Algebra A: Prova 2

UNOFFICIAL

1. Sia R un anello commutativo con unità 1 e sia $I \subset R$ un ideale. Dimostrare che I è massimale se e solo se R/I è un campo.

2. Consideriamo un sistema RSA con chiave pubblica $(13, 209)$.

   (a) Calcolare la chiave privata.

   (b) Calcolare l'unico intero a tale che $0 \leq a < 209$ e $a \equiv 18^{13} \mod 209$, usando l'esponenziazione veloce (metodo dei quadrati ripetuti) e calcoli mod 11, mod 19 e il teorema cinese dei resti.

   (c) Enumeriamo le lettere A-Z da 0 a 25. Si scrive ogni intero tra 0 e 91 come $a_0 + 26a_1$ con $0 \leq a_i \leq 25$. Così ogni lettera viene criptata con due lettere. Criptare la lettera S.

3. Sia $f : \mathbb{Z}[i] \to \mathbb{Z}/29\mathbb{Z}$ definita da $f(a + bi) = [a - 12b]_{29}$. Sia $I = \langle 5 - 2i \rangle$ l'ideale di $\mathbb{Z}[i]$ generato da $5 - 2i$.

   (a) Dimostrare che f è un omomorfismo suriettivo di anelli.

   (b) Dimostrare che 29, $12 + i$ stanno in I.

   (c) Dimostrare che il nucleo di f è I. (Suggerimento: per una direzione osservare che $a + bi = a - 12b + (12 + i)b$.)

   (d) Dimostrare che $\mathbb{Z}[i]/I$ è isomorfo a $\mathbb{Z}/29\mathbb{Z}$.

   (e) Dimostrare che I è massimale.

Algebra A: Prova 2 - Soluzioni

1. Si veda la dimostrazione della proposizione 2.6.23 a pagina 43 delle note.

2. (a) Si ha che $209 = 11 \cdot 19$, quindi $\varphi(209) = 10 \cdot 18 = 180$. Ora applichiamo l'algoritmo di Euclide esteso per determinare due interi s, t tali che $180s + 13t = 1$. Si ha quindi

$$\begin{array}{rcrcr} 180 & = & 180 & + & 0 \\ 13 & = & 0 & + & 13 \\ 11 & = & 180 & + & (-13) \cdot 13 \\ 2 & = & (-1) \cdot 180 & + & (14) \cdot 13 \\ 1 & = & (6) \cdot 180 & + & (-83) \cdot 13 \end{array}$$

ovvero che $-83 \cdot 13 \equiv 97 \cdot 13 \equiv 1 \mod 180$, quindi possiamo affermare che la chiave privata è $(97, 209)$.

(b) Scomponendo 13 come somma di potenze di 2 otteniamo $13 = 8 + 4 + 1$, quindi calcoliamo 18^8, 18^4 e 18^1:

$$\begin{array}{lll|lll} 18 \equiv 7 & \mod 11 & & 18 \equiv -1 & \mod 19 \\ 18^2 \equiv 49 \equiv 5 & \mod 11 & & 18^2 \equiv 1 & \mod 19 \\ 18^4 \equiv 25 \equiv 3 & \mod 11 & & 18^4 \equiv 1 & \mod 19 \\ 18^8 \equiv 9 & \mod 11 & & 18^8 \equiv 1 & \mod 19 \end{array}$$

$$\rightsquigarrow \begin{array}{ll} 18^{13} = 18^8 \cdot 18^4 \cdot 18 \equiv 9 \cdot 3 \cdot 7 \equiv 21 \cdot 9 \equiv -9 \equiv 2 & \mod 11 \\ 18^{13} = 18^8 \cdot 18^4 \cdot 18 \equiv -1 \cdot 1 \cdot 1 \equiv -1 \equiv 18 & \mod 19 \end{array}$$

Ora risolviamo il sistema di congruenze

$$\begin{cases} x \equiv 2 & \mod 11 \\ x \equiv 18 & \mod 19 \end{cases} \rightsquigarrow x = 18 + 19\lambda$$

$$\rightsquigarrow 19\lambda \equiv 2 - 18 \equiv 6 \mod 11$$

Calcoliamo ora il reciproco di $8 \mod 11$ con l'algoritmo di Euclide esteso:

$$\begin{array}{rcrcr} 11 & = & 11 & + & 0 \\ 8 & = & 0 & + & 8 \\ 3 & = & 11 & + & (-1) \cdot 8 \\ 2 & = & (-2) \cdot 11 & + & (3) \cdot 8 \\ 1 & = & (3) \cdot 11 & + & (-4) \cdot 8 \end{array}$$

da cui $-4 \cdot 8 \equiv 7 \cdot 8 \equiv 1 \mod 11$. Segue quindi che $\lambda \equiv 6 \cdot 7 \equiv 42 \equiv 9 \mod 11$, quindi $x = 18 + 19 \cdot 9 = 189$.

