Universitá degli Studi Roma Tre - Corso di Laurea in Matematica

Esercizi CR510

Dario Giannini

3 Aprile 2014

1. Sia $char(K) = 3$ e sia $E:\ y^2 = x^3 + a_2x^2 + a_4x + a_6$ curva ellittica con coefficienti in K.

$$j(E) := \frac{a_2^6}{a_2^2a_4^2 - a_2^3a_6 - a_4^3}$$

(a) Supponiamo per assurdo che $a_2 = a_4 = 0$, allora la curva ellittica sará del tipo $E:\ y^2 = x^3 + a_6$. In particolare si avrá che $x^3 + a_6 = x^3 + \left(\sqrt[3]{a_6}\right)^3 = (x + \sqrt[3]{a_6})^3$ in quanto in caratteristica 3 vale la formula sbagliata. Avrei dunque una radice tripla in $x = \sqrt[3]{a_6}$ e ció andrebbe contro la non singolaritá della curva ellittica E.

(b) Opero il seguente cambio di variabili:

$$\begin{cases} x_1 = x - \dfrac{a_4}{a_2} \\ y_1 = y \end{cases} \rightarrow \begin{cases} x = x_1 + \dfrac{a_4}{a_2} \\ y = y_1 \end{cases}$$

$y_1^2 = \left(x_1 + \dfrac{a_4}{a_2}\right)^3 + a_2\left(x_1 + \dfrac{a_4}{a_2}\right)^2 + a_4\left(x + \dfrac{a_4}{a_2}\right) + a_6;$

$y_1^2 = x_1^3 + \frac{a_4^3}{a_2^3} + a_2x_1^2 + \frac{a_4^2}{a_2} + 2a_4x + a_4x + \frac{a_4^2}{a_2} + a_6$

Basta porre $a_2' = a_2$ e $a_6' = \frac{a_4^3}{a_2^3} + 2\frac{a_4^2}{a_2} + a_6$ per ottenere:

$y_1^2 = x_1^3 + a_2'x^2 + a_6'$.

(c) Se $j(E) = j(E') \Rightarrow \dfrac{a_2^3}{a_6} = \dfrac{(a_2')^3}{a_6'} \Rightarrow$

$a_2^3 = \dfrac{a_6}{a_6'}(a_2')^3$. Se si pone $\frac{a_6}{a_6'} = \mu^6 \ \Rightarrow\ a_2 = \mu^2a_2'$, con $\mu \in \overline{K}^*$.

Dalla relazione precedente si ha anche che $a_6 = \left(\frac{a_2}{a_2'}\right)^3 a_6' = \mu^6a_6'$.

(d)

(e) Se $a_2 = 0 \ \Rightarrow\ j(E) = 0$

Se $a_4 = 0$ basta sostituire nella formula del $j-$invariante per avere $j(E) = -\dfrac{a_2^3}{a_6}$. Per il punto (b) se $a_2 \neq 0$ posso fare un cambiamento di variabile che mi riporti al caso $a_4 = 0$. Sia $k \in \mathbb{K}$ considero la famiglia di curve ellittiche $E_k:\ y^2 = x^3 + kx^2 - k^2 \ \Rightarrow\ j(E) = k$.

(f) Se $j(E) = 0 \ \Rightarrow\ a_2 = 0$ si ha che il cambiamento di variabile esiste per il punto **(b)**.

Se $j(E) \neq 0 \ \Rightarrow\ a_2 \neq 0$ e posso sempre supporre $a_4 = 0$, il cambiamento esiste per il punto **(c)**.

2. Sia $\alpha(x,y) := \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right)$ t.c. $gcd(p(x),q(x)) = gcd(s(x),t(x)) = 1$;
α é un endomorfismo di $E:\ y^2 = x^3 + Ax + B$.

