TRENTO, A.A. 2021/22
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 10

Esercizio 10.1. Sia $B > 1$ un intero. Dimostrate che ogni $a \in \mathbf{N}$ si scrive in modo unico *in base* B, ovvero nella forma

$$a_0 + a_1 B + a_2 B^2 + \dots$$

cone $0 \leq a_i < B$.

Esercizio 10.2. In base $B > 1$, come si scrive B^k, e come si scrive $B^k - 1$?

(Suggerimento: Visto che la scrittura è unica, B^k si scrive come $0 + 0 \cdot B + 0 \cdot B^2 + \dots + 1 \cdot B^k$, dunque come $100 \dots 0$ (con k zeri) in base B, analogamente al fatto che 10^k in base 10 si scriva $10 \dots 0$ (con k zeri).

Poi si può notare come

$$\begin{aligned}(B-1) + (B-1)B + (B-1)B^2 + \dots + (B-1)B^{k-1} = \\ = B - 1 + B^2 - B + B^3 - B^2 + \dots + B^k - B^{k-1} = B^k - 1,\end{aligned}$$

dunque B^{k-1} in base B si scrive come k volte la "cifra" $B - 1$, analogamente al fatto che $10^k - 1 = 99 \dots 9$.)

Esercizio 10.3. Si scrivano i numeri interi da 0 a 32 in base 2. Come si scrivono i numeri $2^{100} - 1, 2^{100}, 2^{100} + 1$ in base 2?

Esercizio 10.4 (Albergo di Hilbert). Consideriamo i seguenti sottoinsiemi di $\mathbf{N}^* = \mathbf{N} \setminus \{ 0 \}$, per $i \in \mathbf{N}$,

$$S_i = \left\{ x \in \mathbf{N} : x \equiv 2^i \pmod{2^{i+1}} \right\}.$$

Dunque

$$S_0 = \{ x \in \mathbf{N} : x \equiv 1 \pmod 2 \}$$

è l'insieme dei numeri dispari, cioè non divisibili per 2

$$S_1 = \{ x \in \mathbf{N} : x \equiv 2 \pmod 4 \}$$

è l'insieme dei numeri pari, cioè divisibili per 2, che non sono divisibili per 4, ecc.

- Mostrate che S_i è l'insieme dei numeri divisibili per 2^i ma non 2^{i+1}.
- Mostrate che $\mathbf{N}^* = \mathbf{N} \setminus \{ 0 \}$ è unione disgiunta degli S_i.

(Suggerimento: Si tratta solo di formalizzare quanto già scritto qua sopra.

Se $a \in S_t$, cioè $a \equiv 2^t \pmod{2^{t+1}}$, allora $a = 2^t + c2^{t+1}$ per qualche c, dunque $a = 2^t(1 + 2c)$ è divisibile per 2^t ma non per 2^{t+1}. Viceversa un numero divisibile per 2^t ma non per 2^{t+1} è della forma $a = 2^t d$, con d dispari, dunque $d = 1 + 2c$ per qualche c, e $a = 2^t + c2^{t+1} \equiv 2^t \pmod{2^{t+1}}$.

Sia $a \in \mathbf{N}^*$. Dato che ogni numero intero positivo si può scrivere in modo unico come prodotto di numeri primi, sarà, $a = 2^t b$ per opportuni $t \geq 0$, e b dispari, univocamente determinati. Allora $2^t \mid a$, ma $2^{t+1} \nmid a$. Dunque $a \in S_t$.

D'altra parte gli S_i sono a due a due disgiunti, perché se $i < j$, allora per il criterio che abbiamo visto, il sistema di congruenze

$$\begin{cases} x \equiv 2^i \pmod{2^{i+1}} \\ x \equiv 2^j \pmod{2^{j+1}} \end{cases}$$

non ha soluzione: $\gcd(2^{i+1}, 2^{j+1}) = 2^{i+1}$ non divide $2^j - 2^i = 2^i(2^{j-i} - 1)$.)

Esercizio 10.5. Un insieme infinito A si dice *numerabile* se esiste una funzione suriettiva $\nu : \mathbf{N} \to A$. Ad esempio, $\mathbf{N}$ è numerabile, prendendo $\nu = \mathbf{1}_{\mathbf{N}}$, la funzione identica su $\mathbf{N}$.

Mostrate che $\mathbf{Z}$ e $\mathbf{Q}$ sono numerabili. Non c'è bisogno di scrivere esplicitamente ν, ma occorre mostrare come la si può costruire, come ho fatto a lezione.

Esercizio 10.6 (L'esempio di RSA che ho fatto a lezione).

Alice vuol mandare un messaggio a Bob.

(1) Bob pensa i numeri primi $p = 3$ e $q = 5$, e calcola $n = pq = 15$.
(2) Bob calcola $\varphi(n) = 8$, e sceglie $r = 7$.
(3) Bob calcola s, t tali che
$$rs + \varphi(n)t = 1.$$
Si può scegliere
$$7 \cdot (-1) + 8 \cdot 1 = 1$$
o meglio
$$7 \cdot 7 + 8 \cdot (-6) = 1.$$
Dunque possiamo prendere $s = 7$.
(4) Alice vuole trasmettere $m = 2$. Calcola
$$\begin{aligned} c = m^r &\equiv 2^7 \\ &\equiv 2^{1+2+4} \\ &\equiv 2^1 \cdot 2^2 \cdot 2^4 \\ &\equiv 8 \pmod{15}, \end{aligned}$$
e trasmette $c = 8$.
(5) Per decifrare, Bob calcola prima $8^2 = 2^2 4^2 \equiv 4 \pmod{15}$ e $8^4 = (8^2)^2 \equiv 4^2 \equiv 1 \pmod{15}$, e dunque
$$\begin{aligned} m = c^s &\equiv 8^7 \\ &\equiv 8^{1+2+4} \\ &\equiv 8^1 \cdot 8^2 \cdot 8^4 \\ &\equiv 8 \cdot 4 \\ &\equiv 2 \pmod{15}. \end{aligned}$$

Esercizio 10.7. Si consideri il seguente schema RSA, in cui Bob manda un messaggio ad Alice.

