Nonabelian Chabauty study group

1 Calcolo dell'accoppiamento di Weil sui punti di 2-torsione

Sia C la curva (proiettiva, iperellittica, di genere g) corrispondente all'equazione $y^2 = f(x)$, con $f(x) \in K[x]$ di grado $2g+1$ e libero da quadrati. Siano $\alpha_1, \ldots, \alpha_{2g+1}$ le radici di $f(x)$ in $\overline{K}$ e sia $D_i := (\alpha_i, 0) - \infty$. La 2-torsione di $J := \mathrm{Jac}(C)$ è un $\mathbb{F}_2$-spazio vettoriale di dimensione $2g$, generato da $D_1, \ldots, D_{2g+1}$, che rispettano l'unica relazione lineare $\sum D_i = 0 \in J$ (in quanto $\sum D_i = \mathrm{div}(y)$). Vogliamo calcolare $\langle D_i, D_j \rangle$, dove $\langle \cdot, \cdot \rangle$ è l'accoppiamento di Weil. Lo facciamo in modo leggermente indiretto: siano i, j, k tre indici diversi. Calcoliamo $\langle D_i, D_j - D_k \rangle$. Per calcolare l'accoppiamento di Weil è sufficiente trovare funzioni f_1, f_2[1] tali che $\mathrm{div}(f_1) = 2D_i$, $\mathrm{div}(f_2) = 2(D_j - D_k)$ e calcolare $\dfrac{f_1(D_j - D_k)}{f_2(D_i)}$. Possiamo prendere $f_1 = x - \alpha_i$, $f_2 = \dfrac{x - \alpha_j}{x - \alpha_k}$. Otteniamo quindi:

$$\langle D_i, D_j - D_k \rangle = \frac{f_1((\alpha_j, 0))/f_1((\alpha_k, 0))}{f_2((\alpha_i, 0))} = \frac{(\alpha_j - \alpha_i)/(\alpha_k - \alpha_i)}{(\alpha_i - \alpha_j)/(\alpha_i - \alpha_k)} = +1.$$

Ne segue che per ogni terna i, j, j di indici distinti si ha $\langle D_i, D_j \rangle = \langle D_i, D_k \rangle$. In particolare, se si avesse $\langle D_i, D_j \rangle = +1$ per qualche coppia $i \neq j$, allora si avrebbe $\langle D_i, D_k \rangle = +1$ per *ogni* scelta dell'indice k, il che contraddice il fatto che l'accoppiamento di Weil è non degenere. Abbiamo ottenuto:

Lemma 1.1. $\langle D_i, D_j \rangle = \begin{cases} +1, & i = j \\ -1, & i \neq j \end{cases}$

2 Discesa su una curva iperellittica

Notazione: $f(x) = x(x-1)(x-2)(x-5)(x-6)$, C la curva (proiettiva corrispondente a) $y^2 = f(x)$ su $\mathbb{Q}$, J la sua Jacobiana, $L = \mathbb{Q}[x]/(f(x))$, $L_p = \mathbb{Q}_p[x]/(f(x))$, δ la mappa di cobordo in coomologia, δ_p la sua corrispondente su $\mathbb{Q}_p$. In questo discorso p può anche essere ∞, nel qual caso $\mathbb{Q}_p$ è $\mathbb{R}$. Il nostro scopo è dimostrare che $\mathrm{rk}\, J(\mathbb{Q}) = 1$.

[1] con il supporto di $\mathrm{div}(f_1)$ disgiunto dal supporto di $D_j - D_k$ e $\mathrm{div}(f_2)$ disgiunto da D_i

Consideriamo il diagramma

$$\begin{array}{ccc} J(\mathbb{Q}) & \xrightarrow{\delta} & L^\times/L^{\times 2} \\ \downarrow{\scriptstyle \iota_p} & & \downarrow{\scriptstyle \pi_p} \\ J(\mathbb{Q}_p) & \xrightarrow{\delta_p} & L_p^\times/L_p^{\times 2} \end{array}$$

e notiamo che quindi $\pi_p(\delta(J(\mathbb{Q}))) \subseteq \delta_p(J(\mathbb{Q}_p))$.

Lemma 2.1. *Se $J/\mathbb{Q}$ è la Jacobiana di una curva di genere g si ha*

$$\dim_{\mathbb{F}_2} \delta_p(J(\mathbb{Q}_p)) = \dim_{\mathbb{F}_2} J(\mathbb{Q}_p)[2] + \begin{cases} g & p = 2 \\ 0 & p \neq 2, \infty \\ -g & p = \infty \end{cases}$$

Calcoliamo $\delta(J(\mathbb{Q}_p))$ per $p = \infty, 3, 5$ (avrei voluto evitare $p = 2$, ma a posteriori sembra servire; vedere più in basso).

