TERZA PROVETTA DI ALGEBRA
TRENTO, 27 NOVEMBRE 2015

Nota: Questi fogli contengono gli esercizi delle quattro diverse versioni della provetta che sono state assegnate. L'esercizio $x.y$ è l'esercizio x della versione y.

Esercizio 1.1. Alice e Bob giocano a testa o croce per telefono.

(1) Alice pensa i due numeri primi $p = 23$ e $q = 47$ (che siano primi ve lo diciamo noi, ma dovete verificare che siano entrambi congrui a 3 modulo 4), calcola $N = p \cdot q$, e trasmette N a Bob.
(2) Bob le comunica $b = 72$.
(3) Si mostri come fa Alice a trovare le quattro radici quadrate di b modulo N, e le si trovino effettivamente.
(4) Si spieghi come prosegue il gioco. In particolare, si mostri come fa Bob, se ha vinto, a dimostrare ad Alice di aver vinto, cioè facendo vedere che è in grado di trovare p e q.

Esercizio 1.2. Alice e Bob giocano a testa o croce per telefono.

(1) Alice pensa i due numeri primi $p = 11$ e $q = 103$ (che siano primi ve lo diciamo noi, ma dovete verificare che siano entrambi congrui a 3 modulo 4), calcola $N = p \cdot q$, e trasmette N a Bob.
(2) Bob le comunica $b = 59$.
(3) Si mostri come fa Alice a trovare le quattro radici quadrate di b modulo N, e le si trovino effettivamente.
(4) Si spieghi come prosegue il gioco. In particolare, si mostri come fa Bob, se ha vinto, a dimostrare ad Alice di aver vinto, cioè facendo vedere che è in grado di trovare p e q.

Esercizio 1.3. Alice e Bob giocano a testa o croce per telefono.

(1) Alice pensa i due numeri primi $p = 19$ e $q = 59$ (che siano primi ve lo diciamo noi, ma dovete verificare che siano entrambi congrui a 3 modulo 4), calcola $N = p \cdot q$, e trasmette N a Bob.
(2) Bob le comunica $b = 843$.
(3) Si mostri come fa Alice a trovare le quattro radici quadrate di b modulo N, e le si trovino effettivamente.
(4) Si spieghi come prosegue il gioco. In particolare, si mostri come fa Bob, se ha vinto, a dimostrare ad Alice di aver vinto, cioè facendo vedere che è in grado di trovare p e q.

Esercizio 1.4. Alice e Bob giocano a testa o croce per telefono.

(1) Alice pensa i due numeri primi $p = 31$ e $q = 43$ (che siano primi ve lo diciamo noi, ma dovete verificare che siano entrambi congrui a 3 modulo 4), calcola $N = p \cdot q$, e trasmette N a Bob.

(2) Bob le comunica $b = 317$.
(3) Si mostri come fa Alice a trovare le quattro radici quadrate di b modulo N, e le si trovino effettivamente.
(4) Si spieghi come prosegue il gioco. In particolare, si mostri come fa Bob, se ha vinto, a dimostrare ad Alice di aver vinto, cioè facendo vedere che è in grado di trovare p e q.

Esercizio 2.1. Si consideri $\alpha = \sqrt{2} + \sqrt{5} \in \mathbf{C}$.

(1) Si trovi un polinomio monico $f \in \mathbf{Q}[x]$ di grado 4 di cui α è radice.
(2) Si mostri che $|\mathbf{Q}[\alpha] : \mathbf{Q}| \leq 4$.
(3) Si mostri che $\sqrt{2} \in \mathbf{Q}[\alpha]$.
(4) Si mostri che $K = \mathbf{Q}[\sqrt{2}] \subseteq \mathbf{Q}[\alpha]$.
(5) Si mostri che $\sqrt{5} \in \mathbf{Q}[\alpha]$.
(6) Si mostri che $K[\sqrt{5}] \subseteq \mathbf{Q}[\alpha]$.
(7) Si mostri che $|\mathbf{Q}[\sqrt{2}] : \mathbf{Q}| = 2$.
(8) Si mostri che $|K[\sqrt{5}] : K| = 2$.
(9) Si deduca dai due punti precedenti che $|K[\sqrt{5}] : \mathbf{Q}| = 4$.
(10) Si mostri che $K[\sqrt{5}] = (\mathbf{Q}[\sqrt{2}])[\sqrt{5}] = \mathbf{Q}[\alpha]$.
(11) Si mostri che $|\mathbf{Q}[\alpha] : \mathbf{Q}| = 4$.
(12) Si mostri che f è il polinomio minimo di α su $\mathbf{Q}$.

Esercizio 2.2. Si consideri $\alpha = \sqrt{3} + \sqrt{5} \in \mathbf{C}$.

