TRENTO, A.A. 2021/22
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 14

Attenzione! Notazione! Nel seguito scrivo $a \sim b$ per dire che a e b sono associati, cioè $a \mid b$ e $b \mid a$.

Esercizio 14.1.

(1) Sia p un primo. Si mostri che scegliendo $a \not\equiv 0 \pmod{p}$ casualmente, metà delle volte si avrà
$$a^{(p-1)/2} \equiv -1 \pmod{p}.$$

(2) Si mostri che se $p \equiv 1 \pmod{4}$ è un primo, scegliendo $a \not\equiv 0 \pmod{p}$ casualmente si avrà metà delle volte
$$\left(a^{(p-1)/4}\right)^2 \equiv -1 \pmod{p},$$
cioè metà delle volte $a^{(p-1)/4}$ è una radice quadrata di -1 in $\mathbf{Z}/p\mathbf{Z}$.

Esercizio 14.2. Con l'algoritmo visto a lezione, si scrivano come somma di due quadrati alcuni dei seguenti numeri primi, spiegando i vari passaggi (cioè descrivendo l'algoritmo per scrivere un numero primo congruo a $1 \pmod{4}$ come somma di due quadrati mentre lo si usa).
$$29, 41, 53, 89, 97, 433.$$
(Fate in particolare almeno uno fra 89 e 433, che richiedono più di una divisione con resto.)

Esercizio 14.3 (Assolutamente facoltativo). 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 14.4 (Pure facoltativo). 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 14.5 (Facoltativo, ma utile da sapere). 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 $e_i, f_i \geq 0$. 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 14.6 (Assolutamente 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: Per lo svolgimento, vedete gli appunti del corso, Lemma 7.12.6 e risultati immediatamente precedenti..)

Esercizio 14.7. Si enunci e si dimostri la formula per le terne pitagoriche primitive.