Relazioni di congruenza modulo un intero *n*

domenica 10 ottobre 2021 19:02

DEF. Sia *n* un intero diverso da zero e siano *a* e *b* due interi qualsiasi. Si definisce *a* congruo *b* modulo *n* ($a \equiv b \ mod \ n$) se e solo se $a - b = nh$, per qualche h intero, ovvero se e solo se la differenza fra *a* e *b* è divisibile per *n*.

OSS. $a \equiv b \ mod \ n$ se e solo se *a* e *b* hanno lo stesso resto se divisi per *n.*
DIM: Se $a = kn + r$ e $b = hn + r$ allora $a - b = n(k - h) + (r - r) = n(k - h)$, quindi se hanno lo stesso resto *r* sono congrui.
Se $a = kn + r_1$ e $b = hn + r_2$ allora $a - b = n(k - h) + (r_1 - r_2)$, quindi se $a - b$ è divisibile per *n* allora $r_1 - r_2$ è divisibile per *n*, ovvero $r_1 = nl + r_2$, ma $0 \leq r_1, r_2 < n$ quindi $l = 0$, ovvero $r_1 = r_2$.

PROP. Ogni intero a è congruo modulo *n* ad un UNICO intero *r* tale che $0 \leq r < n$.
DIM: $a \equiv r \ mod \ n$ con *r* resto UNICO della divisione di a per *n*. $a = ln + r \ \ 0 \leq r < n$, ovvero $a - r = ln$.

r si dice la classe di congruenza di a modulo n.

Le congruenze sono riflessive $a \equiv a \ mod \ n$, simmetriche $a \equiv b \ mod \ n \iff b \equiv a \ mod \ n$ e transitive $a \equiv b \ mod \ n \ e \ b \equiv c \ mod \ n \implies a \equiv c \ mod \ n$. Dimostrare per esercizio le tre proprietà appena elencate.
Ogni relazione con le tre proprietà appena descritte si dice relazione d'equivalenza.

PROP. Sia $n \geq 2$ *e* a, b, c, d *interi tali che* $a \equiv b \ mod \ n$ *e* $c \equiv d \ mod \ n$ allora

A) ▪ $a + c \equiv b + d \ mod \ n$
B) ▪ $a - c \equiv b - d \ mod \ n$
C) ▪ $ac \equiv bd \ mod \ n$

DIM: $(a - b) + (c - d) = (k_1 + k_2)n$ per ipotesi, quindi $(a + c) - (b + d) = hn$, ovvero la prima proprietà risulta dimostrata. La seconda proprietà si dimostra in modo analogo.
Relativamente alla terza basta considerare che $ac - bd = ac - bc + bc - bd = (a - b)c + (c - d)b = (k_1 c + k_2 b)n$, ovvero $ac \equiv bd \ mod \ n$.

PROP. Se $a \equiv b \ mod \ n$ allora

1) ▪ $a + c \equiv b + c \ mod \ n$ per ogni *c* intero
2) ▪ $ac \equiv bc \ mod \ n$
3) ▪ $a^k \equiv b^k \ mod \ n$ per ogni *k* naturale
4) ▪ Se $d | n$ allora $a \equiv b \ mod \ d$

DIM:

1): Utilizzando A) con $d = c$ si dimostra 1)

2): " C) " " " " 2)

3): $a^k = \underbrace{a \cdot a \cdot a \dots a}_{k \text{ volte}}$, quindi basta applicare 3) con $a = c$ e $b = d$ per k volte

4) $a - b = k \cdot h = k \cdot t \cdot d \implies d | a - b = 0 \ \ a \equiv b \ mod \ d$

DIVISIONI

- Se $ac \equiv bc \ mod \ n \ e \ (c,n) = 1 \ allora \ a \equiv b \ mod \ n$ (Dim: $c(a-b) = kn \ con \ (c,n) = 1 \Rightarrow n|a-b$)
- Se $ac \equiv bc \ mod \ n \ allora \ a \equiv b \ mod \frac{n}{d} \ con \ d = (c,n)$ (Dim: $c(a-b) = kn \iff (a-b)\frac{c}{d} = k\frac{n}{d} \quad ma \quad \left(\frac{n}{d}, \frac{c}{d}\right) = 1 \Rightarrow \frac{n}{d} | (a-b)$)

PROBLEMI

- Determinare la classe di congruenza modulo 7 del numero $N = 9^3 + 15^4 - 20^2 + 2 \cdot 52^{10}$.