   (a) Per ipotesi si ha che $\alpha(x,y) \in E$, quindi:

$$y^2\frac{s^2(x)}{t^2(x)} = \left(\frac{p(x)}{q(x)}\right)^3 + A\left(\frac{p(x)}{q(x)}\right) + B$$

   Ora si fa il minimo comune multiplo e si sfrutta il fatto che anche $(x,y) \in E$:

$$(x^3 + Ax + B)\frac{s^2(x)}{t^2(x)} = \frac{p^3(x) + Ap(x)q^2(x) + Bq^3(x)}{q^3(x)}$$

   Basta porre $u(x) = p^3(x) + Ap(x)q^2(x) + Bq^3(x)$ per ottenere l'identitá cercata.
   Mi rimane da mostrare che $gcd(u(x),q(x)) = 1$.
   Supponiamo per assurdo che esista $r \in K$, dove K é il campo in cui é definito E, t.c. $u(r) = q(r) = 0$.
   Tuttavia si ha che $u(r) = p^3(r) = 0 \Leftrightarrow p(r) = 0$ ma ció contraddice l'ipotesi di coprimalitá dei polinomi $p(x)$ e $q(x)$ (avrebbero r come radice in comune).

   (b) Sia $t(x_0) = 0$; dal punto precedente si ricava che:

$$\frac{t^2(x_0)}{s^2(x_0)(x_0^3 + Ax_0 + B)} = \frac{q^3(x_0)}{u(x_0)}$$

   Affinché $q(x_0)$ sia uguale a 0 mi basta che si annulli sempre il primo membro dell'equazione. Ció é sempre vero in quanto $gcd(s(x),t(x)) = 1$ per ipotesi e le radici di $t^2(x)$ sono tutte con molteplicitá almeno 2, mentre quelle di $x^3 + Ax + B$ sono semplici poiché E curva ellittica. In particolare ció vuol dire che lo zero del numeratore non potrá mai essere semplificato con un eventuale zero del denominatore.

3. Sia $E:\ y^2 = x^3 + ax$, con $a \neq 0$ e $L:\ y = mx$.
Vado a vedere qual é l'ordine di intersezione tra retta e curva:

$$\begin{cases} y^2 = x^3 + ax \\ y = mx \end{cases} \quad \Rightarrow \quad x^2(x + a - m^2) = 0$$

Se $m \neq \pm\sqrt{a}$ si ha che $ord_{L,(0,0)}(E) = 2$ in quanto $x = 0$ é radice doppia del polinomio.
Se $m = \pm\sqrt{a}$ si ha che $ord_{L,(0,0)}(E) = 3$ in quanto $x = 0$ é radice tripla del polinomio.

4. (a) Sia $C:\ u^2 + v^2 = 1$ e sia $P = (-1,0)$.
   Considero la retta nel piano (u,v) passante per P e avente coefficiente angolare m, descritta dalle cordinate parametriche

$$\begin{cases} u = -1 + t \\ v = mt \end{cases}$$

Per cercare una parametrizzazione della curva C dipendente da un solo parametro considero il secondo punto di intersezione tra C stessa e la retta dipendente da m.
$(t-1)^2 + m^2t^2 = 1 \quad t^2 - 2t + m^2t^2 = 0 \quad t(t(1+m^2) - 2) = 0 \Leftrightarrow$
$t = 0 \to P$,
$t = \dfrac{2}{1+m^2}$ che descrive il secondo punto di intersezione al variare di m. Andando a sostituire nell'equazione parametrica della retta si ottiene la parametrizzazione di C cercata:

$$u = \frac{1-m^2}{1+m^2} \quad v = \frac{2m}{1+m^2}$$

(b) Mi basta passare a coordinate proiettive per poter scrivere un punto generico della curva al variare di m come $Q = \left[\dfrac{1-m^2}{1+m^2} : \dfrac{2m}{1+m^2} : 1\right] =$ $[1-m^2 : 2m : 1+m^2]$. Q nella sua forma omogenea é equivalente a $[n^2 - m^2 : 2mn : m^2 + n^2]$.
Se x é pari per simmetria dell'equazione posso considerare il punto $[2mn : n^2 - m^2 : m^2 + n^2]$. Si é dunque dimostrato che se $\exists x, y, z \in \mathbb{Z}$ t.c. $x^2 + y^2 = z^2$ e x é pari al variare di m, n in $\mathbb{Z}$ posso descrivere la soluzione dell'equazione come:

