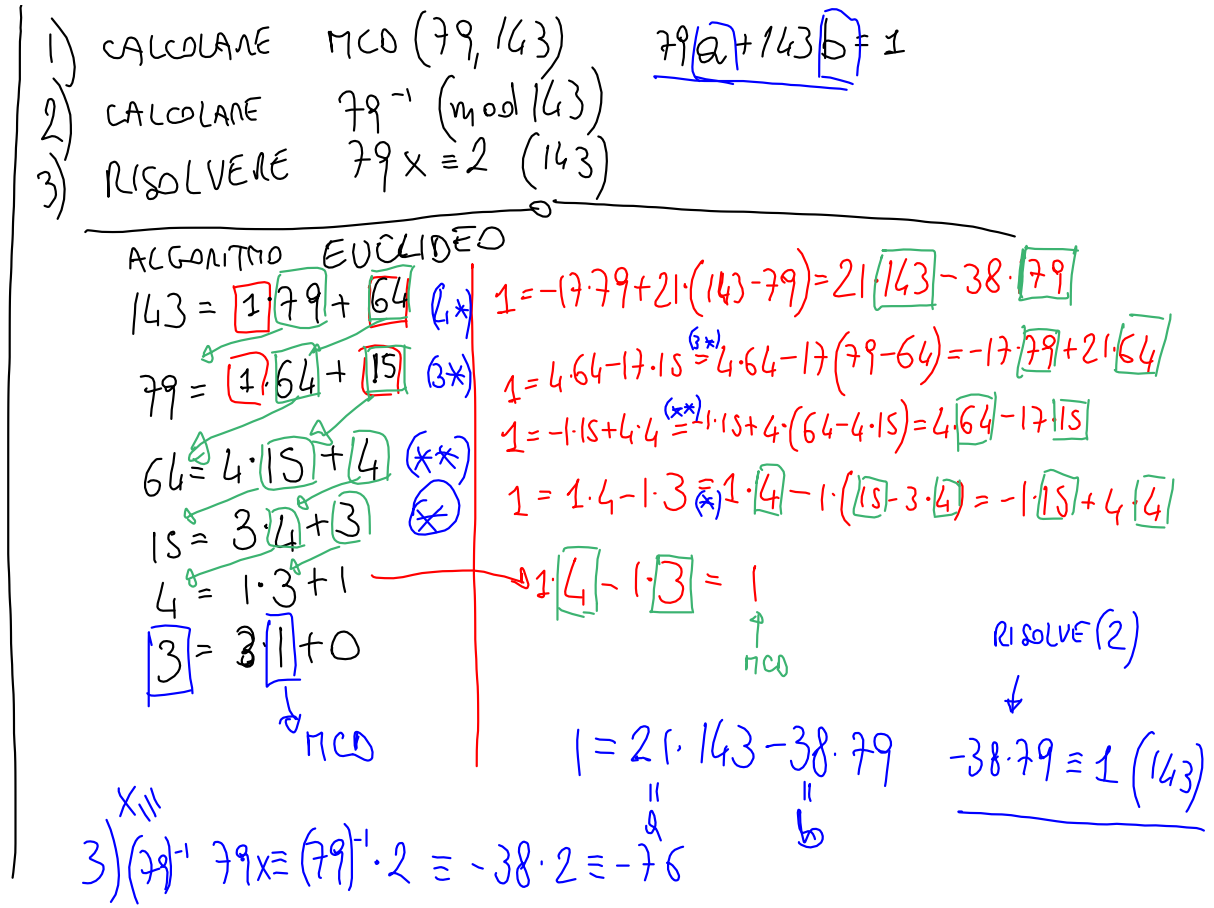
1) CALCOLARE MCD (79, 143)
2) CALCOLARE 79^-1 (mod 143)
3) RISOLVERE 79x ≡ 2 (143)
79·9 + 143·5 = 1
ALGORITMO EUCLIDEO
143 = 1·79 + 64 (1*)
79 = 1·64 + 15 (3*)
64 = 4·15 + 4 (**)
15 = 3·4 + 3 (*)
4 = 1·3 + 1
3 = 3·1 + 0
MCD
1 = -17·79 + 21·(143 - 79) = 21·143 - 38·79
1 = 4·64 - 17·15 (3*) 4·64 - 17(79 - 64) = -17·79 + 21·64
1 = -1·15 + 4·4 (**) 1·15 + 4·(64 - 4·15) = 4·64 - 17·15
1 = 1·4 - 1·3 (*) 1·4 - 1·(15 - 3·4) = -1·15 + 4·4
1·4 - 1·3 = 1
MCD
RISOLVE (2)
1 = 21·143 - 38·79
a
b
-38·79 ≡ 1 (143)
3) (79)^-1 79x ≡ (79)^-1 · 2 ≡ -38·2 ≡ -76
X III

