SECONDA PROVETTA DI ALGEBRA
TRENTO, 6 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.

(1) Sia B un anello commutativo con unità, estensione dell'anello A, e sia $\alpha \in B$. Si definisca $A[\alpha]$.

(2) Si dimostri il

Lemma. *Sia* $\alpha \in \mathbf{C}$ *con la proprietà che*

(a) $\alpha \notin \mathbf{Q}$, *e*

(b) α *è radice di un polinomio* $x^2 + c_1 x + c_0 \in \mathbf{Z}[x]$.

Allora vale che $\mathbf{Z}[\alpha] = \{ a_0 + a_1\alpha : a_0, a_1 \in \mathbf{Z} \}$, *e la scrittura degli elementi di* $\mathbf{Z}[\alpha]$ *nella forma* $a_0 + a_1\alpha$ *è unica.*

Esercizio 1.2. Sia F un campo. Si mostri che se $I \neq \{ 0 \}$ è un ideale dell'anello dei polinomi $F[x]$, allora

$$I = (f) = \{ fz : z \in F[x] \},$$

ove $f \neq 0$ è un polinomio di grado minimo fra gli elementi di I.

Esercizio 1.3.

(1) Sia B un anello commutativo con unità, estensione dell'anello A, e sia $\alpha \in B$. Si definisca $A[\alpha]$.

(2) Si dimostri il

Lemma. *Sia* $\alpha \in \mathbf{C}$ *con la proprietà che*

(a) $\alpha \notin \mathbf{Q}$, *e*

(b) α *è radice di un polinomio* $x^2 + c_1 x + c_0 \in \mathbf{Z}[x]$.

Allora vale che $\mathbf{Z}[\alpha] = \{ a_0 + a_1\alpha : a_0, a_1 \in \mathbf{Z} \}$, *e la scrittura degli elementi di* $\mathbf{Z}[\alpha]$ *nella forma* $a_0 + a_1\alpha$ *è unica.*

Esercizio 1.4. Sia F un campo. Si mostri che se $I \neq \{ 0 \}$ è un ideale dell'anello dei polinomi $F[x]$, allora

$$I = (f) = \{ fz : z \in F[x] \},$$

ove $f \neq 0$ è un polinomio di grado minimo fra gli elementi di I.

Esercizio 2.1. Si mostri che $\sqrt{3} \notin \mathbf{Q}$.

Esercizio 2.2. Si mostri che $\sqrt{5} \notin \mathbf{Q}$.

Esercizio 2.3. Si mostri che $\sqrt{7} \notin \mathbf{Q}$.

Esercizio 2.4. Si mostri che $\sqrt{11} \notin \mathbf{Q}$.

Esercizio 3.1. Si consideri il seguente schema RSA.

Alice pensa i numeri primi $p = 17$ e $q = 53$, e calcola $n = pq$. Fatelo anche voi.

Notate che $26^2 \leq n < 26^3$, dunque con questo n si possono cifrare coppie di lettere, e così faremo nel seguito. Ogni lettera viene prima trasformata in un numero p_i fra 0 e 25, secondo lo schema $A \mapsto 0$, $B \mapsto 1$, $\dots Z \mapsto 25$, e poi di ogni coppia di lettere si fa un unico numero compreso fra 0 e n: spiegate come.

Alice calcola $\varphi(n)$ (fatelo anche voi, spiegando come fate), e sceglie $r = 119$. Verificate che sia $(r, \varphi(n)) = 1$, e calcolate s, t tali che $rs + \varphi(n)t = 1$.

Alice comunica r, n a Bob, che dopo un po' le manda il messaggio

$$[730, 708, 637].$$

Decifratelo.

Esercizio 3.2. Si consideri il seguente schema RSA.

Alice pensa i numeri primi $p = 19$ e $q = 53$, e calcola $n = pq$. Fatelo anche voi.

Notate che $26^2 \leq n < 26^3$, dunque con questo n si possono cifrare coppie di lettere, e così faremo nel seguito. Ogni lettera viene prima trasformata in un numero p_i fra 0 e 25, secondo lo schema $A \mapsto 0$, $B \mapsto 1$, $\dots Z \mapsto 25$, e poi di ogni coppia di lettere si fa un unico numero compreso fra 0 e n: spiegate come.

Alice calcola $\varphi(n)$ (fatelo anche voi, spiegando come fate), e sceglie $r = 535$. Verificate che sia $(r, \varphi(n)) = 1$, e calcolate s, t tali che $rs + \varphi(n)t = 1$.

Alice comunica r, n a Bob, che dopo un po' le manda il messaggio

$$[97, 152, 861].$$

Decifratelo.

Esercizio 3.3. Si consideri il seguente schema RSA.

Alice pensa i numeri primi $p = 11$ e $q = 83$, e calcola $n = pq$. Fatelo anche voi.

