TRENTO, A.A. 2022/23
CORSO DI ALGEBRA B
FOGLIO DI ESERCIZI # 1

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

Alice pensa i due numeri primi $p = 103$ e $q = 127$ (verificare che siano entrambi congrui a 3 modulo 4), calcola $N = p \cdot q$, e trasmette N a Bob.

Bob le comunica $b = 14$. Alice, che qui è generosa, gli consiglia di ripensarci. (Perché?)

Bob si scusa, e le comunica $b = 5167$. Perché stavolta Alice è soddisfatta?

Si mostri come fa Alice a trovare le quattro radici quadrate di b modulo N, e si spieghi come prosegue il gioco.

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

Alice pensa due numeri primi p, q, calcola $N = p \cdot q$, e trasmette $N = 19781$ a Bob. (Non sarebbe difficile per Bob fattorizzare N, ma supponiamo che N sia troppo grande per questo.)

Bob prende il numero $a = 201$, e calcola $b = a^2 \pmod N$ (fatelo).

Ora Alice gli comunica un'altra radice quadrata di b modulo N, cioè $c = 18925$. Bob ha vinto! Si mostri come fa a dimostrarlo ad Alice, che non si fida troppo.

Esercizio 1.3 (Facoltativo). C'è almeno un altro modo di giocare a testa o croce per telefono.

Alice pensa due numeri primi grandi $A \neq B$, in modo che uno sia congruo a 1, e l'altro a 3 modulo 4.

Alice calcola $n = AB$, e lo dice a Bruno.

Bruno, che non ha modo di fattorizzare n, getta la moneta scegliendo una delle due affermazioni seguenti:

(1) il più piccolo fattore primo di n è congruo a 1 modulo 4;
(2) il più grande fattore primo di n è congruo a 1 modulo 4.

Dopo che Bruno ha fatto la sua scelta, Alice gli dice A e B, cosí Bruno controlla se ha vinto, cioè se ha indovinato.

Esercizio 1.4 (Sempre più facoltativo). Ma Alice potrebbe essere tentata di imbrogliare, nel modo seguente.

Alice pensa tre numeri primi grandi p, q, r, in modo che $p < q$, $pq < r$, e che siano

$$\begin{cases} p \equiv 1 \pmod 4 \\ q \equiv 3 \pmod 4 \\ r \equiv 1 \pmod 4 \end{cases}$$

A questo punto Alice trasmette a Bruno $n = pqr$, e gli dice (imbrogliando) che n è il prodotto di due numeri primi A e B, uno congruo a 1, l'altro congruo a 3 modulo 4. Bruno, che non ha modo di fattorizzare n, getta la moneta come sopra, cercando di indovinare se è il più piccolo o il più grande fra i presunti primi A e B che è congruo a 1 modulo 4.

Ma Alice, che come abbiamo visto sta cercando di imbrogliare, ha in mente questo. Se Bruno dice che il più piccolo fattore primo di n è congruo a 1 modulo

4, lei gli dice che i fattori sono $A = pq \equiv 3 \pmod 4$ e $B = r \equiv 1 \pmod 4$. (Per ipotesi, $A = pq < r = B$.) Se invece Bruno le dice che il più grande fattore primo di n è congruo a 1 modulo 4, Alice gli dice che i fattori sono $A = p \equiv 1 \pmod 4$, e $B = qr \equiv 3 \pmod 4$. (Anche qui $A = p < q < qr = B$.) In entrambi i casi sembra che Bruno abbia sbagliato.

Bruno fa meglio a non fidarsi, e dovrebbe controllare che A e B siano veramente primi. Per questo non ha bisogno di fattorizzare A e B, ma gli basta usare un test di primalità.

Magari provate a costruire un esempio.

Esercizio 1.5. Siano Ω, Δ due insiemi non vuoti, e $f : \Omega \to \Delta$ una biezione.

Si mostri che per $\sigma \in S(\Delta)$ si ha, con la composizione **da sinistra a destra**, dunque agiscono prima f, poi σ, poi f^{-1},

$$f \circ \sigma \circ f^{-1} \in S(\Omega).$$

Notate che a priori so solo che $f \circ \sigma \circ f^{-1}$ è una funzione da Ω a Ω, devo far vedere che sia biettiva, e dunque un elemento di $S(\Omega)$.

Mostrate che la funzione

$$\begin{aligned} S(\Delta) &\to S(\Omega) \\ \sigma &\mapsto f \circ \sigma \circ f^{-1} \end{aligned}$$

è un isomorfismo di gruppi.

Esercizio 1.6.

