TRENTO, A.A. 2019/20
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 13

Esercizio 13.1.

(1) Si mostri che gli interi di Gauss sono un dominio euclideo.
(2) Si trovi il MCD fra 4 e $3 + 5i$ negli interi di Gauss.
(3) Si elenchino le unità degli interi di Gauss.
(4) Si trovi la decomposizione di 2 come prodotto di irriducibili negli interi di Gauss.
(5) Si mostri che se un primo dispari è somma di due quadrati, allora è congruo a 1 modulo 4.
(6) Si mostri che gli interi che sono primi e congrui a 3 modulo 4 sono irriducibili negli interi di Gauss.

Esercizio 13.2. Si enunci e si dimostri il lemma dei cassetti generalizzato.

Esercizio 13.3. Sia p un numero primo *dispari*, e scriviamo

$$F = \mathbf{Z}/p\mathbf{Z} = \{ 0, 1, \dots, p-1 \} .$$

(1) Si mostri che se $a \in F^\star$, allora $a \neq -a$.
(2) Si mostri che l'insieme dei quadrati non nulli

$$Q = \left\{ a^2 : a \in F^\star \right\}$$

ha

$$\frac{p-1}{2}$$

elementi.

(3) Si mostri che Q è l'insieme delle radici del polinomio

$$x^{(p-1)/2} - 1 \in F[x].$$

(4) Si mostri che se $a \in F^\star$, allora

$$a^{(p-1)/2} = \begin{cases} 1 & \text{se } a \text{ è un quadrato in } F, \text{ dunque } a \in Q \\ -1 & \text{se } a \text{ non è un quadrato in } F, \text{ dunque } a \notin Q. \end{cases}$$

Attenzione! Si ha intanto che $a^{(p-1)/2} \in \{ 1, -1 \}$, perchè $(a^{(p-1)/2})^2 = a^{p-1} = 1$ per Eulero-Fermat, e dunque $a^{(p-1)/2}$ è una radice del polinomio $x^2 - 1$. Dunque abbiamo di fronte due "se e solo se", nel senso che se a è un quadrato, allora $a^{(p-1)/2} = 1$, ma d'altra parte se $a^{(p-1)/2} = 1$, a non può essere un non quadrato, altrimenti sarebbe $a^{(p-1)/2} = 1 \neq -1$.

Esercizio 13.4. Sia $p \in \mathbf{N}^\star$ un primo dispari con $p \equiv 1 \pmod 4$. Sia $F = \mathbf{Z}/p\mathbf{Z}$.

(1) Si verifichi che -1 è un quadrato modulo p.
(2) Si mostri che, se c è una radice quadrata modulo p, allora $-c$ è un'altra radice quadrata e $c \neq -c$.
(3) Sia $B = \{1, -1, c, -c\}$. Si dimostri che, per ogni $a \in F^*$, si ha

$$a^{\frac{p-1}{4}} \in B$$

(4) Si consideri la funzione

$$\begin{aligned} f : F^\star &\to B \\ x &\mapsto x^{\frac{p-1}{4}} \end{aligned}$$

Si dimostri che

$$|f^{-1}(b)| = \frac{p-1}{4}$$

per ogni $b \in B$.

Esercizio 13.5. Con l'algoritmo visto a lezione, si scrivano come somma di due quadrati alcuni dei seguenti numeri primi.

$$29, 41, 53, 89, 97, 433.$$

(Fate in particolare almeno uno fra 89 e 433, che richiedono più di una divisione con resto.)

E se vi avessi chiesto di scrivere come somma di due quadrati il numero primo

$$10751759?$$

Esercizio 13.6. Sia p un primo, $p \equiv 1 \pmod 8$. Si mostri che se per un certo $c \in \mathbf{Z}/p\mathbf{Z}^\star$ si ha

$$c^{\frac{p-1}{4}} = -1,$$

allora

$$c^{\frac{p-1}{8}}$$

è una radice quadrata di -1.

Esercizio 13.7. Sia $a + ib \in \mathbf{Z}[i]$. Si mostri che sono equivalenti

(1) $1 + i \mid a + ib$, e
(2) a e b hanno la stessa parità.

