

ANNALI DELLA SCUOLA NORMALE SUPERIORE DI PISA *Classe di Scienze*

G. GEROTTO

Congruenze per integrali ellittici

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4^e série, tome 10, n° 1 (1983), p. 55-68

http://www.numdam.org/item?id=ASNSP_1983_4_10_1_55_0

© Scuola Normale Superiore, Pisa, 1983, tous droits réservés.

L'accès aux archives de la revue « Annali della Scuola Normale Superiore di Pisa, Classe di Scienze » (<http://www.sns.it/it/edizioni/riviste/annaliscienze/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Congruenze per integrali ellittici (*).

G. GEROTTO

È ben noto come i coefficienti dello sviluppo locale di un differenziale di prima specie su una curva ellittica, definita su un anello p -adico, soddisfino a parecchie congruenze, la più celebrata delle quali è quella detta di Atkin e Swynnerton-Dyer (si vedano però le formule 9.2, 9.5 e 9.6 di [2], valide più in generale per gli integrali di una varietà abeliana, dalle quali si ricava subito questa congruenza).

In un recente lavoro (vedi [3]) P. R. Cibotto ne presenta di nuove per i coefficienti del differenziale dx/y sulla curva di equazione $y^2 = (1-x^2)(1-\lambda x)$. Il metodo con cui le ricava si basa sulla seguente osservazione: data una curva ellittica E , definita sull'anello di valutazione discreta $\mathcal{O}$, e presi su di essa due differenziali, linearmente indipendenti, di seconda specie (su $\mathcal{O}$, una condizione più forte del pretendere che i residui siano tutti nulli e i coefficienti del differenziale in $\mathcal{O}$) i loro integrali risultano dipendenti nel completamento formale di E . Questa relazione lineare tra i due integrali determina, in generale, delle congruenze tra i coefficienti dei differenziali. In realtà, in [3] si fanno delle ipotesi restrittive sia su E che su $\mathcal{O}$. Si suppone infatti che E abbia buona riduzione ordinaria e che $\mathcal{O}$ non abbia ramificazione. Quello che conta, invece, è che la riduzione del completamento formale di E sia isomorfa all'iper-algebra del gruppo moltiplicativo. Questa generalizzazione dell'idea della Cibotto permette di trovare delle funzioni analitiche p -adiche globali e rende possibili agganci con alcuni risultati di Dwork (vedi [4], [7]).

In questo lavoro useremo, per la curva ellittica, l'equazione canonica di Jacobi $Y^2 = (1 - X^2)(1 - \lambda X^2)$, perchè per questa si dispone, nella letteratura, di una grande quantità di formule.

La terminologia usata è generalmente quella di Barsotti. Per le poche nozioni di analisi p -adica che usiamo nell'ultimo paragrafo abbiamo seguito la nomenclatura di Dwork.

(*) Lavoro eseguito nell'ambito del G.N.S.A.G.A. del C.N.R.
Pervenuto alla Redazione il 31 Agosto 1981.

1. — Sia K un campo di integrità locale con primo massimo $\mathfrak{p}$, noetheriano e completo rispetto alla topologia $\mathfrak{p}$ -adica. Siano C e k rispettivamente il corpo quoziente e il corpo residuo di K ; supporremo k di caratteristica $p > 0$.

Indichiamo con $R = K[[x]]$ un'iperalgebra su K di dimensione 1 e con $\mathbf{P}$ il suo coprodotto che è dunque un omomorfismo K -lineare di R su $R \hat{\otimes}_K R$. Un elemento η di $C[[x]]$ si dice un *integrale* di R se $d\eta/dx$ è elemento di $K[[x]]$. Seguendo le definizioni date da Barsotti in [1] diremo che un integrale di R è *invariante* se $\mathbf{P}\eta - \eta \hat{\otimes} 1 - 1 \hat{\otimes} \eta = 0$, mentre diremo che è *semiinvariante* se $\mathbf{P}\eta - \eta \hat{\otimes} 1 - 1 \hat{\otimes} \eta$ è elemento di $R \hat{\otimes}_K R$. Chiaramente tra gli integrali semiinvarianti ci sono gli elementi di R . Denoteremo i K -moduli degli integrali invarianti normalizzati e degli integrali semiinvarianti normalizzati di R con $\text{Int}_1 R$ e $\text{Int}_2 R$ rispettivamente (un integrale η si dice *normalizzato* se $\eta(0) = 0$). È ben noto che $\text{Int}_1 R$ è un K -modulo libero di ordine 1 (cfr., p. es. [6]).

Sia M un K -modulo (con topologia discreta); un *sistema di fattori* (addittivo e simmetrico) su $M \hat{\otimes}_K R = R_M$ è un elemento z di $R_M \hat{\otimes}_K R_M$, invariante per scambio di argomenti, tale che $(\mathbf{P} \hat{\otimes} \iota)z + z \hat{\otimes} 1 = (\iota \hat{\otimes} \mathbf{P})z + 1 \hat{\otimes} z$; un sistema di fattori z su R_M si dice *associato a zero* se esiste un elemento y di R_M tale che $z = \mathbf{P}y - y \hat{\otimes} 1 - 1 \hat{\otimes} y$. Indicheremo con $Z_M^2(R)$ il K -modulo dei sistemi di fattori su R , con $B_M^2(R)$ il K -modulo dei sistemi di fattori associati a zero e con $H_M^2(R)$ il K -modulo $Z_M^2(R)/B_M^2(R)$.