$(79)^{-1}\,79x \equiv 2(79)^{-1}(143)$

$x \equiv 2\cdot(-38) \Rightarrow x \equiv 2\cdot(-38) \equiv -76 \equiv 67$

Calcolare

$\underbrace{4X^4-X^2+2X-1}_{a(X)} : \underbrace{2X^2+2X+1}_{b(X)}$ (divisione con resto)

Esistono sempre $q(X)$, $r(X)$ t.c. $a(X) = q(X)b(X) + r(X)$

e $\deg r(X) < \deg b(X)$

(oppure $r(X) = 0$)

$a(x)$ $b(x)$ $q_1(x)$ $q_2(x)$ $q_3(x)$ $\mathbb{Z}[x]$

$4x^4 + 0\cdot x^3 - x^2 + 2x - 1 : 2x^2+2x+1 = 2x^2 - 2x + \frac{1}{2}$ $q(x), r(x) \in \mathbb{Q}[x]$

$4x^4+4x^3+2x^2$ ← $b(x)\cdot q_1(x)$

$-4x^3-3x^2+2x-1$ ← differenza $a(x) - b(x)\cdot q_1(x)$

$(2x^2+2x+1)\cdot 2x^2 = 4x^4+4x^3+2x^2$

$-4x^3-4x^2-2x$ ← $b(x)\cdot q_2(x)$

$(2x^2+2x+1)\cdot(2x^2-2x) =$

$= 4x^4 + \cancel{4x^3} + 2x^2 - \cancel{4x^3} - 4x^2 - 2x =$

x^2+4x-1 ← differenza

$= 4x^4 - 2x^2 - 2x$

$x^2+x+\frac{1}{2}$ ← $b(x)\cdot q_3(x)$

$3x-\frac{3}{2}$ ← resto

$$a(x) = b(x)\underbrace{\left(2x^2-2x+\frac{1}{2}\right)}_{\text{quoziente}} + \underbrace{3x-\frac{3}{2}}_{\text{resto}}$$

: SERVE FARE DIVISIONI, SI PUÒ FARE IN UN CAMPO

PERÒ SE $b(x)$ È MONICO (TERMINE DI GRADO PIÙ ALTO HA COEFF. 1)

NON SERVONO DIVISIONI

$4x^4+0\cdot x^3-x^2+2x-1 : x^2+2x+1 = 4x^2-8x+11$

quoziente

$-4x^4+8x^3+4x^2$

$-8x^3-5x^2+2x-1$

$-8x^3-16x^2-8x$

$11x^2+10x-1$

$11x^2+22x+11$

$-12x-12$

resto

$\mathbb{Z}[x]$

Quello

$4x^4-x^2+2x-1=(x^2+2x+1)\cdot(4x^2-8x+11)+(-12x-12)$

$197x^{17} = \frac{197}{5}x^{14}\cdot 5x^3$

$ax^m = \frac{a}{b}x^{m-n}\cdot bx^n$

$4x^4 - 0x^3 - x^2 + 2x - 1 : 2x^2 + 2x + 1 = 2x^2 - 2x + 3$ conti in $\mathbb{Z}_5[x]$