(1) Si trovi un polinomio monico $f \in \mathbf{Q}[x]$ di grado 4 di cui α è radice.
(2) Si mostri che $|\mathbf{Q}[\alpha] : \mathbf{Q}| \leq 4$.
(3) Si mostri che $\sqrt{3} \in \mathbf{Q}[\alpha]$.
(4) Si mostri che $K = \mathbf{Q}[\sqrt{3}] \subseteq \mathbf{Q}[\alpha]$.
(5) Si mostri che $\sqrt{5} \in \mathbf{Q}[\alpha]$.
(6) Si mostri che $K[\sqrt{5}] \subseteq \mathbf{Q}[\alpha]$.
(7) Si mostri che $|\mathbf{Q}[\sqrt{3}] : \mathbf{Q}| = 2$.
(8) Si mostri che $|K[\sqrt{5}] : K| = 2$.
(9) Si deduca dai due punti precedenti che $|K[\sqrt{5}] : \mathbf{Q}| = 4$.
(10) Si mostri che $K[\sqrt{5}] = (\mathbf{Q}[\sqrt{3}])[\sqrt{5}] = \mathbf{Q}[\alpha]$.
(11) Si mostri che $|\mathbf{Q}[\alpha] : \mathbf{Q}| = 4$.
(12) Si mostri che f è il polinomio minimo di α su $\mathbf{Q}$.

Esercizio 2.3. Si consideri $\alpha = \sqrt{3} + \sqrt{7} \in \mathbf{C}$.

(1) Si trovi un polinomio monico $f \in \mathbf{Q}[x]$ di grado 4 di cui α è radice.
(2) Si mostri che $|\mathbf{Q}[\alpha] : \mathbf{Q}| \leq 4$.
(3) Si mostri che $\sqrt{3} \in \mathbf{Q}[\alpha]$.
(4) Si mostri che $K = \mathbf{Q}[\sqrt{3}] \subseteq \mathbf{Q}[\alpha]$.
(5) Si mostri che $\sqrt{7} \in \mathbf{Q}[\alpha]$.
(6) Si mostri che $K[\sqrt{7}] \subseteq \mathbf{Q}[\alpha]$.
(7) Si mostri che $|\mathbf{Q}[\sqrt{3}] : \mathbf{Q}| = 2$.
(8) Si mostri che $|K[\sqrt{7}] : K| = 2$.
(9) Si deduca dai due punti precedenti che $|K[\sqrt{7}] : \mathbf{Q}| = 4$.

(10) Si mostri che $K[\sqrt{7}] = (\mathbf{Q}[\sqrt{3}])[\sqrt{7}] = \mathbf{Q}[\alpha]$.
(11) Si mostri che $|\mathbf{Q}[\alpha] : \mathbf{Q}| = 4$.
(12) Si mostri che f è il polinomio minimo di α su $\mathbf{Q}$.

Esercizio 2.4. Si consideri $\alpha = \sqrt{5} + \sqrt{7} \in \mathbf{C}$.

(1) Si trovi un polinomio monico $f \in \mathbf{Q}[x]$ di grado 4 di cui α è radice.
(2) Si mostri che $|\mathbf{Q}[\alpha] : \mathbf{Q}| \leq 4$.
(3) Si mostri che $\sqrt{5} \in \mathbf{Q}[\alpha]$.
(4) Si mostri che $K = \mathbf{Q}[\sqrt{5}] \subseteq \mathbf{Q}[\alpha]$.
(5) Si mostri che $\sqrt{7} \in \mathbf{Q}[\alpha]$.
(6) Si mostri che $K[\sqrt{7}] \subseteq \mathbf{Q}[\alpha]$.
(7) Si mostri che $|\mathbf{Q}[\sqrt{5}] : \mathbf{Q}| = 2$.
(8) Si mostri che $|K[\sqrt{7}] : K| = 2$.
(9) Si deduca dai due punti precedenti che $|K[\sqrt{7}] : \mathbf{Q}| = 4$.
(10) Si mostri che $K[\sqrt{7}] = (\mathbf{Q}[\sqrt{5}])[\sqrt{7}] = \mathbf{Q}[\alpha]$.
(11) Si mostri che $|\mathbf{Q}[\alpha] : \mathbf{Q}| = 4$.
(12) Si mostri che f è il polinomio minimo di α su $\mathbf{Q}$.

Esercizio 3.1. Si enunci e si dimostri il teorema della radice razionale.

Esercizio 3.2. Si mostri che un campo ha caratteristica o 0 o un numero primo p.

Esercizio 3.3. Siano $F \subseteq K \subseteq E$ campi, ognuno estensione di quelli più piccoli, e sia $\alpha \in E$, algebrico su F. Si mostri che α è algebrico anche su K, e che se se m_F, m_k sono rispettivamente i polinomi minimi di α su F e su K, allora

$$m_K \mid m_F.$$

Esercizio 3.4. Siano A, B anelli, $f : A \to B$ un morfismo. Si mostri che sono equivalenti:

(1) f è iniettivo, e
(2) $\ker(f) = \{ 0 \}$.

