57.432^{1142} $\mod 9$

$1.142 \mid 2$
571

$57.432 = 9 \cdot 6.381 + 3$
$\underbrace{\qquad\qquad}_{57.429}$

$57.432 \equiv 3 \pmod 9$ $\qquad 3^2 = 9$

$57.432^{1.142} \equiv 3^{1.142} \pmod 9$ $\qquad 3^{1.142} = (3^2)^{571} = 9^{571}$

$57.432^{1.142} \equiv 9^{571} \pmod 9$ $\qquad 9 \equiv 0 \pmod 9$

$57.432^{1142} \equiv 0 \pmod 9$

il resto è 0.

$362.971^{29.345}$ $\mod 6$

$362.971 \mid 6$
60.495

$362.971 = 6 \cdot 60.495 + 1$

$362.971 \equiv 1 \pmod 6$

$362.971^{29.345} \equiv 1^{29.345} \equiv 1 \pmod 6$

il resto è 1.

$a^{\varphi(n)} \equiv 1 \pmod n$ quando $M.C.D.(a, n) = 1$

Se n è primo $\varphi(n) = n - 1$ e quindi ritorniamo

$2^n > n^2 + 4n + 5$ $\quad n \in \mathbb{N}$ $\quad n \geq 7$

$P(7)$ vero: $\quad 2^7 > 7^2 + 4 \cdot 7 + 5$

$128 \quad 49 + 28 + 5 = 72$

$2^7 = 2^4 \cdot 2^3 = 16 \cdot 8$

$64 + 28 = 92$

$128 > 92$ vero

Per $n = 6$ $\quad 2^6 = 64$ $\quad 6^2 + 4 \cdot 6 + 5 = 36 + 24 + 5 = 65$

$64 \not> 65$.

Passo induttivo: $\quad 2^n > n^2 + 4n + 5$ vero

$2^{n+1} > (n+1)^2 + 4(n+1) + 5$ da verificare

$2^{n+1} = 2^n \cdot 2 = 2^n + 2^n > n^2 + 4n + 5 + n^2 + 4n + 5 = 2n^2 + 8n + 10$

ipotesi d'induz.

$(n+1)^2 + 4(n+1) + 5 = n^2 + 2n + 1 + 4n + 4 + 5$

$n^2 + 6n + 10$

$2n^2 + 8n + 10 > n^2 + 6n + 10$ certamente

$2n^2 + 8n + 10 = n^2 + n^2 + 6n + 2n + 10 = (n^2 + 6n + 10) + n^2 + 2n >$ ($n^2 + 2n > 0$)

$> n^2 + 6n + 10$

Quante combinazioni con ripetizioni

disposizioni

a b a b ≠ a a b b come disposizioni

a b a b = a a b b come combinazione

numero delle disposizioni con ripetizioni di k oggetti di classe n

$$k^n$$

$\sqcup\!\sqcup$ $\sqcup\!\sqcup$ $\sqcup\!\sqcup$ $\sqcup\!\sqcup$ $\sqcup\!\sqcup$ ... $\sqcup\!\sqcup$

k k k k k k

numero delle combinazioni con ripetizioni di k oggetti di classe n

$$\binom{k+n-1}{n}.$$

$(\mathbb{Z}_q, +)$

generatori

$|[6]_q|$ $\langle [6]_q \rangle$

$[a]_n$ è generatore di $(\mathbb{Z}_n, +) \iff M.C.D.(a,n) = 1$

$[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9$ generatori di $(\mathbb{Z}_9, +)$

$$|[6]_9| = \frac{9}{M.C.D(6,9)} = \frac{9}{3} = 3$$

$\langle [6]_9 \rangle$ ha 3 elementi

$$\langle [6]_9 \rangle = \{ [6]_9,\ 2\cdot[6]_9 = [6]_9 + [6]_9 = [12]_9 = [3]_9,$$
$$3[6]_9 = [6]_9 + [6]_9 + [6]_9 = [18]_9 = [0]_9 \} =$$

$$= \{ [6]_9, [3]_9, [0]_9 \}.$$

$$\begin{cases} 2x \equiv 5 \pmod 3 \\ x \equiv 3 \pmod 5 \\ 3x \equiv 4 \pmod 3 \end{cases} \longrightarrow$$
$a \qquad\qquad n$

$M.C.D.(3,3) = 3 \qquad 3 \nmid 4$

e quindi la congruenza non ha soluzioni

Quindi il sistema non ha soluzioni

$$\sum_{i=0}^{n+1} 2i+1 = n^2 + 4n + 4 \qquad n \in \mathbb{N}$$

Passo base $P(0)$ vero $\qquad \sum_{i=0}^{1} 2i+1 = 0^2 + 4\cdot 0 + 4$

$$\sum_{i=0}^{1} 2i+1 = (2\cdot 0+1) + (2\cdot 1+1) = 1+3 = 4$$ //

$0^2+4\cdot 0+4 = 4$ //

$P(0)$ è verificata.