LEMMA 1. *Sia R_0 l'iperalgebra ridotta di $R \bmod \mathfrak{p}$. Se R_0 è iperalgebra equidimensionale di codimensione 0 (ovvero, con altra terminologia, di altezza 1) su k , allora il K -modulo $\text{Int}_2 R$ è canonicamente isomorfo al K -modulo $\text{Int}_1 R \oplus R$. Ne segue che $\text{Int}_2 R/R$ è K -modulo libero di ordine 1.*

DIM. Consideriamo un elemento $\eta \in \text{Int}_2 R$; la coassociatività di $\mathbf{P}$ dice che, posto $z = \mathbf{P}\eta - \eta \hat{\otimes} 1 - 1 \hat{\otimes} \eta \in R \hat{\otimes} R$, z è sistema di fattori su R . Dunque esiste l'applicazione σ del K -modulo $\text{Int}_2 R$ sul K -modulo $Z_K^2(R)$ definita da $\sigma\eta = z$; passando al quoziente modulo $B_K^2(R)$ si ottiene un'applicazione $\tilde{\sigma}$ di $\text{Int}_2 R$ su $H_K^2(R)$. È immediato verificare che il nucleo di $\tilde{\sigma}$ è $\text{Int}_1 R \oplus R$ (certamente $\text{Int}_1 R \cap R = 0$, perchè altrimenti R_0 avrebbe un integrale invariante e sarebbe quindi un'iperalgebra additiva, contro l'ipotesi).

Dimostriamo ora che $H_K^2(R) = 0$. Le ipotesi su R_0 ci assicurano intanto che $H_k^2(R_0) = 0$ (si veda [9], Prop. 2.6). Poniamo $M_r = \mathfrak{p}^r/\mathfrak{p}^{r+1}$ e chiamiamo ϱ_r la riduzione di $\mathfrak{p}^r \bmod \mathfrak{p}^{r+1}$. Poniamo poi $R_r = \varrho_r(\mathfrak{p}^r R)$ (dopo aver esteso in modo ovvio ϱ_r a $\mathfrak{p}^r R$). Si ha $R_r = M_r \hat{\otimes}_K R = M_r \hat{\otimes} R_0 = M_r \otimes_K R_0$ perchè M_r , essendo K noetheriano, è k -modulo di dimensione finita. Analogamente si trova $Z_M^2(R) = M_r \otimes_k Z_k^2(R_0)$, $B_M^2(R) = M_r \otimes_k B_k^2(R_0)$ e $H_M^2(R) = M_r \otimes_k H_k^2(R_0)$. Pertanto $H_{M_r}^2(R) = 0$.

Sia $z \in Z_K^2(R)$; allora $\varrho_0 z \in Z_K^2(R_0)$ e dunque esiste un elemento $\bar{y}_0 \in R$ tale che $\mathbf{P}\bar{y}_0 - \bar{y}_0 \hat{\otimes} 1 - 1 \hat{\otimes} \bar{y}_0 = \varrho_0 z$. Sia $y_0 \in R$ tale che $\varrho_0 y_0 = \bar{y}_0$. La differenza $z_1 = z - (\mathbf{P}y_0 - y_0 \hat{\otimes} 1 - 1 \hat{\otimes} y_0)$ sta in $Z_K^2(R)$ ed ha i coefficienti in $\mathfrak{p}$. Quindi $\varrho_1 z_1 \in Z_{M_1}^2(R_0) = B_{M_1}^2(R_0)$ e pertanto si trova un $y_1 \in R$ a coefficienti in $\mathfrak{p}$ tale che $z - (\mathbf{P}(y_0 + y_1) - (y_0 + y_1) \hat{\otimes} 1 - 1 \hat{\otimes} (y_0 + y_1))$ appartenga a $Z_K^2(R)$ e abbia i coefficienti in $\mathfrak{p}^2$. Così proseguendo, per approssimazioni successive, si trova una successione $r \rightarrow y_r$, con $y_r \in \mathfrak{p}^r R$, che, posto $y = \sum_{r=0}^{\infty} y_r \in R$, dà $z = \mathbf{P}y - y \hat{\otimes} 1 - 1 \hat{\otimes} y$, C.V.D.

Questo lemma permette di definire, per ogni generatore libero u di $\text{Int}_2 R/R$ e per ogni elemento v di $\text{Int}_2 R/R$, un elemento $\beta_u(v)$ di K avente la proprietà che

$$(1) \quad v = \beta_u(v) u.$$

È ovvio che $\beta_u(v)$ è unità se e solo se v è generatore libero di $\text{Int}_2 R/R$.

2. — Supponiamo in questo paragrafo che K sia una schiera valutante archimedeo discreta non ramificata di caratteristica 0, con corpo quoziente C e corpo residuo perfetto k di caratteristica $p > 0$. Sia π l'endomorfismo di Frobenius di K . Ricordiamo che π è l'unico endomorfismo di K avente la proprietà che $c^\pi \equiv c^p \pmod{\mathfrak{p}}$ per ogni $c \in K$.

Vogliamo far vedere in questo paragrafo come la (1) dia, come caso particolare, una vecchia conoscenza e cioè l'invariante (generalizzato) di Hasse-Witt. Ricordiamone la definizione. Sia R_0 un'iper algebra di Barsotti-Tate su k ; come è noto il K -modulo M di Dieudonné di R_0 è dotato di due endomorfismi, F (il Frobenius) e V (il Verschiebung). Fissata una K -base $m = (m_1, \dots, m_n)$ di M , la matrice generalizzata (l'invariante, in dimensione 1) di Hasse-Witt è la matrice H tale che $Vm = H\pi^{-1}m$ (si veda [2], parag. 9).

Sia $f(x) = \sum_{n=0}^{\infty} a_n x^n$ una serie di potenze a coefficienti in C ; poniamo:

$$(2) \quad F_* f(x) = \sum_{n=0}^{\infty} a_n^\pi x^{n^p} = f^\pi(x^p),$$

(per questa definizione si vedano [1], [2], [6]).

