*La Matematica nella Società e nella Cultura*

Rivista dell'Unione Matematica Italiana

Antonella Perucca

# L'ordine dei punti nelle riduzioni di varietà abeliane e tori

*La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Serie 1*, Vol. **3** (2010), n.1 (Fascicolo Tesi di Dottorato), p. 59–62.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RIUMI_2010_1_3_1_59_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma bdim (Biblioteca Digitale Italiana di Matematica) SIMAI & UMI*

http://www.bdim.eu/

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Unione Matematica Italiana, 2010.

La Matematica nella Società e nella Cultura
Rivista dell'Unione Matematica Italiana
Serie I, Vol. III, Aprile 2010, 59-62

# L'ordine dei punti nelle riduzioni di varietà abeliane e tori

Antonella Perucca

Ogni matematico conosce le riduzioni degli interi modulo $n$. Il gruppo ciclico $\mathbb{Z}/n\mathbb{Z}$ è costituito dalle classi di resto modulo $n$. Se $p$ è un numero primo ed $a$ è un intero, la classe $(a \bmod p)$ ha ordine 1 se $p$ divide $a$, altrimenti ha ordine $p$.

Escludendo $(0 \bmod p)$, le classi di resto modulo $p$ formano un gruppo per la moltiplicazione. La classe $(a \bmod p)$ ha come ordine ovviamente un divisore di $p-1$. Ma quanto vale l'ordine di $(a \bmod p)$? Cioè qual è il piú piccolo intero positivo $n$ tale che $a^n - 1$ è un multiplo di $p$? Di solito, bisogna fare un calcolo diretto. Nel 1886, Bang ha dimostrato che se $a > 2$ allora per ogni intero positivo $n$ esiste un primo $p$ tale che l'ordine di $(a \bmod p)$ è esattamente $n$ (invece per $a = 2$ bisogna escludere $n = 1, 6$).

In prima approssimazione, l'obiettivo della tesi è generalizzare questo risultato alle riduzioni di alcuni gruppi algebrici commutativi.

Un gruppo algebrico è in particolare una varietà algebrica (non necessariamente connessa) i cui punti hanno una struttura di gruppo. Una varietà abeliana è un gruppo algebrico, proiettivo e connesso. Un toro è un gruppo algebrico tale che, sulla chiusura algebrica del suo campo di definizione, è un prodotto di copie del gruppo moltiplicativo (il gruppo moltiplicativo è un gruppo algebrico affine connesso di dimensione 1, che si immerge nel piano affine con equazione $xy = 1$). Il gruppo dei punti su una varietà abeliana o su un toro è un gruppo abeliano.

Per ridurre un gruppo algebrico modulo $p$, l'idea è ridurre modulo $p$ i coefficienti delle sue equazioni e le coordinate dei punti.

Ricordiamo che la riduzione modulo $p$ di un numero razionale $\frac{a}{b}$ è ben definita se $p$ non divide $b$ e vale $(a \bmod p) \cdot (b \bmod p)^{-1}$, dove il secondo termine del prodotto è l'inverso moltiplicativo di $(b \bmod p)$. Più in generale, sia $K$ un campo di numeri ed $\mathcal{O}$ il suo anello degli interi. Per ogni ideale primo $p$ di $\mathcal{O}$ non-nullo, il quoziente $k_p = \mathcal{O}/p\mathcal{O}$ è un campo finito. Possiamo esprimere ogni elemento di $K$ nella forma $\frac{a}{b}$, dove $a$ e $b$ appartengono all'anello degli interi di $K$. Allora riduciamo $\frac{a}{b}$ come sopra. Osserviamo che $b$ appartiene solo ad un numero finito di ideali primi di $\mathcal{O}$ quindi $(\frac{a}{b} \bmod p)$ è ben definito per quasi ogni $p$.

Sia $G$ il prodotto di una varietà abeliana e di un toro definito su un campo di numeri $K$. Sia $R$ un elemento di $G(K)$, cioè sia un punto di $G$ definito su $K$. Per quasi ogni $p$, possiamo ridurre $G$ ed $R$ modulo $p$. Se escludiamo ancora un numero finito di primi $p$, possiamo supporre che la riduzione $(G \bmod p)$ sia il prodotto di una varietà abeliana e di un toro definiti su $k_p$. Il punto $(R \bmod p)$ appartiene a $(G \bmod p)$ ed è

definito su $k_p$, quindi è un elemento del gruppo finito $(G \bmod p)(k_p)$. Quanto vale l'ordine di $(R \bmod p)$? Come si comporta l'ordine di $(R \bmod p)$ variando $p$?