Passo induttivo $P(n)$ vero: $\sum_{i=0}^{n+1} 2i+1 = n^2+4n+4$ ipotesi di induz.

$P(n+1)$ vero: $\sum_{i=0}^{n+2} 2i+1 = (n+1)^2+4(n+1)+4$

$$\underbrace{(n+1)^2+4(n+1)+4}_{\sum_{i=0}^{n+2} 2i+1} = n^2+2n+1+4n+4+4 = n^2+6n+9$$

$$\sum_{i=0}^{n+2} 2i+1 = \underbrace{\sum_{i=0}^{n+1} 2i+1}_{n^2+4n+4} + (2(n+2)+1) = n^2+4n+4+(2n+4+1) =$$

ipotesi d'induzione

$$= n^2+4n+4+2n+4+1 = n^2+6n+9$$

$P(n+1)$ è verificata.

$a^p \equiv a \pmod p$ induzione su a $\quad a \geq 0$

$0^p \equiv 0 \pmod p$ vera

$a^p \equiv a \pmod p$ ipotesi d'induzione

$(a+1)^p \equiv a+1 \pmod p$

$(x+y)^p \equiv x^p + y^p \pmod p$

$(a+1)^p \equiv a^p + 1^p \pmod p$

$(a+1)^p \equiv a^p + 1 \pmod p$

$a^p \equiv a \pmod p$

$(a+1)^p \equiv a + 1 \pmod p$

$a > 0 \qquad -a < 0$

$(-a)^p \equiv (-a) \pmod p$ perché $-a > 0$

$$0 = (a + (-a))^p \equiv a^p + (-a)^p \equiv a^p + (-a) \pmod p$$

$$\left.\begin{array}{l} a^p + (-a) \equiv 0 \pmod p \\ a \equiv a \pmod p \end{array}\right\} \Rightarrow$$

$$a^p + (-a) + a \equiv 0 + a \pmod p$$

$$a^p \equiv a \pmod p$$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 7 & 2 & 3 & 5 & 1 & 4 & 8 & 9 \end{pmatrix}$$

cicli disgiunti e classe

$|f|$ in $(S_9, \circ)$

$H = \langle f \rangle$

$f = (1\,6) \circ (2\,7\,4\,3)$ di classe pari

$f = (1\,6) \circ (2\,3) \circ (2\,4) \circ (2\,7)$ composta da 4 scambi

$|f| = m.c.m.(|(1\,6)|, |(2\,7\,4\,3)|) = m.c.m.(2,4) = 4$

$|\langle f \rangle| = 4$

$H = \langle f \rangle = \{ f, f^2, f^3, f^4 = id \}$

$f^2 = (1\,6)^2 \circ (2\,7\,4\,3)^2 = id_9 \circ (2\,4) \circ (7\,3) = (2\,4) \circ (7\,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 4 & 7 & 2 & 5 & 6 & 3 & 8 & 9 \end{pmatrix}$

$\left(|f^2| = \frac{4}{M.C.D.(2,4)} = \frac{4}{2} = 2 \right)$

$f^3 = (16)^3 \circ (2743)^3 = (16)^2 \circ (16) \circ (2347) = (16) \circ (2347) =$

$($ $)$

f^{-1} ?

$f^4 = id_g \Rightarrow f \circ f^3 = id_g \Rightarrow f^{-1} = f^3$

$(f^3)^{-1} = f$

$f^2 \circ f^2 = f^4 \Rightarrow (f^2)^{-1} = (f^2)$

$id_1^{-1} = id_g$

$f^5 = f^4 \circ f = f$

$f^3 \circ f^3 = f^6 = f^2$

tavolina di $(H, \circ)$

$\circ$	id_g	f	f^2	f^3
id_g	id_g	f	f^2	f^3
f	f	f^2	f^3	id_g
f^2	f^2	f^3	id_g	f
f^3	f^3	id_g	f	f^2

$f^4 = id_g$

$f^4 = f \circ f^3 = id_g$

$f^4 = f^3 \circ f = id_g$

$f^4 = f^2 \circ f^2 = id_g$

$43.816^{20.321}$ per 10

$43.816 \equiv 6 \pmod{10}$ $\qquad 6^{20.321} \pmod{10}$

M.C.D. $(6,10) \neq 1$

$$6^2 = 36 \equiv 6 \pmod{10}$$

$$6^4 = 1.296 \equiv 6 \pmod{10}$$

$$6^n \equiv 6 \pmod{10} \qquad n \in \mathbb{N}^*$$

per induz.

$$6^1 \equiv 6 \pmod{10}$$

$$6^{n+1} = 6^n \cdot 6 \equiv 6 \cdot 6 \equiv 6 \pmod{10}$$

ipotesi d'induz.

Quindi il resto è 6 perché: $6^{20.321} \equiv 6 \pmod{10}$.