Supponiamo che $R = K[[x]]$ sia iperalgebra con coprodotto $\mathbf{P}$. Vogliamo dimostrare:

LEMMA 2. *L'applicazione F_* definita da (2) induce un endomorfismo π -semilineare del K -modulo $\text{Int}_2 R/R$.*

DIM. Intanto è ovvio che se $f(x) \in C[[x]]$ è integrale di R , anche $F_*f(x)$ lo è. Poniamo $f(x) = \sum_{n=1}^{\infty} n^{-1} c_n x^n$ con $c_n \in K$ per ogni n , e $\mathbb{P}x = \sum_{i,j=0}^{\infty} a_{ij} x^i \hat{\otimes} x^j$ con $a_{ij} \in K$ per ogni i e ogni j . Si ha

$$\begin{aligned} (F_* \hat{\otimes} F_*) \mathbb{P}f(x) &= (F_* \hat{\otimes} F_*) \left(\sum_{n=1}^{\infty} n^{-1} c_n \left(\sum_{i,j=0}^{\infty} a_{ij} x^i \hat{\otimes} x^j \right)^n \right) \\ &= \sum_{n=1}^{\infty} n^{-1} c_n^{\pi} \left(\sum_{i,j=0}^{\infty} a_{ij} x^{ip} \otimes x^{jp} \right)^n. \end{aligned}$$

D'altra parte è

$$\mathbb{P}F_*f(x) = \mathbb{P} \left(\sum_{n=1}^{\infty} n^{-1} c_n^{\pi} x^{np} \right) = \sum_{n=1}^{\infty} n^{-1} c_n^{\pi} (\mathbb{P}x)^{np} = \sum_{n=1}^{\infty} n^{-1} c_n^{\pi} \left(\sum_{i,j=0}^{\infty} a_{ij} x^i \otimes x^j \right)^{np}.$$

Ora, per ogni n , $\left(\sum_{i,j=0}^{\infty} a_{ij} x^i \hat{\otimes} x^j \right)^{np}$ è uguale ad un elemento del tipo $\left(\sum_{i,j=0}^{\infty} a_{ij}^{\pi} x^{ip} \hat{\otimes} x^{jp} + z_n \right)^n$, ove z_n è elemento di $\mathfrak{p}(R \hat{\otimes} R)$. Ma allora $\mathbb{P}F_*f(x)$ è congruo, modulo un elemento di $R \hat{\otimes} R$, a

$$\sum n^{-1} c_n^{\pi} \left(\sum_{i,j=0}^{\infty} a_{ij} x^{ip} \otimes x^{jp} \right)^n,$$

poichè $n^{-1} \binom{n}{i} p^i$ è elemento di Z_p , se $i = 1, 2, \dots, n$.

Dunque:

$$(F_* \hat{\otimes} F_*) \mathbb{P}f(x) \equiv \mathbb{P}F_*f(x) \text{ modulo } R \hat{\otimes} R$$

che è quanto basta per concludere, C.V.D.

Sia u un generatore di $\text{Int}_2 R/R$; allora esiste $\beta_u(F_*u)$, elemento di K . Sia v un altro generatore di $\text{Int}_2 R/R$, tale che $v = au$ con a unità di K . Si ha, per (1), $F_*v = \beta_v(F_*v)v$; d'altra parte è

$$F_*v = F_*(au) = a^{\pi} F_*u = a^{\pi} \beta_v(F_*u)u = a^{\pi-1} \beta_u(F_*u)v,$$

donde

$$\beta_v(F_*v) = a^{\pi-1} \beta_u(F_*u).$$

Quindi la classe di $\beta_u(F_*u)$ modulo un fattore del tipo $a^{\pi-1}$ con a unità di K è univocamente determinata da F_* .

TEOREMA 1. *Se $R = K[[x]]$ è un'iperalgebra che soddisfa alle ipotesi del lemma 1, e u è un generatore di $\text{Int}_1 R$, si ha*

$$(3) \quad F_*u \equiv pH^{-1}u \text{ mod } pR$$

dove H è l'invariante (generalizzato) di Hasse-Witt di R_0 . Se v è un generatore di $\text{Int}_2 R/R$ si ha $\beta_v(F_* v) = pH^{-1}a^{\pi-1}$, per una opportuna unità a di K .

DIM. Sia M il K -modulo di Dieudonné di R_0 . Poichè R_0 ha dimensione 1 e codimensione 0, M ha ordine 1 come K -modulo ed è determinato dalla unità H di K data da $Vm = H^{\pi-1}m$, se m è un generatore libero di M su K (V è il « verschiebung » di M).

Come spiegato nel paragrafo 6 di [1] (dove l' F_* si chiama π_*), la teoria di Honda ([6]) dimostra che l'elemento $u_0 = (1 - p^{-1}HF_*)^{-1}x$ di $C[[x]]$ definisce su $K[[x]]$ una struttura di iperalgebra (col porre $Px = u_0^{-1}(u_0(x \hat{\otimes} 1) + u_0(1 \hat{\otimes} x))$) che risulta isomorfa a quella di R . Pertanto esiste $\varphi(x) \in K[[x]]$ tale che $\varphi(x) \equiv x \pmod{\text{grado } 2}$ e tale che $u = u_0(\varphi(x))$ sia un integrale invariante di R che genera $\text{Int}_1 R$ su K e che ha la proprietà che $(1 - p^{-1}HF_*)u \equiv 0 \pmod{K[[x]]}$ (Prop. 2.5 di [6]). Pertanto la (3) è dimostrata. È evidente ora che una formula analoga alla (3) vale qualunque sia u generatore di $\text{Int}_1 R$. Ne segue che, se $v = au$ è un generatore di $\text{Int}_2 R/R$, risulta $F_* v = pa^{\pi-1}H^{-1}v$, C.V.D.

COROLLARIO. (Tate, cfr. [5], parag. 5 e [4] parag. 4). Nelle notazioni precedenti, sia K la schiera valutante del prolungamento algebrico massimale non ramificato di C ; esiste un elemento c di $\bar{K}$ tale che $\exp cu$ appartenga a $\bar{K}[[x]]$.

DIM. Se H è l'invariante di Hasse-Witt di R_0 si ha $H = c^{\pi-1}$ per una opportuna unità c di $\bar{K}$. Allora, se $v = cu$, si ha $F_* v = pv$. D'altra parte, si ha

$$\begin{aligned} (p - F_*) \log(1 + x) &= (p - F_*) \sum_{n=1}^{\infty} n^{-1} (-)^{n+1} x^n = \sum_{n=1}^{\infty} (-)^{n+1} p n^{-1} x^n \\ &\quad - \sum_{n=1}^{\infty} (-)^{n+1} n^{-1} x^{np} = \sum_{\substack{n=1 \\ p \nmid n}}^{\infty} (-)^{n+1} p n^{-1} x^n \in pZ_p[[x]]. \end{aligned}$$

Quindi, per il Teorema 3 di [6], $\exp cu$ è elemento di $\bar{K}[[x]]$, C.V.D.