Se $R$ in $G(K)$ ha ordine $n$ allora l'ordine di $(R \bmod p)$ vale $n$ per quasi ogni $p$. Adesso supponiamo che $R$ abbia ordine infinito. Sappiamo che l'ordine di $(R \bmod p)$ assume infiniti valori distinti, al variare di $p$. Infatti se per infiniti $p$ l'ordine di $(R \bmod p)$ dividesse un certo intero $n$ si otterrebbe facilemente che $nR$ è l'elemento neutro di $G(K)$, assurdo.

Per tori di dimensione 1, Schinzel nel 1974 ha dimostrato che per quasi ogni intero positivo $n$ esiste un primo $p$ tale che l'ordine di $(R \bmod p)$ è esattamente $n$. L'analogo di questo risultato per varietà abeliane di dimensione 1 (i.e. per curve ellittiche) è stato dimostrato da Silverman, Cheon e Hahn nel 1999. Può lo stesso risultato valere per tori o varietà abeliane di dimensione superiore? La risposta è negativa e adesso vediamo perché.

Chiamiamo $G_R$ il più piccolo sottogruppo algebrico di $G$ che contiene $R$. In particolare, $G_R$ è l'unione di traslati (disgiunti) di un prodotto di una varietà abeliana ed un toro.

Chiamiamo $n_R$ il numero di componenti connesse di $G_R$.

TEOREMA 1. – *Sia $n_R$ il numero di componenti connesse di $G_R$. Allora $n_R$ divide l'ordine di $(R \bmod p)$ per quasi ogni $p$. Inoltre è il più grande intero positivo con tale proprietà.*

Nella nostra tesi ci occupiamo soprattutto di studiare la valutazione $\ell$-adica dell'ordine di $(R \bmod p)$, dove $\ell$ è un numero primo fissato. Scriviamo $ord_\ell$ per indicare la valutazione $\ell$-adica dell'ordine.

TEOREMA 2. – *Sia $a$ un intero non-negativo e consideriamo l'insieme*

$$\Gamma_a = \{p : ord_\ell(R \bmod p) = a\}.$$

*Se $a$ è piú piccolo della valutazione $\ell$-adica di $n_R$, l'insieme $\Gamma_a$ è finito. Negli altri casi, $\Gamma_a$ contiene un insieme di primi $p$ che ha densità di Dirichlet positiva (in particolare, $\Gamma_a$ è un insieme infinito).*

Per dimostrare questi risultati, abbiamo generalizzato un metodo di Khare e Prasad ([2]), che si basa sulla teoria di Kummer (studio dell'azione di Galois sulle radici di $R$) e sulla rappresentazione $\ell$-adica (azione di Galois sui punti di $G$ che hanno ordine una potenza di $\ell$).

Questi risultati erano stati dimostrati da Pink per varietà abeliane ([4]), assumendo che $G_R = G$ (in particolare $n_R = 1$). Per una varietà semi-abeliana (estensione di una varietà abeliana con un toro), la teoria di Kummer e la rappresentazione $\ell$-adica sono molto meno note, quindi non sappiamo se i nostri risultati si possono generalizzare.

Sia $G$ il prodotto di una varietà abeliana e di un toro definiti su un campo di numeri $K$. Prendiamo due punti $P$ e $Q$ in $G(K)$. Il *problema del supporto* studia come sono legati $P$ e $Q$ se supponiamo che la condizione seguente sia verificata:

*per quasi ogni primo $p$ l'ordine di* $(Q \bmod p)$ *divide l'ordine di* $(P \bmod p)$.

Questo accade, ad esempio, se $Q$ è l'immagine di $P$ tramite un endomorfismo di $G$. Per il gruppo moltiplicativo e per varietà abeliane semplici (e.g. curve ellittiche), se $P$ e $Q$ soddisfano la condizione sopra allora esiste un endomorfismo $\phi$ di $G$ tale che $Q = \phi P$. Questi risultati si devono a Corrales-Rodrigàñez e Schoof ([1]) ed a Khare e Prasad ([2]). Nel 2003, Larsen ([3]) ha dimostrato che per una varietà abeliana qualsiasi esistono un intero positivo $c$ (in generale diverso da 1) ed un endomorfismo $\phi$ tale che $cQ = \phi P$. Larsen ha anche dimostrato che l'intero $c$ minimale, pur dipendendo da $P$ e $Q$, divide comunque una costante che dipende solo da $G$ e da $K$. Gli ingredienti della dimostrazione sono ancora una volta la teoria di Kummer e la rappresentazione $\ell$-adica.