Prima di fare questo, decidiamo di rappresentare un elemento di $L^\times/L^{\times 2}$ come una 5-upla di numeri razionali il cui prodotto sia un quadrato in $\mathbb{Q}^\times$. Calcoliamoci anche le immagini dei punti di 2-torsione e degli altri punti noti, che saranno in ogni caso utili:

$$\begin{array}{cc} (0,0) & (15,-1,-2,-5,-6) \\ (1,0) & (1,-5,-1,-1,-5) \\ (2,0) & (2,1,6,-3,-1) \\ (5,0) & (5,1,3,-15,-1) \\ (6,0) & (6,5,1,1,30) \\ (3,6) & (3,2,1,-2,-3) \\ (10,120) & (10,1,2,5,1) \end{array}$$

Il quinto punto è inutile (nel senso che sta nello span dei primi 4), e così pure il settimo, ma poco male.

- $p = \infty$. Come rappresentanti di $L_p^\times/L_p^{\times 2}$ prendo ovviamente $\{\pm 1\}^5$. La dimensione dell'immagine deve essere 2, quindi troviamo facilmente che essa è generata dal primo e terzo elemento nella lista sopra, che localmente vuol dire che è generata da

  $$(1,-1,-1,-1,-1) \quad \text{e} \quad (1,1,1,-1,-1).$$

  In particolare, per ogni elemento del gruppo di Selmer la prima coordinata deve essere positiva, la seconda e la terza devono avere lo stesso segno, e la quarta e la quinta pure. Volendo, questo dividerebbe per 8 il numero di casi (scenderemmo quindi da $16^4 = 2^{16}$ a 2^{13}), ma tanto ora proveremo a non fare nemmeno un caso a mano[2]. Osserviamo peraltro che $\delta_\infty(J(\mathbb{R}))$ è generato da punti che stanno in $\delta_\infty(J(\mathbb{Q}))$, per cui in particolare $\delta(J(\mathbb{Q}))$ si surgetta su $\delta_\infty(J(\mathbb{R}))$.

[2] e, con il senno di poi, falliremo... ma di poco

- $p = 3$. Come rappresentanti prendo $\{\pm 1, \pm 3\}^5$. L'immagine deve avere dimensione 4; riducendo i punti nella tabella trovo che
  - il primo punto corrisponde a $(-3, -1, 1, 1, 3)$;
  - il secondo corrisponde a $(1, 1, -1, -1, 1)$;
  - il terzo corrisponde a $(-1, 1, -3, -3, -1)$ che è indipendente dai precedenti;
  - il quarto corrisponde a $(-1, 1, 3, 3, -1)$, che salvo errori è il prodotto dei precedenti due e quindi non ci interessa;
  - il quinto corrisponde a $(-3, -1, 1, 1, 3)$, che è uguale al primo;
  - il sesto corrisponde a $(3, -1, 1, 1, -3)$, che mi pare essere indipendente dagli altri.

  Abbiamo quindi determinato $\delta_3(J(\mathbb{Q}_3))$, che è generato da

  $$(-3, -1, 1, 1, 3), (1, 1, -1, -1, 1), (-1, 1, -3, -3, -1), (3, -1, 1, 1, -3),$$

  che sono in particolare le immagini del primo, secondo, terzo, e sesto punti globali che già conosciamo. Nuovamente abbiamo che $\delta(J(\mathbb{Q}))$ si surgetta su $\delta_3(J(\mathbb{Q}_3))$.

- $p = 5$. Rappresentanti: $\{1, -2, -5, 10\}^5$ (la scelta leggermente bizzarra sarà utile più avanti – per ora osservo che tutti i rappresentanti scelti sono congrui ad 1 modulo 3). A meno di errori, l'immagine è generata ancora una volta da classi che provengono tutte da punti in $J(\mathbb{Q})$:

  $$\begin{array}{ll} (0,0) & (10, 1, -2, -5, 1) \\ (1,0) & (1, -5, 1, 1, -5) \\ (2,0) & (-2, 1, 1, -2, 1) \\ (3,6) & (-2, -2, 1, -2, -2) \end{array}$$

Ora, chiamiamo H il sottospazio 5-dimensionale di $L^\times/L^{\times 2}$ che già conosciamo (quello generato dalla torsione e dai punti noti) e $H_p = \pi_p^{-1}(\delta_p(J(\mathbb{Q}_p)))$. Per quanto visto sopra, per $p = 3, 5, \infty$ il sottospazio H_p è generato da H e da $\ker \pi_p$, e noi vorremmo intanto calcolare $H_3 \cap H_5 \cap H_\infty$ (perché questo contiene $\delta(J(\mathbb{Q}))$). Prendiamo un elemento x in questa intersezione: a meno di traslare per un elemento di H, possiamo supporre che stia in $\ker \pi_3 \cap H_5 \cap H_\infty$. Notiamo che $\ker \pi_3$ è il sottogruppo delle 5-uple in