3. - Consideriamo ora la curva ellittica di equazione

$$(4) \quad y^2 = (1 - x^2)(1 - \lambda x^2)$$

a coefficienti in $Z[\lambda]$ con λ indeterminata.

Fissato un primo $p \neq 2$, consideriamo il completamento p -adico $\mathcal{O}$ dell'anello $Z[\lambda]$ e sia K il localizzato di $\mathcal{O}$ in $p\mathcal{O}$. Supporremo che l'equazione (4) abbia i coefficienti in K e chiameremo A la curva su K di equazione (4).

Indicheremo con A_0 la ridotta di $A \bmod pK$. È chiaro che A_0 è una curva ellittica su k . Indicheremo poi con E il punto identità di A e con E_0 il punto identità di A_0 . Scegliamo come punto E il punto di co-ordinate $x = 0$ e $y = 1$.

Per le definizioni che seguono si confronti [2], paragrafi 6 e 7. Sia σ la riduzione di $K[x, y] \bmod pK$ che estendiamo al localizzato S di $K[x, y]$ su $pK[x, y]$. Se poniamo $\bar{x} = \sigma x$ e $\bar{y} = \sigma y$, si ha che σ è omomorfismo di S su $k(\bar{x}, \bar{y})$. Sia ora $k(E_0/A_0)^+$ il primo massimo dell'anello locale del punto E_0 su A_0 . Poniamo $K(E/A) = S_{\mathfrak{p}}$ ove $\mathfrak{p} = \sigma^{-1}k(E_0/A_0)^+$. È immediato verificare che un insieme regolare di parametri di $K(E/A)$ è dato da $\{p, x\}$. La legge di composizione su A dà un coprodotto $\mathbf{P}$ di $K(E/A)$ su $K(E \times E/A \times A)$ (analoga definizione) che si estende al completamento $R = K[[x]]$ dell'anello locale $K(E/A)$ rispetto al suo primo massimo. Dunque R è un'iper-algebra che soddisfa le ipotesi della sezione 1, cioè la sua ridotta modulo p è equidimensionale e di codimensione 0. Le seguenti formule che danno il coprodotto di $K(E/A)$ sono classiche

$$\mathbf{P}x = \frac{x \otimes y + y \otimes x}{1 - \lambda x \otimes x}$$

$$\begin{aligned} \mathbf{P}y &= \\ &= \frac{y \otimes y - \lambda x(1 - x^2) \otimes x(1 - x^2) - x(1 - \lambda x^2) \otimes x(1 - \lambda x^2) + \lambda x^2 y \otimes x^2 y}{(1 - \lambda x^2 \otimes x^2)^2}. \end{aligned}$$

(Si veda p. es., [11]).

Un elemento η di $C[[x]] = C \hat{\otimes}_K R$ si dice un *integrale* su A se $d\eta$ è un differenziale su A , cioè se $d\eta/dx$ è elemento di $K(E/A)$. Un integrale η su A si dice *invariante* se $\mathbf{P}\eta = \eta \hat{\otimes} 1 + 1 \hat{\otimes} \eta$; si dice *seminvariante* se $\mathbf{P}\eta - \eta \hat{\otimes} 1 - 1 \hat{\otimes} \eta$ è elemento di $K(E \times E/A \times A)$. Supporremo tutti gli integrali *normalizzati*, cioè tali che $\eta(0) = 0$. Indicheremo con $\text{Int}_1 A$ e $\text{Int}_2 A$ i K -moduli degli integrali rispettivamente invarianti e semiinvarianti (normalizzati) su A . Vale la pena di osservare che, detta A_C la curva estesa su C , si ha $\text{Int}_2 A \subseteq \text{Int}_2 A_C$ e che gli elementi di $\text{Int}_2 A_C$ sono tutti e soli gli integrali dei differenziali di seconda specie (aventi cioè tutti i residui nulli).

(Per inciso, osserviamo quanto segue. Sia A una curva definita sull'anello $\mathcal{K}$. Se $\mathcal{K}$ è un corpo, un differenziale ω su A si dice di seconda specie se per ogni punto P di A esiste uno $z \in \mathcal{K}(A)$, il corpo delle funzioni razionali su A , tale che $\omega - dz$ non abbia polo in P ; se $\mathcal{K}$ ha caratteristica 0 è ben noto (cfr. per esempio [14]) che questa definizione coincide con quella classica che definisce i differenziali di seconda specie come quei differenziali che hanno il residuo nullo in tutti i punti. Se supponiamo invece che $\mathcal{K}$ sia un anello di valutazione discreta, con primo massimo $\mathcal{K}^+$, la definizione di dif-

ferenziale di seconda specie resta la stessa di prima, dove però $\mathcal{K}(A)$ è definito in modo analogo al $K(E/A)$ che si è definito sopra: è l'anello delle funzioni razionali su A un cui denominatore non sia $\equiv 0 \pmod{\mathcal{K}^+}$. In tutti i casi si può dimostrare che se A è curva ellittica, i differenziali di seconda specie sono tutti e soli quelli semiinvarianti (cfr. [15], 2.2)).