Nella tesi, abbiamo esteso i risultati di Larsen a prodotti di varietà abeliane e tori. Abbiamo inoltre indebolito le ipotesi in due modi:

TEOREMA 3 [problema del supporto $\ell$-adico]. – *Sia $\ell$ un numero primo. Siano $P$ e $Q$ due punti di $G(K)$ tali che, per quasi ogni primo $p$, la valutazione $\ell$-adica dell'ordine di* $(Q \bmod p)$ *sia minore o uguale della valutazione $\ell$-adica dell'ordine di* $(P \bmod p)$. *Allora esiste un intero positivo $c$ ed un endomorfismo $\phi$ di $G$ tale che $cQ = \phi P$.*

Con questa ipotesi più debole, abbiamo mostrato che la valutazione $\ell$-adica di $c$, se $c$ è minimale, è zero per quasi ogni $\ell$ e comunque è minore di una costante che dipende solo da $G$ e da $K$.

TEOREMA 4 [problema del supporto radicale]. – *Siano $P$ e $Q$ due punti di $G(K)$ tali che, per quasi ogni primo $p$, il radicale dell'ordine di* $(Q \bmod p)$ *divide il radicale dell'ordine di* $(P \bmod p)$. *Allora esiste un intero positivo $c$ ed un endomorfismo $\phi$ di $G$ tale che $cQ = \phi P$.*

Con questa altra ipotesi abbiamo caratterizzato in maniera analoga la valutazione $\ell$-adica di $c$, se $c$ è minimale. L'unica differenza è che abbiamo perso il controllo su un numero finito di $\ell$.

Si noti che l'origine storica del problema del supporto è una domanda di Erdös del 1988 (a cui Schinzel ha risposto nel 1975!): Supponiamo che $x$ ed $y$ siano interi positivi tali che, per ogni intero $n > 0$ e per quasi ogni numero primo $p$, valga

$$x^n \equiv 1 \pmod p \quad \Rightarrow \quad y^n \equiv 1 \pmod p.$$

È vero che $y$ è una potenza di $x$? La risposta è affermativa. Adattando una dimo-

strazione di Corrales-Rodrigàñez e Schoof, abbiamo mostrato che è possibile richiedere la condizione solo 'per infiniti $n$', se assumiamo la congettura *abc*.

L'ultimo problema di cui ci siamo occupati nella tesi è il *problema di individuare la dipendenza lineare*. La questione è capire se è vero (o quanto fallisce) il seguente principio locale-globale:

*Sia $G$ il prodotto di una varietà abeliana e di un toro definiti su un campo di numeri $K$. Sia $R$ un punto di $G(K)$ e sia $\Lambda$ un sottogruppo finitamente generato di $G(K)$. Il punto $R$ appartiene a $\Lambda$ se e solo se per quasi ogni primo $p$ il punto $(R \bmod p)$ appartiene a $(\Lambda \bmod p)$.*

Questo principio vale per il gruppo moltiplicativo ma non per tori (Schinzel, 1975). Negli anni 2002-2009, diversi autori hanno lavorato al problema: Banaszak, Gajda, Górnisiewicz, Jossen, Kowalski, Krasoń, Weston. Noi abbiamo studiato questo problema come un'applicazione degli altri risultati della tesi.

Abbiamo mostrato che il principio vale se uno assume delle ipotesi su $\Lambda$, come ad esempio se $\Lambda$ è ciclico oppure se è un modulo libero sull'anello degli endomorfismi di $G$. Senza alcuna ipotesi, abbiamo mostrato che un multiplo non nullo di $R$ appartiene al modulo generato da $\Lambda$ sull'anello degli endomorfismi di $G$. Piú recenti sviluppi mostrano che il principio vale per varietà abeliane semplici ma in generale non vale per varietà abeliane.

Come referenza, oltre ai nostri articoli ed alla tesi, si raccomandano principalmente i seguenti:

## BIBLIOGRAFIA

[1] Corrales-Rodrigàñez C. e Schoof R., *The support problem and its elliptic analogue*, J. Number Theory, **64** (1997), 276-290.

[2] Khare C. e Prasad D., *Reduction of homomorphisms mod p and algebraicity*, J. Number Theory, **105** (2004), 322-332.

[3] Larsen M., *The support problem for abelian varieties*, J. Number Theory, **101** (2003), 398-403.

[4] Pink R., *On the order of the reduction of a point on an abelian variety*, Math. Ann., **330** (2004), 275-291.

Via F. Puccinotti 45, 50129 Firenze
e-mail: antonellaperucca@gmail.com
Dottorato in Matematica
con sede presso l'Università di Roma "La Sapienza" – Ciclo XX
Direttore di ricerca: Prof. René Schoof, Università di Roma Tor Vergata