$$x = 2mn \;\; y = n^2 - m^2 \;\; z = m^2 + n^2$$

Ora, ipotizzando che $gcd(x, y, z) = 1$, si vuole dimostrare che $gcd(m, n) = 1$ e che $m \not\equiv n \ (mod\ 2)$.
Supponiamo per assurdo che $gcd(m, n) = d \neq 1$ allora $m = dm'$, $n = dn'$ e si ha che:

$$x = 2d^2m'n' \;\; y = d^2(n'^2 - m'^2) \;\; z = d^2(n'^2 + m'^2)$$

da cui si ricava subito che $gcd(x, y, z) = d^2$ contro l'ipotesi iniziale.
In maniera analoga si dimostra che $m \not\equiv n \ (mod\ 2)$. Supponiamo per assurdo che non sia vero, allora $2|n-m$. Tuttavia poiché $y = n^2 - m^2 = (n-m)(n+m) \Rightarrow 2|y$ e quindi 2 divide anche z in quanto $z^2 = x^2 + y^2$. Tutto ció va contro l'ipotesi di coprimalitá di x, y, z.

5. Siano $p(x), q(x)$ due polinomi t.c. $gcd(p(x), q(x)) = 1$, si vuole dimostrare che:

$$\frac{d}{dx}\left(\frac{p(x)}{q(x)}\right) = 0 \Leftrightarrow p(x) \equiv q(x) \equiv 0$$

$\dfrac{p'(x)q(x) - p(x)q'(x)}{q^2(x)} = 0 \Leftrightarrow p'(x)q(x) = q'(x)p(x)$
Tuttavia ció implica che $q(x)|q'(x)p(x)$. Basta applicare il lemma di Euclide sfruttando l'ipotesi $gcd(p(x), q(x)) = 1$ per ricavarne che $q(x)|q'(x)$. Tale configurazione risulta possibile se e solo se $q'(x) \equiv 0$, in quanto $q'(x)$ é un polinomio di un grado inferiore a $q(x)$. A questo punto se $q'(x) \equiv 0$ si deve avere che $p'(x)q(x) \equiv 0 \Leftrightarrow p'(x) \equiv 0$.

6. Sia $E: \ x^3 + Ax + B$ una curva ellittica definita su un campo K e sia $d \in K^*$.
Sia $E^d := \ x^3 + Ad^2x + Bd^3$.

(a) Si vuole verificare che $j(E) = j(E^d)$:

$$j(E^d) = 1728\frac{4d^6A^3}{4d^6A^3 + 27B^2d^6} = 1728\frac{4A^3}{4A^3 + 27B^2} = j(E)$$

(b) Basta fare il seguente cambiamento di variabile con coefficienti in $E[\sqrt{d}]$:

$$\begin{cases} x \longmapsto dx \\ y \longmapsto d\sqrt{d}y \end{cases}$$

Si ottiene infatti la seguente curva $d^3y^2 = d^3x^3 + Ad^3x + Bd^3$; a questo punto basterá dividere entrambi i membri per d^3 (lo posso fare in quanto K campo e $d \in K^*$, quindi ammette inverso) per ottenere E^d.

(c) Invece la curva E puó essere trasformata in $dy^2 = x^3 + Ax + B$ con il seguente cambiamento di variabile con coefficienti in K:

$$\begin{cases} x \longmapsto dx \\ y \longmapsto d^2y \end{cases}$$

7. Siano $\alpha, \beta \in \mathbb{Z}$ t.c. $gcd(\alpha, \beta) = 1$, con $\alpha \equiv -1 \ (mod\ 4)$ e $\beta \equiv 0 \ (mod\ 32)$.
Sia E la curva ellittica data da $y^2 = x(x-\alpha)(x-\beta)$.