I K -moduli $\text{Int}_1 A$ e $\text{Int}_2 A/K(E/A)$ hanno ordine 1 e 2 rispettivamente (è chiaro che $K(E/A) \subseteq \text{Int}_2 A$). Risulta inoltre $\text{Int}_1 A_C = \text{Int}_1 A \otimes_K C$ e $\text{Int}_2 A_C = \text{Int}_2 A \otimes_K C$. Consideriamo i due differenziali dx/dy e $x^2 dx/y$ su A e siano u e v i rispettivi integrali. Che $u \in \text{Int}_1 A$ è ben noto, mentre che $v \in \text{Int}_2 A$ lo si vede dalla seguente formula classica (vedi, p. es. [12]):

$$\mathbf{P}v = v \otimes 1 + 1 \otimes v + x \otimes x \frac{x \otimes y + y \otimes x}{1 - \lambda x^2 \otimes x^2}.$$

Diamo, come in [3], delle formule esplicite:

$$(5) \quad u = \int dx/y = \sum_{r=0}^{\infty} (2r+1)^{-1} c_{2r+1} x^{2r+1},$$

$$(6) \quad v = x^2 dx/y = \sum_{r=1}^{\infty} (2r+1)^{-1} c_{2r-1} x^{2r+1},$$

ove

$$(7) \quad c_{2r+1} = (-)^r \sum_{j=0}^r \binom{-1/2}{j} \binom{-1/2}{r-j} \lambda^j.$$

In particolare, per $r = (p^i - 1)/2$

$$(8) \quad c_{p^i} = (-)^{(p^i-1)/2} \sum_{j=0}^{(p^i-1)/2} \binom{-1/2}{j} \binom{-1/2}{(p^i-1)/2-j} \lambda^j;$$

si osservi che il termine noto di questo polinomio è

$$(-)^{(p^i-1)/2} \binom{-1/2}{(p^i-1)/2} = ((p^i-1)!)/(2^{p^i-1}((p^i-1)/2)!)^2,$$

che è una unità in Z_p . Questo ci dice che $c_{p^i} \not\equiv 0 \pmod{pK}$, cosa che ci servirà in seguito.

È evidente che ogni elemento di $\text{Int}_2 A$ è elemento anche di $\text{Int}_2 R$. Da ciò segue, applicando i risultati e le notazioni del primo paragrafo, che, in $\text{Int}_2 R/R$, si ha $w = \beta_u(w)u$, per ogni $w \in \text{Int}_2 A$, con $\beta_u(w)$ elemento di K .

Posto $\beta = \beta_u(v)$, come in [3], si può trovare

$$(9) \quad c_{p^i-2} \equiv \beta c_{p^i} \pmod{p^i K},$$

donde

$$(10) \quad \beta(\lambda) = \lim_{i \rightarrow \infty} \frac{c_{p^i-2}(\lambda)}{c_{p^i}(\lambda)}.$$

Altre congruenze di questo tipo si possono ottenere servendosi, invece che di v , di altri elementi di $\text{Int}_2 A$ (i cui coefficienti siano legati, in qualche modo, a quelli di u).

Consideriamo, per esempio, i differenziali $\omega_{2m} = x^{2m} dx/y$. È facile verificare la seguente formula ricorrente (basta derivare $x^{2m-1}y$ mediante la derivazione invariante $d/du = y(d/dx)$):

$$dx^{2m-1}y = (2m-1)\omega_{2(m-1)} - 2m(1+\lambda)\omega_{2m} + (2m+1)\lambda\omega_{2(m+1)}.$$

Detti u_{2m} gli integrali degli ω_{2m} , si ha

$$x^{2m-1}y = (2m-1)u_{2(m-1)} - 2m(1+\lambda)u_{2m} + (2m+1)\lambda u_{2(m+1)}.$$

Da questa formula segue subito, per induzione, che u_{2m} è sempre elemento di $\text{Int}_2 A$, esclusi i casi in cui p divide m . Se $m = p^i n$ con $(p, n) = 1$, allora $p^i u_{2m}$ è elemento di $\text{Int}_2 A$. Per $m = 2$ si ricava

$$3\lambda u_4 = -u + 2(1+\lambda)v + xy,$$

da cui segue, se $p > 3$

$$c_{p^i-4} \equiv \frac{2(1+\lambda)\beta-1}{3\lambda} c_{p^i} \pmod{p^i K}.$$

Consideriamo ora la derivazione Z_p -lineare D_λ di K tale che $D_\lambda \lambda = 1$. Estendiamo D_λ a $K(E/A)$ e ad $R = K[[x]]$, al solito modo, ponendo $D_\lambda x = 0$. È ben noto che $D_\lambda u$ è elemento di $\text{Int}_2 A_G$. Vogliamo dimostrare che $D_\lambda u$ è elemento di $\text{Int}_2 A$. Intanto è

$$D_\lambda(dx/y) = (\tfrac{1}{2})(x^2 dx)/((1-\lambda x^2)y),$$

ed è poi facile verificare, derivando rispetto ad u entrambi i membri, che

$$(\lambda-1) \int \frac{x^2}{1-\lambda x^2} \frac{dx}{y} = -u + v + \frac{xy}{1-\lambda x^2},$$

da cui, in $\text{Int}_2 R/R$

$$(11) \quad (\lambda-1)D_\lambda u = (\tfrac{1}{2})(\beta-1)u.$$

A conclusione di questo paragrafo vogliamo trovare una formula per $\beta_u(F_*u)$. Nel Paragrafo 2 abbiamo definito F_* nell'ipotesi che K fosse anello di valutazione discreta e non ramificata. Estendiamo la definizione al presente K .

Sia $\eta \in \text{Int}_2 R$ con $\eta = \sum_{n=1}^{\infty} n^{-1} a_n(\lambda) x^n$ e gli $a_n(\lambda) \in K$. Poniamo

$$(12) \quad F_*\eta = \sum_{n=1}^{\infty} n^{-1} a_n(\lambda^p) x^{np}.$$

Con la stessa tecnica usata nel lemma 2 si verifica che $F_*\eta$ è elemento di $\text{Int}_2 R/R$. Dunque esiste $\beta_u(F_*u) \in K$ che chiamiamo $\delta(\lambda)$. Si ha, ricordando la (2):

$$F_*u = \sum_{n=1}^{\infty} (2r+1)^{-1} c_{2r+1}(\lambda^p) x^{(2r+1)p};$$

da questa segue, per la (1)

$$(2r+1)^{-1} c_{2r+1}(\lambda^p) \equiv \delta(\lambda) ((2r+1)p)^{-1} c_{(2r+1)p}(\lambda) \pmod{K}.$$

Se facciamo $r = (p^i - 1)/2$, e si moltiplicano ambo i membri per p^{i+1} , si ottiene

$$p c_{p^i}(\lambda^p) \equiv \delta(\lambda) c_{p^{i+1}}(\lambda) \pmod{p^{i+1} K},$$

donde

$$(13) \quad \delta(\lambda) = \lim_{i \rightarrow \infty} \frac{p c_{p^i}(\lambda^p)}{c_{p^{i+1}}(\lambda)}.$$