(1) Alice pensa i numeri primi $p = 23$ e $q = 31$, e calcola $n = pq$.

(2) Notate che $26^2 \leq n < 26^3$. Alice calcola $\varphi(n)$, e sceglie $r = 7$.
(3) Prendete un messaggio di otto lettere, il messaggio che Bob vuole inviare a Alice. Dividetelo in quattro gruppi di due lettere. Codificate ogni lettera come un numero fra 0 e 25, secondo lo schema $A \mapsto 0$, $B \mapsto 1$, $\dots Z \mapsto 25$. Codificate, con il metodo esposto a lezione, ogni coppia di lettere come un numero p_i compreso fra 0 e $26^2-1 < n$, per $i = 1, 2, 3, 4$. Ad esempio, se a, b sono le prime due lettere (già espresse come numeri), allora $p_1 = a + b \cdot 26$.
(4) Mostrate come fa Bob a crittare il messaggio, ottenendo $c_i \equiv p_i^r \pmod{n}$.
(5) Mostrate come fa Alice a decifrare il messaggio, calcolando cioè s, e ottenendo $p_i \equiv c_i^s \pmod{n}$.

Esercizio 10.8. Un altro esempio di RSA: qui voi fate la parte di Alice. Il mittente è sempre Bob.

(1) Alice sceglie i numeri primi $p = 19$ e $q = 37$, e calcola $n = pq$ e $\varphi(n)$. Notate che n è compreso fra 26^2 e 26^3, dunque si possono crittare coppie di lettere.
(2) Alice sceglie poi $r = 85$. Verificate che sia $(r, \varphi(n)) = 1$, e calcolate s, t tali che $rs + \varphi(n)t = 1$.
(3) Comunicate r, n a Bob, che dopo un po' vi manda il messaggio
$$550, 87, 182, 35, 87, 446.$$
Decifratelo.
(4) Ah, dopo aver decifrato, come spiegate l'ultima, strana lettera del messaggio di Bob?

Esercizio 10.9. L'esempio di RSA fatto a lezione.

(1) Bob sceglie i numeri primi $p = 11$ e $q = 67$, e calcola $N = p \cdot q$ e $\varphi(N)$ (fatelo anche voi.
(2) Bob sceglie $r = 283$, e calcola s, t tali che
$$rs + \varphi(N)t = 1.$$
(Fatelo anche voi.)
(3) Bob annuncia la chiave pubblica (N, r).
(4) Alice cifra il messaggio "GATTOX", e lo manda a Bob. (Fatelo anche voi.)
(5) Bob decifra il messaggio. (Fatelo anche voi.)

Esercizio 10.10 (Facoltativo). Sia $n = pq$, ove p, q sono primi distinti. Siano r, s, t tali che
$$rs + \varphi(n)t = 1.$$
Si mostri che $a^{rs} \equiv a \pmod{n}$ per ogni intero a.

Dunque questo esercizio mostra che anche se gli a_i di Bob non soddisfano $\gcd(a_i, n) = 1$, Alice può comunque ricostruirli usando $a_i \equiv a_i^{rs} = (a_i^r)^s \equiv b_i^s \pmod{n}$.

(SUGGERIMENTO: Per $\gcd(a, n) = 1$ questo segue da Eulero-Fermat, come visto a lezione. Si tratta di vedere che la congruenza di cui sopra vale anche se $\gcd(a, n) \neq 1$, e questa parte è facoltativa. In tal caso conviene pensare a cosa può essere, questo massimo comun divisore, e magari usare il Teorema Cinese.)

Esercizio 10.11 (Facoltativo). Siano p, q primi distinti, e sia $n = pq$. La probabilità che un numero $0 \leq a < n$ preso a caso sia relativamente primo con n (ovvero che $\gcd(a, n) = 1$) è

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right) = 1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}.$$

Se $p, q \approx 10^{200}$, si dia una stima della grandezza di $\varphi(n)/n$, ovvero della piccolezza di

$$1 - \frac{\varphi(n)}{n} = \frac{n - \varphi(n)}{n},$$

che rappresenta la probabilità che un numero a preso a caso *non* sia relativamente primo con n (ovvero che $\gcd(a, n) > 1$).

Dunque questo esercizio mostra come sia estremamente improbabile che uno degli a_i di Bob *non* sia coprimo con n. In effetti, se fosse cosí facile trovare (andando per tentativi a caso) un numero $0 < a < n$ che *non* sia coprimo con n, basterebbe poi calcolare $\gcd(a, n)$, che essendo un divisore di $n = pq$ diverso 1 deve essere p o q, per riuscire a fattorizzare n.

Esercizio 10.12. Spiegate come si fa l'elevamento a potenza (modulo N) col metodo della scrittura dell'esponente in base 2, in particolare spiegando quante operazioni (divisioni con resto, moltiplicazioni) sono necessarie.

Nota. Le divisioni con resto non le ho ancora citate a lezione, ne parlerò la prossima settimana.