$9^3 \equiv_7 2^3 = 8 \equiv 1 \qquad 15^4 \equiv_7 1 \qquad 20^2 \equiv (-1)^2 = 1 \qquad 52^{10} \equiv 3^{10} = 9^5 = 9^3 \cdot 9^2 = 4$

$9 \equiv_7 2$

$9^3 + 15^4 \equiv 1 + 1 \qquad N \equiv 1 + 1 - 1 + 4 \cdot 2 = 9 \equiv 2$

- Determinare la cifra delle unità del numero $N = 2^{35} + 3^{102} + 5^{404} + 7^{1034}$.

$N \equiv_{10} ? \qquad 2^5 \equiv_{10} 2 \qquad 2^{35} = (2^5)^7 \equiv (2)^7 = 2^5 \cdot 2^2 \equiv 2 \cdot 2^2 = 8$

$3^2 \equiv -1 \qquad 3^4 \equiv (-1)^2 = 1 \qquad 3^{102} \equiv 3^2 = 9 \equiv -1$

$N \equiv 8 - 1 + 5 - 1 \equiv 1$

- Determinare le ultime due cifre (decine ed unità) del numero 7^{2021}.

$7^{2021} \equiv_{100} ?$

$7^4 \equiv_{100} 01$

$7 \cdot 7^3 \equiv_{100} 01$

$7^2 \cdot 7^2 \equiv_{100} 01$

$53 \ mod \ 273$

$K \cdot 53 \equiv 1 \ mod \ 273$

$K \cdot 53 - 1 = t \cdot 223 \quad K \cdot 53 - t \cdot 253 = 1$

- Determinare le ultime 6 cifre della rappresentazione binaria del numero 585^{13}.

Divido per 64 $\quad n = a_0 2^0 + a_1 2^1 + a_2 2^2 + a_3 2^3 + a_4 2^4 + a_5 2^5 + \underbrace{\dots}_{\text{"0" mod 64}}$

$585 \equiv_{64} 9 \qquad 585^{13} \equiv_{64} 9^{13} = 9 \cdot (9^2)^6 \equiv 9 \cdot 17^6 \equiv 9 \cdot (17^2)^3 \equiv 9 \cdot (33)^3$

$\equiv 9 \cdot 33 \equiv 41 = 2^5 + 2^3 + 1 \Rightarrow 101001$

- Dimostrare che $3^{101} + 8^{101}$ è divisibile per 11. Determinare, inoltre, il numero modulo 13 e modulo 7.

$3^{101} + 8^{101} \equiv (3^2)^{50} \cdot 3 + (8^2)^{50} \cdot 8 \equiv (-1)^{50} \cdot 3 + (-2)^{50} \cdot 8$

$\equiv 3 + \left((-2)^5\right)^{10} \cdot 8 \equiv 3 + 1^{10} \cdot 8 = 11 \equiv 0$

OPPURE $\quad 3^{101} + 8^{101} = (3+8)(3^{100} - 3^{99} \cdot 8 + 3^{98} \cdot 8^2 - \dots)$

- Dire se il polinomio $p(x) = x^5 + 7x^4 + 2x^3 + 6x^2 - x + 1568$ possiede radici intere.

Se $p(k) = 0$ per qualche $k \in \mathbb{Z}$, allora $p(k) \equiv_n 0 \ \forall n$

Ma $\quad x^5 + 7x^4 + 2x^3 + 6x^2 - x + 1568 \equiv_3 x^5 + x^4 + 2x^3 - x + 2$

$p(0) \equiv_3 2 \qquad p(1) \equiv_3 5 \equiv 2 \qquad p(2) = 64 \equiv_3 1 \Rightarrow \nexists k \in \mathbb{Z} \text{ t.c. } p(k) = 0$

- N è divisibile per 3 se e solo se 3 divide la somma delle cifre di N.

$10 \equiv_3 1 \rightarrow 10^m \equiv_3 1 \quad \forall m \in \mathbb{N}$

$N = a_0 + a_1 \cdot \underset{\vdots}{10} + a_2 \cdot \underset{\vdots}{10^2} + a_3 \cdot \underset{\vdots}{10^3} + \dots \equiv a_0 + a_1 + a_2 + a_3 + \dots$

QUINDI OGNI NUMERO É CONGRUO ALLA SOMMA DELLE SUE CIFRE MODULO 3

- N è divisibile per 11 se e solo se 11 divide la somma a segni alterni delle cifre di N.

$10 \equiv_{11} -1 \quad 10^2 \equiv_{11} (-1)^2 = 1 \quad 10^{2m} \equiv_{11} 1 \quad 10^{2m+1} \equiv_{11} -1$

$N = a_0 + a_1 \cdot \underset{\vdots}{10} + a_2 \cdot \underset{\vdots}{10^2} + a_3 \cdot \underset{\vdots}{10^3} + \dots \equiv a_0 - a_1 + a_2 - a_3 + \dots$
$\qquad\qquad\qquad\quad -1 \qquad\quad +1 \qquad\quad -1$