(c) Enumeriamo le lettere come richiesto dall'esercizio e osserviamo che la lettera `S` corrisponde al numero 18. Nel punto precedente abbiamo calcolato $18^{13} \equiv 189$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$\mod 209$ e si ha $189 = 7 + 7 \cdot 26$. Segue quindi che

$$\texttt{S} \mapsto 18 \mapsto 18^{13}18^{13} \equiv 189 \mod 209 \mapsto (7, 7) \mapsto \texttt{HH}$$

da cui la forma criptata del messaggio è `HH`.

3.

(a) Siano $a+ib, c+id \in \mathbb{Z}[i]$, allora

$$f((a+ib)+(c+di)) = f((a+c)+(b+d)i) = [(a+c)-12(b+d)]_{29} = \\ = [a-12b]_{29} + [c-12d]_{29} = f(a+ib) + f(c+id)$$

$$f((a+ib)\cdot(c+di)) = f((ac-bd)+(ad+bc)i) = [(ac-bd)-12(ad+bc)]_{29} = \\ = [a-12b]_{29}\cdot[c-12d]_{29} = f(a+ib)\cdot f(c+id)$$

infatti

$$[a-12b]_{29}\cdot[c-12d]_{29} = [ac-12(ad+bc)+144bd]_{29}$$

e $144 = 29\cdot 4 + 28 \equiv -1 \mod 29$. Di conseguenza f è un omomorfismo di anelli. Per dimostrare che f è suriettivo, sia $[a]_{29} \in \mathbb{Z}/29\mathbb{Z}$. Allora deve esistere $\zeta \in \mathbb{Z}[i]$ tale che $f(\zeta) = [a]_{29}$. Basta ora porre $\zeta = a + 0i$.

(b) Calcoliamo il reciproco di $5-2i$ in $\mathbb{Q}(i)$: $\frac{5+2i}{29}$. Ora

$$\frac{29}{5-2i} = \frac{29(5+2i)}{29} = 5+2i$$

$$\frac{12+i}{5-2i} = \frac{(12+i)(5+2i)}{29} = \frac{60+24i+5i-2}{29} = \frac{58+29i}{29} = 2+i$$

di conseguenza $29 = (5-2i)(5+2i)$ e $12+i = (5-2i)(2+i)$, per cui appartengono a I.

(c)
- $I \subseteq \ker f$. Sia $\xi(5-2i) \in I$. Allora

$$f(\xi(5-2i)) = f(\xi)f(5-2i) = [5+24]_{29} = [0]_{29} \implies \xi(5-2i) \in \ker f$$

- Sia $a+ib \in \ker f$. Allora $f(a+ib) = [a-12b]_{29} = [0]_{29}$, da cui $a-12b = 29k$ per qualche $k \in \mathbb{Z}$. Ora

$$a+ib = \underbrace{a-12b}_{\in I} + \underbrace{(12+i)}_{\in I} b$$

di conseguenza, per definizione di ideale, $a+ib \in I$.

(d) Per il primo teorema di isomorfismo, dato che f è un omomorfismo anelli e $I = \ker f$, esiste ed è ben definito un omomorfismo iniettivo $\psi : \mathbb{Z}[i]/I \to \mathbb{Z}/29\mathbb{Z}$ tale che $\psi([\zeta]) = f(\zeta)$. Inoltre, siccome f è suriettivo, ψ è suriettivo. Segue quindi che ψ è un isomorfismo di anelli, ovvero che $\mathbb{Z}[i]/I \cong \mathbb{Z}/29\mathbb{Z}$.

(e) Possiamo procedere in più modi. Un'idea potrebbe essere quella di provare che $\mathbb{Z}[i]/I$ è un campo (in quanto isomorfo a $\mathbb{Z}/29\mathbb{Z}$, che lo è perché 29 è primo), per cui per la Proposizione 2.6.23 (pag. 43) I è massimale. Un altro modo potrebbe essere provare che $5-2i$ è un primo di Gauss, per cui siccome $\mathbb{Z}[i]$ è un Dominio Euclideo, I è massimale (Lemma 2.6.26 pag. 43).