Università degli Studi Roma Tre
Corso di Laurea in Matematica, A.A. 2002/2003
Soluzione del II Esonero di CR1 - Crittografia 1
A cura di Andrea Susa

1. Definire il concetto di curva ellittica su un campo finito ed il gruppo di Mordell-Weyll associato.

2. Consideriamo la curva $y^2 = x^3 + x + 6$ sul campo F_7. Descrivere $\mathcal{E}(F_7)$.
Soluzione
Per prima cosa verifichiamo che la curva ellittica sia ben definita, cioè valga la relazione:

$$4a^3 + 27b^2 \not\equiv 0 \qquad (\text{mod } 7).$$

Nel nostro caso:

$$4 + 27(-1)^2 \equiv 5 \not\equiv 0 \qquad (\text{mod } 7).$$

Determiniamo i punti finiti di $\mathcal{E}(\mathbb{F}_7)$:

x	$x^3 + x + 6 \pmod 7$	RQ	y
0	6	no	
1	1	si	± 1
2	2	si	± 3
3	1	si	± 1
4	4	si	± 2
5	3	no	
6	4	si	± 2

Quindi $\mathcal{E}(\mathbb{F}_7) \simeq \mathbb{F}_{11}$.
3. Descrivere l'algoritmo dello scambio delle chiavi di Diffie-Helmann sulle curve ellittiche.

4. Sia g una radice primitiva di F_p. Dimostrare le seguenti proprietà del logaritmo discreto:

$$\begin{aligned} \log_g(a \cdot b) &= \log_g(a) + \log_g(b), && (\text{mod } p-1) \\ \log_g(a^n) &= n \log_g(a) && (\text{mod } p-1). \end{aligned}$$

Soluzione
Siano $g^r = a$, $g^s = b$, $g^n = ab$. Quindi $\log_g(ab) = n$. Ma

$$g^n = ab = (g^r)(g^s) = g^{r+s} \quad \Longrightarrow \quad n \equiv r + s \pmod{p-1}.$$

Allora:

$$\log_g(ab) = n \equiv r + s = log_g(a) + \log_g(b) \qquad (\text{mod } p-1).$$

Per induzione su n:
se $n = 2$ per la precedente $\log_g(a^2) = \log_g(a) + \log_g(a) = 2\log_g(a)$.
Per ipotesi induttiva $\log_g(a^{n-1}) = (n-1)\log_g(a)$.
Allora se $n \geq 3$, $\log_g(a^n) = \log_g(a) + \log_g(a^{n-1}) = n\log_g(a)$.

5. Consideriamo il campo base F_5. Determinare il numero dei polinomi monici irriducibili di grado 12. Qual è la probabilità che, preso random un polinomio monico di grado 12, esso sia irriducibile?

Soluzione
Dobbiamo calcolare:

$$5^{12} = \sum_{d|12} dN_d(5).$$

Abbiamo che:

$$N_1(5) = 5, \qquad N_2(5) = 10, \qquad N_3(5) = 40$$

Mentre:

$$N_4(5) = \frac{1}{4}\left(5^4 - N_1(5) - 2N_2(5)\right) = 150$$

$$N_6(5) = \frac{1}{6}\left(5^6 - N_1(5) - 2N_2(5) - 3N_3(5)\right) = 2580$$

Quindi:

$$\begin{aligned} N_{12}(5) &= \frac{1}{12}(5^{12} - 5 - 20 - 120 - 4 \cdot 150 - 6 \cdot 2580) = \\ &= 20343700. \end{aligned}$$

Calcoliamo la probabilità: se indichiamo con $T_k(p) = p^k$ il numero dei polinomi monici di grado k su $\mathbb{F}_p$, allora

$$\frac{N_{12}(5)}{T_{12}(5)} = \frac{20343700}{5^{12}} = 0.08332$$

6. Consideriamo il polinomio $f = x^3 + x + 1 \in F_5[x]$. Dopo aver verificato che è irriducibile, trovare una radice primitiva per il campo:

$$F_5[x]/(f) \ = \{a + b\theta + c\theta^2 \mid \theta^3 = -\theta - 1\}.$$

Soluzione
Il polinomio è irriducibile in quanto ha grado 3, e quindi se fosse riducibile dovrebbe avere una radice sul campo. Ma si calcola che $f(0) = 1$, $f(\pm 1) = (\pm 1) + (\pm 1) + 1 \neq 0$, $f(\pm 2) = (\pm 8) + (\pm 2) + 1 \neq 0$. Quindi f riducibile.
Sia θ una radice formale. Allora $\theta^2 + 1$ è primitiva.

