Esame finale di CR3 - Mercoledì 20 Maggio 2009

NB. Si consegna entro lunedì 25 Maggio alle 9:00AM

a. Sia E una curva ellittica definita su un campo con p elementi e tale che $E(\mathbf{F}_p) = C_{27} \times C_{81}$. Determinare tutti i possibili valori di p e per ciascun valore determinare una curva ellitticha con tale proprietà. Giustificare tutti i passi.

b. Sia $E : y^2 = x^3 + x + 1$. Simulare l'algoritmo di Schoof per calcolare $E(\mathbf{F}_{31})$.

c. Calcolare $\#E(\mathbf{F}_{3^{100}})$ dove $E : y^2 = x^3 + 2x + 1$. Giustificare la risposta.

d. Calcolare l'ordine del punto $(0, 0) \in E(\mathbf{F}_{16})$ dove $E : y^2 + y = x^3 + x$ utilizzando l'algoritmo Baby Step Giant Step. Dedurne l'ordine di $E(\mathbf{F}_{16})$.

f. Sia E una curva definita su un campo finito $\mathbf{F}_q$ e sia E' il suo twist. Dimostrare che $E(\mathbf{F}_q) \times E'(\mathbf{F}_q) \cong E(\mathbf{F}_{q^2})$.

g. Sia $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ un equazione di Weierstrass su un campo e sia α la trasformazione affine definita da $(x, y) \mapsto (u^2x + r, u^3y + su^2x + t)$. Dimostrare che α trasforma l'equazione di Weierstrass in un'altra equazione di Weierstrass. Inoltre se due equazioni di Weierstrass si ottengono l'una dall'altra attraverso una trasformazione affine, allora questa deve avere la forma di α.

h. Sia $\mathbf{F}_q$ un campo finito di caratteristica dispari e siano $a, b \in \mathbf{F}_q$ $a \neq \pm 2b$ e $b \neq 0$ si consideri la curva ellittica di equazione $y^2 = x^3 + ax^2 + b^2x$.

(1) Dimostrare che i punti $(b, b\sqrt{a + 2b})$ e $(-b, -b\sqrt{a - 2b})$ hanno ordine 4.

(2) Dimostrare che almeno uno tra $a + 2b, a - 2b$ e $a^2 - 4b^2$ è un quadrato un $\mathbf{F}_q$.

(3) Dimostrare che se $a^2 - 4b^2$ è un quadrato in $\mathbf{F}_q$, allora $E[2] \subseteq E(\mathbf{F}_q)$.

(4) Mostrare che $\#E(\mathbf{F}_q)$ è un multiplo di 4.

(5) Sia E' la curva ellitticha definita da $y^2 = x^3 - 2ax^2 + (a^2 - 4b^2)x$.

Mostrare che $E'[2] \subseteq E'(\mathbf{F}_q)$ e dedurre che anche $\#E'(\mathbf{F}_q)$ è un multiplo di 4.

i. Produrre vari esempi di interi $m, n \in \mathbf{N}$ tali che non esiste alcun campo finito $\mathbf{F}_q$ per il quale esiste una curva ellittica $E/\mathbf{F}_q$ tale che $E(\mathbf{F}_q) \cong C_m \times C_{mn}$.

j. Si consideri l'equazione proiettiva della curva ellittica E: $F(x, y, z) = y^2z - x^3 - Axz^2 - Bz^3 = 0$. Dimostrare che un punto P su E appartiene a $E[3]$ se e solo se

$$\det \begin{pmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ F_{zx} & F_{zy} & F_{zz} \end{pmatrix} = 0$$

nel punto P, where F_{ab} denota la derivata parziale seconda rispetto a a e b. Il determinante si chiama Hessiano. I punti della curva che annullano l'Hessiano si chiamano flessi.