{p^r} \equiv a \pmod{p^m}, \tag{1}$$

essendo p un numero primo dispari. Noi qui otterremo la risoluzione apiristica di questa congruenza collo stesso metodo che applicammo al caso di $p = 2$ [1]: esso è fondato sullo sviluppo in serie di $\sqrt[p^r]{1-z}$.

1. In virtù del teorema di Fermat-Eulero noi possiamo supporre, senza ledere la generalità, che nella congruenza (1) sia $r < m$, nel qual caso, se la congruenza è possibile, cioè quando è soddisfatta la condizione

$$a^{p^{m-r-1}(p-1)} \equiv 1 \pmod{p^m}, \tag{2}$$

la (1) ammette p^r soluzioni.

Dalla condizione (2) intanto si trae

$$a^{p-1} \equiv 1 \pmod{p^{r+1}}$$

e quindi

$$a^{p^r} \equiv a \pmod{p^{r+1}}.$$

Pertanto si può porre

$$a = a^{p^r} - hp^{r+1},$$

essendo h un numero intero, e quindi

$$a \equiv a^{p^r}(1 - \mathrm{A}p^{r+1}) \pmod{p^m}$$

dov'è

$$\mathrm{A} \equiv ha^{-p^r} \equiv \frac{a^{p^r} - a}{p^{r+1}} a^{-p^r} \pmod{p^m} \tag{3}$$ [2].

Allora la (1) diviene

$$x^{p^r} \equiv a^{p^r}(1 - \mathrm{A}p^{r+1}) \pmod{p^m}, \tag{4}$$

[1] *Estensione di un metodo di Legendre alla risoluzione della congruenza* $x^{2^m} \equiv a \pmod{2^k}$, Rend. della R. Accademia delle scienze f. e m. di Napoli, 1905.

[2] Con a^{-1}, ovvero con $\frac{1}{a}$, si suole anche indicare una soluzione della congruenza $ax \equiv 1 \pmod{p^m}$, supposto $a \not\equiv 0 \pmod{p}$.

e però, se x_0 è una soluzione della congruenza

$$x^{p^r} \equiv 1 - Ap^{r+1} \pmod{p^m}, \tag{5}$$

sarà ax_0 una soluzione della (1). Moltiplicando questa per ciascuno dei numeri $1 + kp^{m-r}$ ($k = 0, 1, 2, \ldots, p^r - 1$), che sono tutte le soluzioni della congruenza $x^{p^r} \equiv 1 \pmod{p^m}$, si ottengono tutte le soluzioni della (1). Occupiamoci quindi della risoluzione della congruenza (5).

2. Lo sviluppo di $\sqrt[p^r]{1 - z}$ in serie di potenze di z:

$$1 - c_1 z - c_2 z^2 - \cdots - c_n z^n - \cdots, \tag{6}$$

dov'è

$$c_1 = \frac{1}{p^r},$$

e per $n > 1$

$$c_n = \frac{(p^r - 1)(2p^r - 1)\ldots(\overline{n-1}\,p^r - 1)}{n!\,p^{rn}}, \tag{7}$$

è convergente entro il cerchio di raggio 1, e però lo sviluppo della sua potenza p^r-esima dovrà essere, entro questo cerchio, identico a $1 - z$. Posto $c_0 = -1$, il coefficiente di z^n nello sviluppo della suddetta potenza è

$$-\sum c_{i_1} c_{i_2} \ldots c_{i_{p^r}},$$

essendo la somma estesa a tutte le soluzioni in numeri interi non negativi dell'equazione

$$i_1 + i_2 + \cdots + i_{p^r}.$$

Per $n > 1$ è dunque

$$\sum c_{i_1} c_{i_2} \ldots c_{i_{p^r}} = 0. \tag{8}$$

Di qua si ricava la seguente espressione del coefficiente c_n per mezzo dei coefficienti i cui indici sono inferiori a n:

$$c_n = \frac{1}{p^r}\left[\binom{p^r}{2}\overset{2}{\underset{n}{\mathrm{S}}} c_k - \binom{p^r}{3}\overset{3}{\underset{n}{\mathrm{S}}} c_k + \cdots - \overset{p^r}{\underset{n}{\mathrm{S}}} c_k\right], \quad (n > 1), \tag{9}$$

dove con la notazione isobarica del Cesàro

$$\overset{i}{\underset{n}{\mathrm{S}}} c_k$$

si indica la somma dei prodotti $c_{k_1} c_{k_2} \ldots c_{k_i}$, essendo $k_1, k_2, \ldots, k_i$ numeri interi positivi (diversi da zero), uguali o disuguali, aventi per somma n.