(1) Si descriva l'algoritmo per scrivere una permutazione su $\Omega = \{ 1, 2, \dots, n \}$ come prodotto di cicli disgiunti.
(2) Siano $a_1, \dots, a_k$ interi positivi distinti. Si mostri che
$$(a_1 a_2)(a_1 a_3) \cdots (a_1 a_k) = (a_1 a_2 a_3 \dots a_k)$$
dove il prodotto è la composizione di funzioni.
(3) Si mostri che due cicli disgiunti commutano, cioè che se
$$\sigma = (a_1 a_2 \dots a_s), \tau = (b_1 b_2 \dots b_t)$$
sono due cicli, con
$$\{ a_1, a_2, \dots, a_s \} \cap \{ b_1, b_2, \dots, b_t \} = \emptyset$$
allora $\sigma\tau = \tau\sigma$.
(4) Più in generale, definiamo il *supporto* di una permutazione σ come
$$\operatorname{supp}(\sigma) = \{ x \in \Omega : x\sigma \neq x \}$$
e l'insieme dei *punti fissi* di σ come
$$\operatorname{fix}(\sigma) = \{ x \in \Omega : x\sigma = x \}.$$
Chiaramente $\Omega = \operatorname{supp}(\sigma) \dot\cup \operatorname{fix}(\sigma)$.
   (a) Mostrate che se σ, τ sono due permutazioni, sono equivalenti
      (i) $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \emptyset$,
      (ii) $\operatorname{supp}(\sigma) \subseteq \operatorname{fix}(\tau)$, e
      (iii) $\operatorname{supp}(\tau) \subseteq \operatorname{fix}(\sigma)$.

(b) Mostrate che se valgono le ipotesi del punto precedente, allora $\sigma\tau = \tau\sigma$.

(5) Si scriva come prodotto di cicli disgiunti la permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 19 & 10 & 20 & 14 & 9 & 13 & 2 & 6 & 8 & 1 & 17 & 7 & 3 & 5 & 18 & 15 & 11 & 4 & 12 & 16. \end{pmatrix}$$

(6) Si scriva prima come prodotto di cicli disgiunti, e poi come prodotto di 2-cicli (cioè cicli lunghi 2, che pero in generale non saranno disgiunti) la permutazione

$$(1,2,3,4,5,6)(6,7,8)(1,3,5,7,9,10).$$

Esercizio 1.7 (Il punto (2) è facoltativo).

(1) Mostrate che un ciclo lungo n ha periodo n.

(2) Mostrate che se la permutazione σ è il prodotto di cicli disgiunti $\sigma = \tau_1 \cdots \tau_k$, e t_i ha lunghezza t_i, allora il periodo di σ è il minimo comune multiplo dei t_i.

SUGGERIMENTO:

(a) Notate che dato che i τ_i commutano fra loro, per ogni e si avrà $\sigma^e = \tau_1^e \cdots \tau_k^e$.

(b) Notate anche che se i ϑ_i sono cicli disgiunti, allora $\vartheta_1 \cdots \vartheta_k = 1$ se e solo se ogni $\vartheta_i = 1$.

Esercizio 1.8. Sia $\Omega = \mathbf{Z}/n\mathbf{Z} = \{\, 0, 1, \ldots, n-1 \,\}$.

(1) Per $a, b \in \mathbf{Z}/n\mathbf{Z}$, si definisca la $f_{a,b}$ su Ω data da

$$f_{a,b} : x \mapsto ax + b.$$

(2) Si mostri che $f_{a,b} = f_{c,d}$ se e solo se $a = c$ e $b = d$.

(3) Si mostri che $f_{1,0}$ è la funzione identica su Ω.

(4) Si mostri che l'insieme

$$N = \{\, f_{a,b} : a, b \in \mathbf{Z}/n\mathbf{Z} \,\}$$

è un monoide rispetto alla composizione.

(5) Si mostri che $f_{a,b} = f_{a,0} \circ f_{1,b}$.

(6) Si mostri che $f_{1,b} : x \mapsto x + b$ è sempre invertibile, con inversa $f_{1,-b} : x \mapsto x - b$.

(7) Si mostri che $f_{a,b}$ è invertibile in N se e solo se a è invertibile, e in tal caso

$$f_{a,b}^{-1} = f_{a^{-1},-a^{-1}b}.$$

(8) Il punto precedente è forse più chiaro notando che, dato che $f_{1,b}$ è invertibile, sono equivalenti

(a) $f_{a,0}$ è invertibile, e

(b) $f_{a,b}$ è invertibile,

e se valgono queste condizioni si ha

$$f_{a,b}^{-1} = (f_{a,0} \circ f_{1,b})^{-1} = f_{1,b}^{-1} \circ f_{a,0}^{-1} = f_{1,-b} \circ f_{a^{-1},0}$$

e

$$xf_{1,-b} \circ f_{a^{-1},0} = (x-b)f_{a^{-1},0} = xa^{-1} - ba^{-1}.$$