TRENTO, A.A. 2019/20
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 9

Esercizio 9.1. 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 9.2. 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 9.3. 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 9.4 (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 $\mathbf{N}^*$ 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, $a = 2^t b$ con $t \geq 0$, e b dispari. 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 9.5. 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 9.6 (Rudimentale, in caso lo sostituisco con una versione migliore). Nella procedura di RSA, viene richiesto a un certo punto di trovare un intero r coprimo con $m = \varphi(n)$. Quanto è difficile questo compito?

Sia m un intero positivo, che si scriva come prodotto

$$m = p_1 \cdot \cdots \cdot p_k$$

di k primi (non necessariamente distinti). Dato che $p_i \geq 2$ per ogni i, si ha $m \geq 2^k$, da cui $k \leq \log_2(m)$.

Ora il Teorema dei Numeri primi dice (a spanne) che fra 1 e m ci sono all'incirca $m/\log(m)$ numeri primi. (Qui $\log(m)$ è il logaritmo naturale, quello in base e.)

Ora

$$\frac{m/\log(m)}{\log_2(m)} = \frac{m}{\log(m)\log_2(m)}$$

tende all'infinito per $m \to \infty$, per cui è facile trovare un numero primo (si veda un altro esercizio) che non divida m, e sia dunque coprimo con m.