2. Algebra Modulare e intro alla Crittografia

Aritmetica Modulare

$\mathbb{Z}_n \rightarrow$ modulo n

$\approx$ da 0 a n

Ex: $\mathbb{Z}_{10} \rightarrow 7+5=? \rightarrow \overline{2}$

Definizione: due numeri sono congruenti modulo n se la loro differenza è <u>multiplo di n</u>

Inverso

<u>No</u> frazioni !!

Definizione: l'inverso di a è quella

x tale che $x \cdot a \rightarrow$ resto 1

Ex: $\mathbb{Z}_7$ inverso di 3?

$$3 \cdot 5 = 15 \xrightarrow{\%\, 7} 1$$

inv. 3 in $\mathbb{Z}_7 = 15$

Definizione 2: a possiede un inverso SOLO SE $\underline{a}$ e $\underline{\text{modulo}}$ non hanno divisori in comune $(MCD = 1)$

$=$ a dire che sono coprimi

Fattorizzazione di Fermat

$\approx$ come fattorizzare numeri grandi dispari

Obiettivo $\rightarrow$ ottenere $x \cdot y$ da n

scrivere n come la differenza di due quadrati

$$n = a^2 - b^2 = (a-b)(a+b)$$

Metodo:

- $\underline{n} \rightarrow \sqrt{n} \rightarrow$ prendiamo il num arrotondato all' intero superiore che chiamo $\underline{a}$
- $a^2 - n = \underline{q}$
  - se $\underline{q}$ quadrato perfetto OK
  - altrimenti $a + 1$ e riprovi.

Crittografia

Cesare, Sostituzione

Esercizi

$n = 595$, fattorizziamo

$\hookrightarrow \quad a^2 - b^2 = (a-b)(a+b)$

$\sqrt{595} = 24{,}39 \to 25 = a$

$a^2 - n = 25^2 - 595 = 625 - 595 = 30$

$(a+1)^2 - n = 26^2 - 595 = 81 \approx \underline{\underline{9^2}}$

$$\begin{cases} b = 9 \quad a = 26 \\ \\ \left.\begin{array}{l} a - b = 26 - 9 = 17 \\ a + b = 26 + 9 = 35 \end{array}\right\} \underline{35 \cdot 17} \end{cases}$$