Notate che $26^2 \leq n < 26^3$, dunque con questo n si possono cifrare coppie di lettere, e così faremo nel seguito. Ogni lettera viene prima trasformata in un numero p_i fra 0 e 25, secondo lo schema $A \mapsto 0$, $B \mapsto 1$, $\dots Z \mapsto 25$, e poi di ogni coppia di lettere si fa un unico numero compreso fra 0 e n: spiegate come.

Alice calcola $\varphi(n)$ (fatelo anche voi, spiegando come fate), e sceglie $r = 703$. Verificate che sia $(r, \varphi(n)) = 1$, e calcolate s, t tali che $rs + \varphi(n)t = 1$.

Alice comunica r, n a Bob, che dopo un po' le manda il messaggio

$$[477, 842, 783].$$

Decifratelo.

Esercizio 3.4. Si consideri il seguente schema RSA.

Alice pensa i numeri primi $p = 23$ e $q = 41$, e calcola $n = pq$. Fatelo anche voi.

Notate che $26^2 \leq n < 26^3$, dunque con questo n si possono cifrare coppie di lettere, e così faremo nel seguito. Ogni lettera viene prima trasformata in un numero p_i fra 0 e 25, secondo lo schema $A \mapsto 0$, $B \mapsto 1$, $\dots Z \mapsto 25$, e poi di ogni coppia di lettere si fa un unico numero compreso fra 0 e n: spiegate come.

Alice calcola $\varphi(n)$ (fatelo anche voi, spiegando come fate), e sceglie $r = 503$. Verificate che sia $(r, \varphi(n)) = 1$, e calcolate s, t tali che $rs + \varphi(n)t = 1$.

Alice comunica r, n a Bob, che dopo un po' le manda il messaggio

$$[314, 426, 355].$$

Decifratelo.

Esercizio 4.1. Si dia la definizione di elementi primi e irriducibili in un dominio.

Partendo dall'eguaglianza

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}),$$

si mostri che $1 + \sqrt{-5}$ è irriducibile, ma non primo, in $\mathbf{Z}[\sqrt{-5}]$.

Si mostri che 6 e $2 \cdot (1 + \sqrt{-5})$ non hanno un massimo comun divisore in $\mathbf{Z}[\sqrt{-5}]$.

Esercizio 4.2. Si dia la definizione di elementi primi e irriducibili in un dominio.

Partendo dall'eguaglianza

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}),$$

si mostri che $1 - \sqrt{-5}$ è irriducibile, ma non primo, in $\mathbf{Z}[\sqrt{-5}]$.

Si mostri che 6 e $2 \cdot (1 - \sqrt{-5})$ non hanno un massimo comun divisore in $\mathbf{Z}[\sqrt{-5}]$.

Esercizio 4.3. Si dia la definizione di elementi primi e irriducibili in un dominio.

Partendo dall'eguaglianza

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}),$$

si mostri che 3 è irriducibile, ma non primo, in $\mathbf{Z}[\sqrt{-5}]$.

Si mostri che 6 e $3 \cdot (1 + \sqrt{-5})$ non hanno un massimo comun divisore in $\mathbf{Z}[\sqrt{-5}]$.

Esercizio 4.4. Si dia la definizione di elementi primi e irriducibili in un dominio.

Partendo dall'eguaglianza

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}),$$

si mostri che 2 è irriducibile, ma non primo, in $\mathbf{Z}[\sqrt{-5}]$.

Si mostri che 6 e $3 \cdot (1 - \sqrt{-5})$ non hanno un massimo comun divisore in $\mathbf{Z}[\sqrt{-5}]$.

Esercizio 5.1. Si scriva il numero primo 449 come somma di due quadrati.
(**Attenzione!** Si usi l'algoritmo esposto a lezione, illustrandone i passaggi.)

Esercizio 5.2. Si scriva il numero primo 281 come somma di due quadrati.
(**Attenzione!** Si usi l'algoritmo esposto a lezione, illustrandone i passaggi.)

Esercizio 5.3. Si scriva il numero primo 137 come somma di due quadrati.
(**Attenzione!** Si usi l'algoritmo esposto a lezione, illustrandone i passaggi.)

Esercizio 5.4. Si scriva il numero primo 113 come somma di due quadrati.
(**Attenzione!** Si usi l'algoritmo esposto a lezione, illustrandone i passaggi.)

Esercizio 6.1.
(1) Sia F un campo, $a \in F[x]$. Si mostri che sono equivalenti:
  (a) a è una unità in $F[x]$;
  (b) $\text{grado}(a) = 0$;
  (c) a è una costante non nulla, cioè $a \in F^*$.
(2) Questo risultato vale ancora se al posto di un campo prendiamo $\mathbf{Z}$?