Per trovare ora una analoga formula per l'invariante di Hasse-Witt dobbiamo estendere K ad un anello K^* che soddisfi le condizioni richieste dal paragrafo 2. Consideriamo il completamento p -adico $\mathcal{O}^*$ dell'anello $Z[\lambda, \lambda^{1/p}, \lambda^{1/p^2}, \dots]$ e denotiamo con K^* il localizzato di $\mathcal{O}^*$ in $p\mathcal{O}^*$ (vedi [3]). Questo anello coincide con l'anello dei vettori di Witt sul perfezionato di $F_p(\bar{\lambda})$, ove $\bar{\lambda}$ è una indeterminata su F_p ; allora λ diventa il rappresentante di Teichmüller di $\bar{\lambda}$. Il Frobenius di K è l'endomorfismo Z_p -lineare π tale che $\lambda^\pi = \lambda^p$. Questo dice che l' F_* che si definisce con π come nel paragrafo 2, coincide con l' F_* che abbiamo definito nella (12). (Naturalmente il secondo opera sugli elementi di $\text{Int}_2 R^*$, ove $R^* = R \hat{\otimes}_K K^*$).

Dalla (3), se indichiamo con $H(\lambda)$ l'invariante di Hasse-Witt di R_0^* , si ricava, con considerazioni analoghe a quelle svolte per $\alpha(\lambda)$,

$$p c_{p^i}(\lambda^p) \equiv p H(\lambda)^{-1} c_{p^{i+1}}(\lambda) \pmod{p^{i+2} K^*},$$

donde,

$$(14) \quad c_{p^{i+1}}(\lambda) \equiv H(\lambda) c_{p^i}(\lambda^p) \bmod p^{i+1} K^*$$

da cui

$$H(\lambda) = \lim_{i \rightarrow \infty} \frac{c_{p^{i+1}}(\lambda)}{c_{p^i}(\lambda^p)}.$$

Da questa formula segue che $H(\lambda)$ è in realtà elemento di K .

Dalle (14) segue, facendo $i = 0$, che

$$c_p(\lambda) \equiv H(\lambda) \bmod pK$$

e quindi

$$(15) \quad c_{p^t}(\lambda) \equiv (c_p(\lambda))^{(p^t-1)/(p-1)} \bmod pK.$$

4. — In questo paragrafo studieremo la specializzazione di alcune delle formule del paragrafo precedente. Indicheremo, come usuale, con Ω il completamento p -adico della chiusura algebrica di $\mathbb{Q}_p$, il corpo dei numeri p -adici. Con $\mathcal{O}$ e $\mathcal{T}$ indicheremo, rispettivamente, l'anello degli interi di Ω e il suo primo massimo. Indicheremo con $|\cdot|$ il valore assoluto non archimedeo di Ω .

Introduciamo le notazioni seguenti: fissato $\alpha \in \mathcal{O}$, consideriamo il corpo $Q_p(\alpha) \subset \Omega$; in $Q_p(\alpha)$, l'anello valutante $\mathcal{O}$ induce un anello di valutazione discreta che prolunga quella p -adica; indicheremo con K_α la chiusura in $\mathcal{O}$ di questo anello di valutazione e con K_α^+ il suo primo massimo (è chiaro che la topologia indotta da $\mathcal{O}$ è quella K_α^+ -adica). Chiaramente $Z_p[\alpha] \subset K_\alpha \subset \mathcal{O}$. Indicheremo con A_α la curva su K_α di equazione

$$y^2 = (1 - x^2)(1 - \alpha x^2)$$

(che si ottiene specializzando per $\lambda = \alpha$ la (4)) considerata a coefficienti in K_α ; indicheremo inoltre con $R(\alpha)$ l'iper algebra su K_α della curva A_α e con $R_0(\alpha)$ la sua ridotta mod $\mathcal{T}$ (in realtà mod $\mathcal{T} \cap K_\alpha$). Poniamo $u(\alpha) = \int dx/y \in \text{Int}_1 R(\alpha)$ e $v(\alpha) = \int x^2 dx/y \in \text{Int}_2 R(\alpha)$. Definiamo, purchè sia possibile (e diremo subito quando lo è)

$$\tilde{\beta}(\alpha) = \beta_{u(\alpha)}(v(\alpha)).$$

Dai risultati del paragrafo 1 segue subito che $\tilde{\beta}(\alpha)$ esiste per tutti e soli i valori di $\alpha \in \mathcal{O}$ per i quali l'iper algebra $R_0(\alpha)$ soddisfa le condizioni del lemma 1, cioè tutti i valori di $\alpha \in \mathcal{O}$ esclusi quelli che danno alla curva A_α una ridu-

zione supersingolare. È ben noto che gli α che danno riduzione supersingolare sono quelli che annullano, mod $\mathfrak{F}$, il coefficiente c_p in (8), o equivalentemente, gli zeri, mod $\mathfrak{F}$, del polinomio

$$H_0(\lambda) = \sum_{j=0}^{(p-1)/2} \binom{-1/2}{j} \lambda^j.$$

In tutti gli altri casi $\tilde{\beta}(\alpha)$ esiste ed è un elemento di $\mathcal{O}$. Qualche dubbio potrebbero far sorgere i valori $\equiv 0, 1 \pmod{\mathfrak{F}}$. Ma osserviamo che

a) se $\alpha \equiv 0 \pmod{\mathfrak{F}}$ e $\alpha \neq 0$, la (4) dà una curva ellittica con cattiva riduzione;

b) se $\alpha = 0$, la (4) dà il cerchio di equazione $x^2 + y^2 = 1$;

c) se $\alpha \equiv 1 \pmod{\mathfrak{F}}$, e $\alpha \neq 1$, la (4) è una curva ellittica con cattiva riduzione e la ridotta è una curva riducibile la cui componente connessa contenente l'identità è la parabola di equazione $y = 1 - x^2$;