Dalla (9), per induzione completa, si ricava subito la seguente proprietà notevole: *i coefficienti* c_n, *ridotti ai minimi termini, hanno per denominatore una potenza di* p. L'esponente di questa potenza è, come risulta subito dalla (7),

$$rn + \mathrm{mp}\,(p\,,\,n!),$$

dove con la notazione $\mathrm{mp}\,(a\,,\,b)$, essendo a e b due numeri interi, si indica l'esponente della più alta potenza di a che divide b (1).

3. Ciò posto, possiamo dimostrare che una soluzione della congruenza (5) è

$$(10)\quad x_0 \equiv 1 - c_1 \mathrm{A} p^{r+1} - c_2 \mathrm{A}^2 p^{2(r+1)} - \cdots - c_k \mathrm{A}^k p^{k(r+1)} \pmod{p^m}$$

dov'è

$$k = m + 1 + \left[\frac{m-2}{p-2}\right].$$

Dobbiamo innanzi tutto dimostrare che i termini di (10) sono interi, e ciò equivale a dimostrare che è

$$rn + \mathrm{mp}\,(p\,,\,n!) \leqq (r+1)\,n\,.$$

Infatti si ha

$$\mathrm{mp}\,(p\,,\,n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^{[\log_p n]}}\right] \leqq \frac{n-1}{p-1},$$

e però

$$rn + \mathrm{mp}\,(p\,,\,n!) \leqq rn + \frac{n-1}{p-1} < (r+1)\,n\,.$$

Innalziamo ora ambo i membri della (10) alla potenza p^r-esima e sviluppiamo la potenza del secondo membro, ponendo al solito $c_0 = -1$. Si ottiene

$$(11)\quad x_0^{p^r} \equiv -\sum_{n=0}^{k} \mathrm{A}^n p^{n(r+1)} \sum_{(\mathrm{I})_n} c_{i_1} c_{i_2} \ldots c_{i_{p^r}} -$$

$$- \sum_{n=k+1}^{p^r k} \mathrm{A}^n p^{n(r+1)} \sum_{(\mathrm{II})_n} c_{i_1} c_{i_2} \ldots c_{i_{p^r}} \pmod{p^m}.$$

Al secondo membro la somma segnata con $(\mathrm{I})_n$ si estende a tutte le soluzioni in numeri interi non negativi dell'equazione

$$(12)\quad i_1 + i_2 + \cdots + i_{p^r} = n\,,$$

e quindi in virtù di (8) per $n > 1$ è nulla, onde la prima somma si riduce

(1) Peano, *Formulaire mathématique*, 1902, première partie, pag. 73.

a $1 - Ap^{r+1}$. La somma segnata con $(II)_n$ devesi estendere a tutte le soluzioni in numeri interi non negativi e *non superiori ad* n, dell'equazione (12), e noi ora dimostreremo che in tale ipotesi tutti i termini della seconda somma sono divisibili per p^m.

Infatti, indicando con α l'esponente della più alta potenza di p, che divide

$$p^{n(r+1)} \sum_{(II)_n} c_{i_1} c_{i_2} \dots c_{i_{p^r}} \tag{13}$$

si ha

$$\alpha = n(r+1) - \sum_{s=1}^{p^r} [i_s r + mp(p, i_s!)] = n - \sum_{s=1}^{p^r} mp(p, i_s!),$$

e poichè

$$mp(p, n!) \geq \sum_{s=1}^{p^r} mp(p, i!),$$

si ottiene

$$\alpha = n - \sum_{s=1}^{p^r} mp(p, i_s!) \geq n - mp(p, n!) \geq n - \frac{n-1}{p-1}.$$

