ES.: SIA $n \in \mathbb{P}$ IL PARAMETRO PUBBLICO DI UN CODICE RSA. DIMOSTRARE CHE, SE $\Phi(n)$ È NOTO, ALLORA POSSO ROMPERE RSA.

ABBIAMO CHE

$$n = p \cdot q \quad , \quad \Phi(n) = (p-1)(q-1)$$

$$\Rightarrow \quad p = \frac{n}{q} \quad \Rightarrow \quad \Phi(n) = \left(\frac{n}{q} - 1\right)(q-1)$$

$$\Rightarrow \quad q \cdot \Phi(n) = (n-q)(q-1)$$

$$\Rightarrow \quad q \cdot \overline{\Phi}(n) = nq - q^2 - n + q$$

$$\Rightarrow \quad q^2 + q\left(\overline{\Phi}(n) - n - 1\right) + n = 0$$

$$\Rightarrow \quad q = \frac{n+1-\overline{\Phi}(n) \pm \sqrt{\left(\overline{\Phi}(n)-n-1\right)^2 - 4n}}{2}$$

$$\Rightarrow \quad p = \frac{n}{q}.$$

ES.: QUANTI SOTTOINSIEMI DI $[7]$ CI SONO DI CARDINALITÀ 4?

SAPPIAMO DALLA TEORIA CHE IL NUMERO È

$$\binom{7}{4} = \frac{7 \cdot 6 \cdot 5 \cdot 4}{4!} = 7 \cdot 5 = 35.$$

POTREI ANCHE CALCOLARLO CON LA F.G.:

$$(1+x)^7 = (1+x)^3 (1+x)^3 (1+x)$$

$$= (1+3x+3x^2+x^3)(1+3x+3x^2+x^3)(1+x)$$

$$= (1+3x+3x^2+x^3+3x+9x^2+9x^3+3x^4+$$

$$+3x^2+9x^3+9x^4+3x^5+x^3+3x^4+3x^5+x^6)(1+x)$$

$$= (1+6x+15\cdot x^2+20\cdot x^3+15\cdot x^4+6\cdot x^5+x^6)(1+x)$$

$$= (1+6x+15\cdot x^2+20\cdot x^3+15\cdot x^4+6\cdot x^5+x^6+$$

$$+x+6x^2+15\cdot x^3+20\cdot x^4+15\cdot x^5+6\cdot x^6+x^7)$$

$$= 1 + 7x + 21 \cdot x^2 + 35 \cdot x^3 + \underset{\uparrow}{35} \cdot x^4 + 21 \cdot x^5 + 7 \cdot x^6 + x^7.$$

$$\binom{7}{4}$$

ES.: CALCOLARE

$$\left| \{ A \subseteq [9] : \ 2 \notin A \ \text{o} \ 8 \notin A \} \right|.$$

ABBIAMO CHE

$$\{ A \subseteq [9] : \ 2 \notin A \ \text{o} \ 8 \notin A \} = X \cup Y$$

DOVE

$$X = \{A \subseteq [9] : 2 \notin A\}$$

E

$$Y = \{A \subseteq [9] : 8 \notin A\}.$$

DEVO CALCOLARE $|X \cup Y| \Rightarrow$ USO I.E.

ABBIAMO

$$|X \cup Y| = |X| + |Y| - |X \cap Y|$$

MA

$$|X| = \left|\{A \subseteq [9] : 2 \notin A\}\right| = \left|\{A \subseteq \{1,3,4,5,6,7,8,9\}\}\right|$$

$$= 2^8$$

E

$$|Y| = \ldots = 2^8$$

INFINE

$$|X \cap Y| = \left|\{A \subseteq [9] : 2 \notin A \text{ E } 8 \notin A\}\right|$$

$$= \left| \{ A \subseteq \{1,3,4,5,6,7,9\} \} \right| = 2^7.$$

QUINDI

$$\left| \{ A \subseteq [9] : 2 \notin A \text{ o } 8 \notin A \} \right| = |X \cup Y|$$

$$= 2^8 + 2^8 - 2^7 = 2^7 (2+2-1)$$

$$= 3 \cdot 2^7.$$

ES.: CALCOLARE

$$\left| \{ f \in S_9 : f(2) \neq 2 \text{ E } f(4) \neq 4 \} \right|.$$

RAGIONAMENTO EURISTICO: "E" => INTERSEZIONE. FACILE? NON DIREI. PRINCIPIO DI I-E? IMPOSSIBILE. QUINDI?

DE MORGAN!

ABBIAMO CHE

$$\{f \in S_9 : f(2) \neq 2 \text{ E } f(4) \neq 4\} =$$

$$S_9 \setminus \{f \in S_9 : f(2) = 2 \text{ o } f(4) = 4\}$$

CALCOLIAMO QUINDI

$$|\{f \in S_9 : f(2) = 2 \text{ o } f(4) = 4\}|.$$

DOBBIAMO CALCOLARE

$$|X \cup Y|$$

DOVE

$$X = \{ f \in S_9 : f(2) = 2 \}$$

E

$$Y = \{ f \in S_9 : f(4) = 4 \}.$$

APPLICHIAMO I.E. DOBBIAMO CALCOLARE

$$|X|, \quad |Y|, \quad |X \cap Y|.$$

ABBIAMO CHE

$$|X| = |\{f \in S_9 : f(2) = 2\}| = 8!$$

$(f = x_1\, 2\, x_3\, x_4\, x_5\, x_6\, x_7\, x_8\, x_9)$

8 SCELTE, 7, 6 ETC...

SIMILMENTE $|Y| = \ldots = 8!$. INFINE

$$|X \cap Y| = |\{f \in S_9 : f(2) = 2 \text{ E } f(4) = 4\}|$$

$= 7!$ $(x_1\, 2\, x_3\, 4\, x_5\, x_6\, x_7\, x_8\, x_9 = f)$

7 SCELTE

PERTANTO

$$|X \cup Y| = 8! + 8! - 7!$$

CONCLUDENDO

$$\left| \{ f \in S_9 : f(2) \neq 2 \ E \ f(4) \neq 4 \} \right| =$$

$$9! - (|X \cup Y|) = 9! - (8! + 8! - 7!)$$

$$= 9! - 8! - 8! + 7!$$

$$= (9 \cdot 8 - 8 - 8 + 1) \cdot 7! = 57 \cdot 7!$$