d) se $\alpha = 1$, la (4) dà una curva riducibile la cui componente contenente l'identità è come prima la parabola di equazione $y = 1 - x^2$. In tutti e quattro i casi è facile accertarsi che l'iper-algebra $R(\alpha)$ soddisfa le condizioni del lemma 1. Nei casi b e d si ha rispettivamente

$$(16) \quad \int dx/y = \arcsen x, \quad \int x^2 dx/y = (\tfrac{1}{2}) \int dx/y - (\tfrac{1}{2}) xy$$

e

$$(17) \quad \int dx/y = -(\tfrac{1}{2}) \log((x-1)/(x+1)), \quad \int x^2 dx/y = \int dx/y - x,$$

da cui si vede che $t = x + \sqrt{-1}y$ (dopo aver aggiunto eventualmente $\sqrt{-1}$) e $t = (x-1)/(x+1)$, rispettivamente, sono elementi moltiplicativi (cioè tali che $\mathbf{P}t = t \otimes t$) in $R(\alpha)$, che restano tali in $R_0(\alpha)$, mentre nei casi a e c questi stessi elementi si riducono ad elementi moltiplicativi in $R_0(\alpha)$.

Concludendo, se poniamo $\mathfrak{D} = \{\alpha | \alpha \in \mathcal{O}, |H_0(\alpha)| = 1\}$ (vedi [4]), si ha che $\tilde{\beta}$ dà una funzione definita su $\mathfrak{D}$, a valori in $\mathcal{O}$. La (9) continua a valere per la $\tilde{\beta}(\alpha)$, si ha cioè

$$(18) \quad c_{p^i-2}(\alpha) \equiv \tilde{\beta}(\alpha) c_{p^i}(\alpha) \pmod{p^i \mathcal{O}}.$$

D'altra parte, per la (15), gli zeri mod $\mathfrak{F}$ di $c_{p^i}(\lambda)$ sono tutti e soli gli zeri, mod $\mathfrak{F}$, di $c_p(\lambda)$. Da questo segue che, per ogni $\alpha \in \mathcal{O}$, le funzioni razionali

$c_{p^i-2}(\lambda)/c_{p^i}(\lambda)$ sono elementi dell'anello $K_\alpha[\lambda]_q$, ove $\mathfrak{p} = K_\alpha^+ K_\alpha[\lambda] + (\lambda - \alpha) \cdot K_\alpha[\lambda]$. Pertanto la (10) dice che $\beta(\lambda)$ è elemento della chiusura di $K_\alpha[\lambda]_q$ nel completamento K_α^+ -adico dell'anello $K_\alpha[\lambda]_{K_\alpha^+[\lambda]}$, e che quindi $\beta(\alpha)$ esiste ed è elemento di K_α . Confrontando le (9) e le (18) si può concludere che $\tilde{\beta} = \beta$. Infine, risulta

$$\left| \frac{c_{p^i-2}(\alpha)}{c_{p^i}(\alpha)} - \beta(\alpha) \right| \leq p^{-1}$$

uniformemente in $\mathfrak{D}$.

Ricordiamo che una funzione definita su un dominio quasi connesso $\mathfrak{D}$, a valori in Ω , si dice un *elemento analitico di supporto* $\mathfrak{D}$ se è limite uniforme di funzioni razionali senza poli in $\mathfrak{D}$ (si vedano [4], [8], [10]). È pertanto dimostrato

TEOREMA 2. *La funzione β nella (10) è un elemento analitico di supporto $\mathfrak{D}$.*

Osserviamo che dalle (17) segue subito che se $\alpha \equiv 1 \pmod{\mathfrak{F}}$ è anche $\beta(\alpha) \equiv 1 \pmod{\mathfrak{F}}$; poichè β assume valori in $\mathfrak{O}$, il lemma 1.2 di [13] ci assicura che la serie di Taylor di β intorno a $\lambda = 1$ ha i coefficienti in $\mathfrak{O}$. Dunque possiamo scrivere $\beta = 1 + 2(\lambda - 1)\gamma$, con γ elemento analitico, uniformemente limitato, di supporto $\mathfrak{D}$. Dalla (11) segue allora che

$$(19) \quad D_\lambda u = \gamma u$$

con γ elemento analitico, uniformemente limitato, di supporto $\mathfrak{D}$.

La (19) permette di dare una dimostrazione di un caso particolare di un risultato di Dwork ([4], paragrafi 1, 2, 3).

Indichiamo con f la serie ipergeometrica $f(1/2, 1/2, 1, \lambda) = \sum_{j=0}^{\infty} \binom{-1/2}{j} \lambda^j$.

TEOREMA 3. *L'elemento analitico γ della (19) dà il prolungamento analitico su $\mathfrak{D}$ di $D_\lambda \log f$.*

DIM. Ricordiamo un classico teorema (p. es. si veda [14]), secondo il quale l'operatore differenziale di Gauss

$$L = D_\lambda^2 + ((2\lambda - 1)/(\lambda(\lambda - 1)))D_\lambda + 1/(4\lambda(\lambda - 1))$$

a coefficienti funzioni razionali di λ , annulla l'integrale invariante u , dato dalla (5), nel modulo differenziale $\text{Int}_2 A$.

Estendendo gli scalari al corpo delle funzioni meromorfe su $\mathfrak{D}$, la (19) dice che l'operatore $D_\lambda - \gamma$ dà un fattore di L . Sia $z(\lambda)$ una soluzione ologomorfa in 0 dell'equazione differenziale $D_\lambda - \gamma = 0$. Allora (lemma 3.2 di [4])

$z(\lambda)$ è soluzione dell'equazione $L = 0$, non ha zeri in $\mathcal{F} \cap \mathcal{D} = \mathcal{F}$ e quindi deve essere limitata in $\mathcal{F}$ (si vedano le prime righe della dimostrazione del lemma 4.2 di [4]). Ma, sempre dal lemma 4.2 di [4], si sa che l'unica soluzione, olomorfa in 0 e limitata, di $L = 0$ è (a meno di un fattore costante) la f , C.V.D.