(Suggerimento: $1 + i \mid a + ib$ se e solo se esiste $x + iy \in \mathbf{Z}[i]$ tale che $a + ib = (1 + i)(x + iy) = x - y + i(x + y)$, ovvero il sistema diofanteo

$$\begin{cases} x - y = a \\ x + y = b \end{cases} \tag{1}$$

ha soluzioni $x, y \in \mathbf{Z}$. Se il sistema ha soluzione, allora sommando le due equazioni si ha $2x = a + b$ (e $2y = -a + b$), ovvero a e b hanno la stessa parità. Se viceversa a e b hanno la stessa parità, allora $a + b$ e $a - b$ sono pari, e dunque

$$\begin{cases} x = \dfrac{a+b}{2} \\ y = \dfrac{-a+b}{2} \end{cases}$$

è una soluzione intera del sistema (1).)

Esercizio 13.8. Si enunci e si dimostri la formula per le terne pitagoriche primitive.

Esercizio 13.9 (In realtà già svolto). Sia A un UFD, $a \in A$ un elemento che non sia né zero, né una unità.

Dunque si può scrivere a come prodotto di irriducibili q_i:

$$a = q_1 \cdots q_n.$$

Alcuni dei q_i potrebbero essere associati fra loro. Per fare un esempio semplice, potrebbe essere $a = q_1 q_2$, con $q_2 = \varepsilon q_1$, ove ε è una unità. Allora possiamo scrivere $a = \varepsilon q_1^2$. Questo per esempio è il caso quando $A = \mathbf{Z}$ e $a = -4$, allora $-4 = 2 \cdot (-2) = (-1) \cdot 2^2$.

In generale, si capisce che posso scrivere

$$a = \varepsilon p_1^{e_1} \cdots p_k^{e_k}, \tag{2}$$

con ε una unità, p_1 irriducibili, con $p_i \not\sim p_j$ per $i \neq j$, e $e_i > 0$. Ad esempio in $A = \mathbf{Z}$ posso scrivere $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$.

Notate che la formula (2) copre anche il caso in cui a sia una unità, con $k = 0$.

Esercizio 13.10 (facoltativo). Si mostri che in un UFD esistono MCD e mcm.

(Suggerimento: Ci appelliamo alle formule che avevamo imparato a scuola. Siano $a, b \in A$, entrambi diversi da zero. Scriviamo

$$a = \varepsilon p_1^{e_1} \cdots p_k^{e_k}, \quad b = \varepsilon p_1^{f_1} \cdots p_k^{f_k}, \tag{3}$$

ove i p_i sono primi, p_i non è associato a p_j, per $i \neq j$, e $e_i, f_i \geq 0$. Allora si vede che

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} \cdots p_k^{\min(e_k, f_k)},$$

e

$$\operatorname{lcm}(a, b) = p_1^{\max(e_1, f_1)} \cdots p_k^{\max(e_k, f_k)}.$$

Ne segue anche che $\gcd(a, b) \cdot \operatorname{lcm}(a, b) \sim ab$.)

Esercizio 13.11 (facoltativo). Sia A un UFD, $a \in A$ un elemento che non sia né zero, né una unità.

Sia $a^2 = bc$ con $\gcd(b, c) = 1$.

Si mostri che $b = \sigma b_1^2$, $c = \tau c_1^2$, con $b_1, c_1 \in A$, e σ, τ unità.

(Suggerimento: Nella notazione di (2), si ha

$$a^2 = \varepsilon^2 p_1^{2e_1} \cdots p_k^{2e_k}, \tag{4}$$

dove gli esponenti dei p_i sono tutti pari. Se viceversa

$$a = \eta p_1^{2e_1} \cdots p_k^{2e_k},$$

con gli esponenti dei p_i pari, e η una unità, allora

$$a = \eta (p_1^{e_1} \cdots p_k^{e_k})^2.$$

Abbiamo ottenuto

Lemma. Sono equivalenti, per a come in (2)

(1) $a = \zeta b^2$, per qualche $b \in A$, e una unità ζ, e

(2) tutti gli esponenti e_i sono pari.

Siano ora $b, c \in A$ tali che $\gcd(b, c) = 1$ e

$$a^2 = bc.$$

Se a^2 è come in (4), prendiamo ad esempio p_1. Si ha che $p_1 \mid a^2 = bc$, dunque p_1 divide o b o c, dato che in un UFD gli irriducibili sono primi. Ma p_1 non può dividere sia b che c, che sono coprimi. Quindi nella fattorizzazione di b, diciamo, compare l'intera potenza $p_1^{2e_1}$. Lo stesso vale per tutti i p_i. Ne segue, per il Lemma, che $b = \sigma b_1^2$, $c = \tau c_1^2$, con $b_1, c_1 \in A$, e σ, τ unità.)