Essendo poi

$$n \geq k+1 \geq m+2+\left[\frac{m-2}{p-2}\right] \geq m+1+\frac{m-1}{p-2} = \frac{m(p-1)+p-3}{p-2},$$

sarà

$$\alpha \geq n - \frac{n-1}{p-1} = \frac{(p-2)n+1}{p-1} \geq \frac{1}{p-1}[m(p-1)+p-2] > m.$$

Poichè l'esponente della più alta potenza di p, che divide (13), è superiore ad m, tutti i termini della seconda somma di (11) sono divisibili per p^m, e così resta dimostrato che la (10) è una soluzione apiristica della congruenza (5). La (1) ammette quindi la soluzione apiristica

$$x_1 \equiv -a \sum_{n=0}^{k} c_n (1 - a^{1-p^r})^n \pmod{p^m}. \tag{14}$$

4. Il numero k dato dalla formola

$$k = m+1+\left[\frac{m-2}{p-2}\right]$$

è un limite oltre al quale non occorre più spingere il calcolo dei termini, perchè i termini successivi sono tutti divisibili per p^m. Ma alcuni termini, fra i k che si devono considerare, possono essere divisibili per p^m; basterà, p. es., che il coefficiente c_n abbia a denominatore una potenza di p

tale che il suo esponente non sia superiore a $n(r+1)-m$, perchè il termine corrispondente sia divisibile per p^m.

Quest'osservazione torna utile in pratica, come si vedrà nel seguente esempio.

Si voglia determinare una soluzione apiristica della congruenza

$$x^3 \equiv a \pmod{81}.$$

Qui è $r=1$, $m=4$, e però $k=7$. Si ottiene facilmente

$$c_1=\frac{1}{3}\ ,\quad c_2=\frac{1}{3^2}\ ,\quad c_3=\frac{5}{3^4}\ ,\quad c_4=\frac{10}{3^5}\ ,$$
$$c_5=\frac{22}{3^6}\ ,\quad c_6=\frac{73}{3^8}\ ,\quad c_7=\frac{22.17}{3^9}\ .$$

In virtù dell'osservazione fatta, si possono trascurare i termini coi coefficienti c_5, c_6, c_7; una soluzione apiristica della congruenza data è dunque

$$x_1=a\left(1+\frac{a^{16}-1}{3}-\frac{(a^{16}-1)^2}{3^2}+\frac{5(a^{16}-1)^3}{3^4}-\frac{10(a^{16}-1)^4}{3^5}\right).$$

Con questa si possono ottenere subito le radici (quando esistono) di qualunque congruenza binomia cubica secondo il mod. 81.

Matematica. — *Sugli integrali multipli.* Nota di G. Fubini, presentata dal Socio Luigi Bianchi.

1. Mi occuperò qui degli integrali superficiali di una funzione di due variabili x, y. E, come è oramai necessario in questo ordine di studî, mi riferirò agli integrali del Lebesgue (1). Il teorema, che dimostreremo, è il seguente:

Se $f(x,y)$ è una funzione di due variabili x, y, limitata o illimitata, integrabile in un'area Γ del piano (x,y), allora si ha sempre:

$$\int_\Gamma f(x,y)d\sigma=\int dy\int f(x,y)dx=\int dx\int f(x,y)dy\,,$$

quando con $d\sigma$ si intenda l'elemento d'area di Γ (2).

Sull'area Γ faremo dapprima l'ipotesi (del resto non essenziale) che la sua intersezione (3) con una qualsiasi retta $x=\text{cost}$, oppure $y=\text{cost}$ sia (linearmente) misurabile. (Cfr. il n° 2).

(1) Lebesgue, *Intégrale, longuer, aire.* Annali di Matematica 1902.

(2) Quando la presente Nota era già in corso di stampa, mi fu fatto notare che in una osservazione a pie' della pag. 30 della Memoria: *Sul principio di Dirichlet* (Rend. del Circ. Mat. di Palermo, tomo 22), il prof. B. Levi accenna a questo teorema, partendo da alcuni lavori del sig. Pringsheim sugli integrali superficiali di Riemann.

(3) Intersezione di un campo Γ, o di un aggregato E con una retta $x=\text{cost}$, op-