Come corollario di questo teorema possiamo dare una formula esplicita per la β di (10), perlomeno per $\alpha \in \mathcal{F}$:

$$\beta(\alpha) = 1 + 2(\alpha - 1)(D_\lambda f/f)(\alpha).$$

Attorno ad altri punti di $\mathcal{D}$ si hanno formule analoghe a questa, in cui, al posto della f , si sostituiscono le soluzioni, olomorfe e limitate, in quei punti, dell'equazione di Gauss $L = 0$.

Passiamo ora alla funzione $\delta(\lambda)$ che compare nella (13). Un argomento perfettamente analogo a quello svolto per la $\beta(\lambda)$ fa vedere che la formula

$$p c_{p^i}(\alpha^p) \equiv \delta(\alpha) c_{p^{i+1}}(\alpha) \pmod{p^{i+1} \mathcal{O}}$$

è vera uniformemente su λ , donde risulta che $\delta(\lambda)$ è elemento analitico di supporto $\mathcal{D}$.

Sia ora $\mathcal{K}$ l'anello delle funzioni di λ olomorfe e limitate in un intorno Δ di 0 tale che $\Delta^p \subseteq \Delta$ e consideriamo l' $\mathcal{K}$ -modulo $M_{\mathcal{K}} = \text{Int}_2 R \otimes \mathcal{K}$. Poniamo inoltre $R_{\mathcal{K}} = R \hat{\otimes} \mathcal{K}$ (i prodotti tensoriali si fanno prendendo per esempio $Z_p[\lambda]$ come anello di base). Se $\eta \in M_{\mathcal{K}}$, si può scrivere $\eta = \sum_{n=1}^{\infty} n^{-1} c_n(\lambda) x^n$, con $c_n \in \mathcal{K}$. È evidente che F_* si estende ad $M_{\mathcal{K}}$ e che se $\eta \in M_{\mathcal{K}}$ e $c(\lambda) \in \mathcal{K}$ si ha $F_*(c(\lambda)\eta) = c(\lambda^p)F_*\eta$.

Ora, se f è, come sopra la serie $f(\frac{1}{2}, \frac{1}{2}, 1, \lambda)$, si ha che $f^{-1}u \in M_{\mathcal{K}}$. D'altra parte l'operatore D_λ si può ovviamente estendere a $M_{\mathcal{K}}$ e allora risulta, tenuto conto della (18) e del Teorema 3,

$$D_\lambda(f^{-1}u) = f^{-2}(fD_\lambda u - (D_\lambda f)u) = f^{-2}(f\gamma - D_\lambda f)u$$

che in Δ è uguale a zero (come elemento di $M_{\mathcal{K}}/R_{\mathcal{K}}$). Dunque, facendo $\lambda = 0$, si ha $f^{-1}u = (f^{-1}u)(0) = f^{-1}(0)u(0) = u(0)$ in $M_{\mathcal{K}}/R_{\mathcal{K}}$. Pertanto $F_*(f^{-1}u) = f_*u(0) = \delta(0)u(0) = \delta(0)f^{-1}u$ in $M_{\mathcal{K}}/R_{\mathcal{K}}$. D'altra parte $F_*(f^{-1}u) = f^{-1}(\lambda^p)F_*u = f^{-1}(\lambda^p)\delta(\lambda)u$, donde $\delta(\lambda) = \delta(0)f(\lambda^p)/f(\lambda)$. Se osserviamo ora che $\delta(\lambda)$ non ha zeri in $\mathcal{D}$, perchè $\delta(\lambda) = pH(\lambda)^{-1}$ e $H(\lambda)$ non ha zeri in $\mathcal{D}$, è dimostrato (vedi [7], prop. 6.13), il seguente

TEOREMA 4. (Dwork [4]). *Nelle notazioni precedenti la funzione $f(\lambda)/f(\lambda^p)$ è prolungabile ad un elemento analitico di supporto $\mathcal{D}$.*

BIBLIOGRAFIA

- [1] I. BARSOTTI, *Bivettori*, Symp. Math., **24** (1981), pp. 23-63.
- [2] I. BARSOTTI, *Varietà abeliane su corpi p -adici*, Symp. Math., **1** (1968), pp. 109-173.
- [3] P. R. CIBOTTO, *Congruences for Abelian Integrals*, Boll. Un. Mat. Ital, (5) **18-A** (1981), pp. 431-433.
- [4] B. DWORK, *p -adic cycles*, Inst. Hautes Études Sci., Publ. Math., no. 37 (1969), pp. 27-115.
- [5] B. DWORK, *A deformation theory for the zeta function of a hypersurface*, Proc. Int. Cong. Math. Stockholm (1962), pp. 247-259.
- [6] T. HONDA, *On the theory of commutative formal groups*, J. Math. Soc. Japan, **22** (1970), pp. 213-246.
- [7] N. KATZ, *Introduction aux travaux récents de Dwork*, Proc. Symp. Pure Math. Amer. Math. Soc., **20** (1971), pp. 65-75.
- [8] M. KRASNER, *Prolongement analytique uniforme et multiforme dans les corps valués complets*, Colloque Int. C.N.R.S., no. 143, Paris, 1966.
- [9] J. LUBIN - J. TATE, *Formal moduli for one-parameter formal Lie groups*, Bull. Soc. Math. France, **94** (1966), pp. 45-59.
- [10] P. ROBBA, *Fonctions analytiques sur les corps values ultrametriques complets*, Asterisque, **10** (1973), pp. 109-220.
- [11] R. FRICKE, *Die Elliptischen Funktionen*, Leipzig-Berlin, 1916.
- [12] E. T. WHITTAKER - G. N. WATSON, *A Course of Modern Analysis*, Cambridge, 1927.
- [13] B. DWORK, *On the zeta function of a hypersurface*, Inst. Hautes Études Sci., Publ. Math., no. 12 (1962), pp. 5-68.
- [14] C. CHEVALLEY, *Introduction to the theory of algebraic functions of one variable*, Amer. Math. Soc., New York, N. Y., 1951.
- [15] I. BARSOTTI, *Factor sets and differentials on abelian varieties*, Trans. Amer. Math. Soc., **84** (1957), pp. 85-108.

Istituto di Algebra e Geometria
Università di Padova
Via Belzoni, 7
35100 Padova