(a) Si deve dimostrare che $\alpha \equiv 0 \ (mod\ p) \ \Rightarrow \ \beta \not\equiv 0 \ (mod\ p)$.
Se $gcd(\alpha, \beta) = 1 \ \Rightarrow \ \exists a, b \in \mathbb{Z}: \ a\alpha + b\beta = 1$.
Se $\alpha \equiv 0 \ (mod\ p) \ \Rightarrow \ a\alpha + b\beta \equiv b\beta \equiv 1 \ mod\ p \ \Rightarrow \ \beta \not\equiv 0 \ (mod\ p)$.

(b) Applico il cambiamento di variabile indicato:

$$\begin{cases} x = 4x_1 \\ y = 8y_1 + 4x_1 \end{cases}$$

$64y_1^2 + 64x_1y_1 + 16x_1^2 = [4x_1(4x_1 - \alpha)(4x_1 - \beta)]$
$64y_1^2 + 64x_1y_1 + 16x_1^2 = 64x_1^3 - 16x_1^2\beta - 16x_1^2\alpha + 4x_1\alpha\beta$
Dividendo tutto per 64 si ha che:
$y_1^2 + x_1y_1 = x_1^3 - \dfrac{1+\alpha+\beta}{4}x_1^2 + \dfrac{\alpha\beta}{16}x_1$ ossia l'equazione di E_1 che si voleva ottenere.

(c) Poiché $\beta \equiv 0 \ (mod\ 32)$ si ha che $32|\beta$, ossia $\beta = 32t$, con $t \in \mathbb{Z}$.
Inoltre $\alpha \equiv -1 \ (mod\ 4)$, quindi $\alpha = -1 + 4k$, con $k \in \mathbb{Z}$.
L'equazione di E_1 diventa $y_1^2 + x_1y_1 = x_1^3 - \frac{4k-32t}{4}x_1^2 + 2(-1+4k)tx_1$.
Se si riduce questa equazione modulo 2 si ha:

$$y_1^2 + x_1y_1 = x_1^3 - ex_1^2$$

dove $k \equiv e \ (mod\ 2)$.

(d) Sia $r: \ y_1 = \gamma x_1$ con $\gamma = \textit{costante}$. Si vuole calcolare l'ordine di intersezione della retta con la curva ellittica ridotta modulo 2 del punto precedente nell'origine.

$$\begin{cases} y_1 = \gamma x_1 \\ y_1^2 + x_1 y_1 = x_1^3 + e x_1^2 \end{cases} \rightarrow \begin{cases} y_1 = \gamma x_1 \\ \gamma^2 x_1^2 + \gamma x_1^2 = x_1^3 + e x_1^2 \end{cases}$$

$x_1^3 + (e - \gamma^2 - \gamma)x^2 = 0 \ \Rightarrow \ x^2(x + e - \gamma^2 - \gamma) = 0$.
L'ordine d'intersezione in $(0,0)$ risulta quindi essere 3 se $\gamma^2 + \gamma = e$ e 2 se $\gamma^2 + \gamma \neq e$.

(e) Se $e = 0$ ho due radici distinti in $\mathbb{F}_2$ (sia 1, sia 0 risolvono il polinomio). Se $e = 1$ per il teorema fondamentale dell'algebra $\exists$ due radici in $\overline{\mathbb{F}_2}$, quindi mi basta dimostrare che sono distinte facendo vedere che il massimo comune divisore fra il polinomio e la sua derivata é sempre 1. In questo caso $\dfrac{d}{dx}(x^2 + x + 1) = 2x + 1 = 1$, da cui si ricava banalmente che $gcd(x^2 + x + 1, 1) = 1$ e quindi che le due radici sono distinte fra loro.