Esercizio 6.2.
(1) Sia F un campo, $a \in F[x]$. Si mostri che sono equivalenti:
  (a) a è una unità in $F[x]$;
  (b) $\text{grado}(a) = 0$;
  (c) a è una costante non nulla, cioè $a \in F^*$.
(2) Questo risultato vale ancora se al posto di un campo prendiamo $\mathbf{Z}$?

Esercizio 6.3.
(1) Sia F un campo, $a \in F[x]$. Si mostri che sono equivalenti:
  (a) a è una unità in $F[x]$;
  (b) $\text{grado}(a) = 0$;
  (c) a è una costante non nulla, cioè $a \in F^*$.
(2) Questo risultato vale ancora se al posto di un campo prendiamo $\mathbf{Z}$?

Esercizio 6.4.
(1) Sia F un campo, $a \in F[x]$. Si mostri che sono equivalenti:
  (a) a è una unità in $F[x]$;
  (b) $\text{grado}(a) = 0$;
  (c) a è una costante non nulla, cioè $a \in F^*$.
(2) Questo risultato vale ancora se al posto di un campo prendiamo $\mathbf{Z}$?

Esercizio 7.1. Sia F un campo. Si mostri che se $I \neq \{ 0 \}$ è un ideale dell'anello dei polinomi $F[x]$, allora

$$I = (f) = \{ fz : z \in F[x] \},$$

ove $f \neq 0$ è un polinomio di grado minimo fra gli elementi di I.

Esercizio 7.2.
(1) Sia B un anello commutativo con unità, estensione dell'anello A, e sia $\alpha \in B$. Si definisca $A[\alpha]$.

(2) Si dimostri il

Lemma. *Sia* $\alpha \in \mathbf{C}$ *con la proprietà che*
(a) $\alpha \notin \mathbf{Q}$, *e*
(b) α *è radice di un polinomio* $x^2 + c_1 x + c_0 \in \mathbf{Z}[x]$.
Allora vale che $\mathbf{Z}[\alpha] = \{ a_0 + a_1\alpha : a_0, a_1 \in \mathbf{Z} \}$, *e la scrittura degli elementi di* $\mathbf{Z}[\alpha]$ *nella forma* $a_0 + a_1\alpha$ *è unica.*

Esercizio 7.3. Sia F un campo. Si mostri che se $I \neq \{ 0 \}$ è un ideale dell'anello dei polinomi $F[x]$, allora

$$I = (f) = \{ fz : z \in F[x] \},$$

ove $f \neq 0$ è un polinomio di grado minimo fra gli elementi di I.

Esercizio 7.4.

(1) Sia B un anello commutativo con unità, estensione dell'anello A, e sia $\alpha \in B$. Si definisca $A[\alpha]$.
(2) Si dimostri il

Lemma. *Sia* $\alpha \in \mathbf{C}$ *con la proprietà che*
(a) $\alpha \notin \mathbf{Q}$, *e*
(b) α *è radice di un polinomio* $x^2 + c_1 x + c_0 \in \mathbf{Z}[x]$.
Allora vale che $\mathbf{Z}[\alpha] = \{ a_0 + a_1\alpha : a_0, a_1 \in \mathbf{Z} \}$, *e la scrittura degli elementi di* $\mathbf{Z}[\alpha]$ *nella forma* $a_0 + a_1\alpha$ *è unica.*

Esercizio 8.1.

(1) Si dia la definizione di dominio euclideo.
(2) Si mostri che la norma di un dominio euclideo è speciale.

Esercizio 8.2.

(1) Si dia la definizione di dominio euclideo.
(2) Si mostri che in un dominio euclideo gli irriducibili sono primi.

Esercizio 8.3.

(1) Si dia la definizione di dominio euclideo.
(2) Si mostri che la norma di un dominio euclideo è speciale.

Esercizio 8.4.

(1) Si dia la definizione di dominio euclideo.
(2) Si mostri che in un dominio euclideo gli irriducibili sono primi.

Esercizio 9.1. Sia A un dominio dotato di una norma speciale. Si mostri che ogni elemento diverso da zero di A si scrive come prodotto di irriducibili.

Esercizio 9.2. Sia A un dominio in cui gli irriducibili sono primi. Si mostri che se i p_i, q_i sono irriducibili, e

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_m,$$

allora $n = m$, e a meno di riordinare i q_i, si ha che p_i è associato a q_i per ogni i.

Esercizio 9.3. Sia A un dominio dotato di una norma speciale. Si mostri che ogni elemento diverso da zero di A si scrive come prodotto di irriducibili.

Esercizio 9.4. Sia A un dominio in cui gli irriducibili sono primi. Si mostri che se i p_i, q_i sono irriducibili, e

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_m,$$

allora $n = m$, e a meno di riordinare i q_i, si ha che p_i è associato a q_i per ogni i.