7. Calcolare il $\log_3(13)$ nel campo $\mathbb{F}_{31}$, utilizzando un qualsiasi metodo.

Soluzione
Utiliziamo l'algortimo di Shanks:
$m = [\sqrt{31}] = 5$. Otteniamo le seguenti liste:

j	0	1	2	3	4
g^{mj}	1	26	25	30	5

i	0	1	2	3	4
$13 \cdot g^{-i}$	13	25	29	20	17

Le coppie sono: $(2, 25)$ e $(1, 25)$. Quindi $\log_3(13) = mj + i = 5 \cdot 2 + 1 = 11$.

8. Dimostrare che il polinomio $x^2 + 1$ è irriducibile su tutti i campi finiti F_p con $p \equiv 3 \pmod 4$.

Soluzione Il polinomio $f = x^2 + 1$ è irriducibile su $\mathbb{F}_p$ se e soltanto se non ha radici su $\mathbb{F}_p$, cioè se $\left(\frac{-1}{p}\right) = -1$. Ma questo accade se e soltanto se $p \equiv 3 \pmod 4$.

9. Si descrivino tutti i valori di $a \in F_p$ per cui il polinomio: $f(x) = x^2 + a$ è irriducibile, e si dimostri che tale polinomio non può mai essere primitivo.
Soluzione f è irriducibile per ogni $a \in F_p$ tale che $\left(\frac{-a}{p}\right) = -1$.
Se per assurdo f fosse primitivo, allora avremmo che la sua radice θ è tale che:

$$ord_p(\theta^2) = ord_p(-a) \leq p - 1.$$

Quindi: $ord_p(\theta) = p^2 - 1 = \frac{1}{2} ord_p(\theta^2) \leq \frac{p-1}{2}$ e questo è assurdo.

10. Mostrare che tutti i polinomi del tipo $x^p + x + 1$ sono riducibili su $\mathbb{F}_p$, per $p \geq 3$.
Soluzione I polinomi del tipo $x^p + x + 1$ hanno sempre una radice sul campo $\mathbb{F}_p$. Infatti $(p-2)^*$, cioè l'inverso aritmetico di $-2 \pmod p$ è sempre soluzione del polinomio:

$$(p - 2^*)^p + (p - 2^*) + 1 \equiv (-2^*) + (-2^*) + 1 \equiv -2 \cdot (2^*) + 1 \equiv 0 \qquad (\text{mod } p).$$

11. Dopo aver scritto tutti i polinomi irriducibili di grado ≤ 4 su F_2, mostrare che il polinomio $f(x) = x^5 + x^2 + 1$ è irriducibile.

Soluzione La seguente tabella mostra tutti i polinomi irriducibili di grado ≤ 4.

$n = 1$	x	$x + 1$	
$n = 2$	$x^2 + x + 1$		
$n = 3$	$x^3 + x^2 + 1$	$x^3 + x + 1$	
$n = 4$	$x^4 + x + 1$	$x^4 + x^3 + 1$	$x^4 + x^3 + x^2 + x + 1$

Si verifica che f non ha radici sul campo, quindi se fosse riducibile dovrebbe essere il prodotto di un polinomio di grado tre con un polinomio di grado due. Ma svolgendo la divisione di f con l'unico polinomio polinomio irriducibile di grado 2 otteniamo:

$$f = (x^2 + x + 1)(x^3 + x^2) + 1$$

quindi f è irriducibile.

12. Descrivere tutti i sottocampi di $F_{5^{30}}$.

Soluzione Esiste un sottocampo per ogni divisore proprio di 30.