Esercizio 4.1. Sia $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z} = \{ 0, 1, -1 \}$ il campo con 3 elementi.

(1) Si mostri che i polinomi monici e irriducibili di grado 2 in $\mathbf{F}_3[x]$ sono tutti e soli i seguenti:
$$\begin{cases} f_1 = x^2 + x - 1, \\ f_2 = x^2 - x - 1, \\ f_3 = x^2 + 1. \end{cases}$$
(2) Si costruisca un campo $E = \mathbf{F}_3[\alpha]$ con 9 elementi, ove α è radice di f_1.
(3) Si mostri che ogni elemento di E si scrive in modo unico nella forma
$$a_0 + a_1\alpha, \quad \text{per } a_0, a_1 \in \mathbf{F}_3.$$
(4) Si calcolino le potenze di α, costruendo la tabella del logaritmo discreto.
(5) Si trovino in E tutte le radici di f_1, f_2, f_3.

Esercizio 4.2. Sia $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z} = \{ 0, 1, -1 \}$ il campo con 3 elementi.

(1) Si mostri che i polinomi monici e irriducibili di grado 2 in $\mathbf{F}_3[x]$ sono tutti e soli i seguenti:
$$\begin{cases} f_1 = x^2 + x - 1, \\ f_2 = x^2 - x - 1, \\ f_3 = x^2 + 1. \end{cases}$$
(2) Si costruisca un campo $E = \mathbf{F}_3[\alpha]$ con 9 elementi, ove α è radice di f_2.
(3) Si mostri che ogni elemento di E si scrive in modo unico nella forma
$$a_0 + a_1\alpha, \quad \text{per } a_0, a_1 \in \mathbf{F}_3.$$
(4) Si calcolino le potenze di α, costruendo la tabella del logaritmo discreto.
(5) Si trovino in E tutte le radici di f_1, f_2, f_3.

Esercizio 4.3. Sia $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z} = \{\, 0, 1, -1 \,\}$ il campo con 3 elementi.

(1) Si mostri che i polinomi monici e irriducibili di grado 2 in $\mathbf{F}_3[x]$ sono tutti e soli i seguenti:
$$\begin{cases} f_1 = x^2 + x - 1, \\ f_2 = x^2 - x - 1, \\ f_3 = x^2 + 1. \end{cases}$$
(2) Si costruisca un campo $E = \mathbf{F}_3[\alpha]$ con 9 elementi, ove α è radice di f_1.
(3) Si mostri che ogni elemento di E si scrive in modo unico nella forma
$$a_0 + a_1\alpha, \quad \text{per } a_0, a_1 \in \mathbf{F}_3.$$
(4) Si calcolino le potenze di α, costruendo la tabella del logaritmo discreto.
(5) Si trovino in E tutte le radici di f_1, f_2, f_3.

Esercizio 4.4. Sia $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z} = \{\, 0, 1, -1 \,\}$ il campo con 3 elementi.

(1) Si mostri che i polinomi monici e irriducibili di grado 2 in $\mathbf{F}_3[x]$ sono tutti e soli i seguenti:
$$\begin{cases} f_1 = x^2 + x - 1, \\ f_2 = x^2 - x - 1, \\ f_3 = x^2 + 1. \end{cases}$$
(2) Si costruisca un campo $E = \mathbf{F}_3[\alpha]$ con 9 elementi, ove α è radice di f_2.
(3) Si mostri che ogni elemento di E si scrive in modo unico nella forma
$$a_0 + a_1\alpha, \quad \text{per } a_0, a_1 \in \mathbf{F}_3.$$
(4) Si calcolino le potenze di α, costruendo la tabella del logaritmo discreto.
(5) Si trovino in E tutte le radici di f_1, f_2, f_3.

Esercizio 5.1.

(1) Si enunci il Lemma di Eisenstein.
(2) Si mostri che il polinomio
$$x^4 + x^3 + x^2 + x + 1$$
è irriducibile in $\mathbf{Z}[x]$.

Esercizio 5.2.

(1) Si enunci il Lemma di Eisenstein.
(2) Si mostri che il polinomio

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

è irriducibile in $\mathbf{Z}[x]$.

Esercizio 5.3.

(1) Si enunci il Lemma di Eisenstein.
(2) Si mostri che il polinomio

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

è irriducibile in $\mathbf{Z}[x]$.

Esercizio 5.4.

(1) Si enunci il Lemma di Eisenstein.
(2) Si mostri che il polinomio

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

è irriducibile in $\mathbf{Z}[x]$.