$4x^4 + 4x^3 + 2x^2$

$-4x^3 - 3x^2 + 2x - 1$

$-4x^3 - 4x^2 - 2x$

$x^2 + 4x - 1$

$6x^2 + 6x + 3$

$0 \quad 3x - 4 \equiv 3x + 1$

in $\mathbb{Z}_5[x]$,

$4x^4 - x^2 + 2x - 1 = (2x^2 + 2x + 1) \cdot (2x^2 - 2x + 3) + 3x + 1$

Non funziona in $\mathbb{Z}/(6)$

Funziona anche in $\mathbb{Z}/(5)$

Serve che il coefficiente del termine di grado più alto abbia inverso

$x^2 = \boxed{3} \cdot 2x^2$

Dimostrare (per induzione) che per ogni $n \in \mathbb{N}$

$5^{2n} \equiv 1 \pmod{12}$ $P(n)$

Sol: PASSO BASE $P(0)$: $5^{2 \cdot 0} \equiv 1 \pmod{12}$

PASSO INDUTTIVO so $P(n)$, dimostro $P(n+1)$

$P(n)$: $5^{2n} \equiv 1 \pmod{12}$

dimostro $P(n+1)$: $5^{2(n+1)} = 5^{2n} \cdot 5^2 \equiv 5^2 \equiv 25 \equiv 1$

(provate a farlo direttamente, senza induzione)

ES

DIMOSTRARE CHE $n^3+(n+1)^3+(n+2)^3 \equiv 0 \mod 3$ $\quad P(n)$

PER OGNI $n \in \mathbb{N}$

$P(0)$ ~ FACILE

$P(n) \Rightarrow P(n+1)$: so che $n^3+(n+1)^3+(n+2)^3 \equiv 0 \ (3)$

$(n+1)^3+(n+2)^3+(n+3)^3 \overset{\text{ipotesi}}{\equiv} (n+1)^3+(n+2)^3+(n+3)^3 - n^3-(n+1)^3-(n+2)^3 \equiv$

posso sottrarlo perché $\equiv 0$

$\equiv (n+3)^3 - n^3 \equiv n^3+9n^2+27n+81-n^3 \equiv 0$

tutti multipli di 3

(LMM 2007, giugno)

1) Trovare tutti gli interi che soddisfano

$$1386x \equiv 1890 \mod 294$$

Posso dividere tutto per un multiplo comune

Sono tutti multipli di 42! Posso eliminarlo

$$33x \equiv 45 \pmod 7$$

L'altro modo in cui si può semplificare è dividere per cose prime con il modulo

$$3^{-1} \cdot 33x \equiv 45 \cdot 3^{-1} \pmod 7$$

$$\Downarrow$$

$$11x \equiv 15 \pmod 7$$

$11x \equiv 15 \pmod 7$

Posso anche sottrarre multipli di 7 ai numeri che compaiono:

$2 \cdot 4x \equiv 1 \cdot 2 \pmod 7$

$\Downarrow$

$x \equiv 2 \pmod 7$ $\qquad 7k+2$

2. $1386x^2 \equiv 1890 \pmod{294}$

... tutto come prima fino a...

$2 \cdot 4x^2 \equiv 1 \cdot 2 \pmod 7$

$x^2 \equiv 2 \pmod 7$

Sol. (a forza bruta):

$x \equiv 3, 4 \mod 7$

$\equiv \pm 3$

$0^2 \equiv 0$

$1^2 \equiv 1$

$2^2 \equiv 4$

$3^2 \equiv 9 \equiv 2$

$4^2 \equiv (-3)^2 \equiv 2$

$5^2 \equiv (-2)^2 \equiv 4$

$6^2 \equiv (-1)^2 \equiv 1$

3.

$1386x^3 \equiv \dots$

$x^3 \equiv 2 \pmod 7$

mai!

$0^3 \equiv 0$
$1^3 \equiv 1$
$2^3 \equiv 8 \equiv 1$
$3^3 \equiv -1$
$4^3 \equiv (-3)^3 \equiv -3^3 \equiv 1$
$5^3 \equiv -1$
$6^3 \equiv -1$

$(-x)^3 \equiv -x^3$

$x \equiv -52 \pmod 4$

$x \equiv -52 + 60 \equiv 8$

(RISPOSTE STUDENTI) ES: modulo 7, potenze pcipde

5, 6 primi tra loro

Allora esiste $6-5=1$ — Bézout

Funziona sempre se $\mathrm{mcd}(\text{esponente}, p-1)=1$ (per $x \neq 0$)

$x = \frac{x^6}{x^5} = \frac{1}{x^5}$

Se fosse $x \neq y$ ma $x^5 \equiv y^5$, allora $x \equiv \frac{1}{x^5} \equiv \frac{1}{y^5} \equiv y$, assurdo