$$\{1, -2, -5, 10\}^5$$

il cui prodotto degli elementi sia un quadrato. Visto che la condizione a 5 è espressa esattamente in termini di questi elementi, scopriamo che $\ker \pi_3 \cap H_5$ è generato da

$$(10, 1, -2, -5, 1), (1, -5, 1, 1, -5), (-2, 1, 1, -2, 1), (-2, -2, 1, -2, -2) \text{ e } \ker \pi_3 \cap \ker \pi_5;$$

quest'ultima intersezione, a sua volta, è banale, come si vede facilmente dal momento che l'unico numero in $\{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}$ che sia un quadrato sia in $\mathbb{Q}_3$ che

in $\mathbb{Q}_5$ è 1. Osserviamo inoltre che $(10,-5,-2,-5,-5)$ è un elemento di H, quindi a meno di traslare per questo ulteriore elemento possiamo assumere che la prima coordinata di x sia 1 o -2.

Prendendo ora in considerazione anche H_∞, ci siamo ridotti a calcolare l'intersezione

$$\langle (1,-5,1,1,-5),(-2,1,1,-2,1),(-2,-2,1,-2,-2)\rangle \cap H_\infty,$$

che (sostituendo l'ultimo generatore con il prodotto di secondo e terzo) è la stessa cosa di

$$\langle (1,-5,1,1,-5),(1,-2,1,1,-2),(-2,1,1,-2,1)\rangle \cap H_\infty,$$

che a sua volta (siccome la prima coordinata degli elementi di H_∞ è positiva) è la stessa cosa di

$$\langle (1,-5,1,1,-5),(1,-2,1,1,-2)\rangle \cap H_\infty,$$

che per verifica diretta non contiene altro che l'elemento banale e $(1,10,1,1,10)$. Reality check: questo elemento è sicuramente banale modulo 3 e modulo ∞, ed è compatibile con le condizioni modulo 5 dal momento che

$$(1,10,1,1,10) = (1,-5,1,1,-5)(-2,1,1,-2,1)(-2,-2,1,-2,-2).$$

Quindi per quanto ne sappiamo finora potrebbe davvero stare nel gruppo di Selmer.

Deduciamo quindi che le condizioni locali a 3, 5, e infinito non bastano, e dobbiamo davvero calcolare il malefico $\delta_2(J(\mathbb{Q}_2))$, che ha dimensione 6. Come rappresentanti di $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ prendiamo $\{\pm 1,\pm 3\}\cup\{\pm 2,\pm 6\}$. Il nostro H (di dimensione 5) per fortuna si inietta in $\delta_2(J(\mathbb{Q}_2))$, quindi per determinare l'intero $\delta_2(J(\mathbb{Q}_2))$ è sufficiente esibire un unico elemento in $\delta_2(J(\mathbb{Q}_2))$ che non stia nel sottospazio generato dalle immagini di H in $L_2/L_2^{\times 2}$. A meno di errori causati dall'ora tarda, i seguenti elementi generano l'immagine di H nella coomologia locale:

$$(1,-2,-6,-6,-2),(1,3,-1,-1,3),(-1,2,3,-2,3),(2,1,6,-3,-1),(3,2,1,-2,-3).$$

Osservo ora che per $x=7$ abbiamo $f(x) = 7\cdot 6\cdot 5\cdot 2\cdot 1 = 420 = 4\cdot 105$, e che 105 è un quadrato in $\mathbb{Z}_2^\times$ (dal momento che è $\equiv 1 \pmod 8$), quindi l'immagine di δ_2 contiene l'immagine del divisore $(7, 2\sqrt{105}) - \infty$, che è $(-1,6,-3,2,1)$. Ma questo è il prodotto del secondo e terzo generatore che abbiamo, mannaggia a lui.

Tuttavia, lo stesso giochino funziona anche con $x=11$, e il divisore corrispondente va in $(3,-6,1,6,-3)$. Questo, a meno di errori, non sta nell'immagine di H, e quindi abbiamo trovato $\delta_2(J(\mathbb{Q}_2))$. Un ultimo sforzo: verifichiamo che $(1,10,1,1,10)$ non rispetti le condizioni locali a 2, ovvero che la sua immagine locale $(1,-6,1,1,-6)$ non stia in $\delta_2(J(\mathbb{Q}_2))$. Siccome

$$(3,-6,1,6,-3)(3,2,1,-2,-3) = (1,-3,1,-3,1)$$

è sufficiente verificare che $(1,-6,1,1,-6)$ non stia nel generato da

$$(1,-2,-6,-6,-2),(1,3,-1,-1,3),(1,-3,1,-3,1),$$

e questo mi sembra chiaro (basta guardare la terza coordinata). Ouf! Fine: questo dimostra che $\dim_{\mathbb{F}_2}\delta(J(\mathbb{Q})) = 5$, e dunque, siccome $\dim_{\mathbb{F}_2} J(\mathbb{Q})[2] = 4$, otteniamo $\operatorname{rk} J(\mathbb{Q}) = 1$ come voluto.