Stage di TERNI - (26/01/2011)

Titolo nota 26/01/2011

ARITMETICA - Avenzi

1. num. primi
2. equazioni con numeri interi (fattorizzando, raccogliendo i quadrati)
3. congruenze
4. le 4 operazioni
$\left(\begin{array}{c} a-b \text{ è mult. di } m \\ a \equiv b \ (m) \end{array}\right)$ (CAVEAT: la divisione)
5. equazioni di 1° grado con le congruenze (es: $2x \equiv 1 \ (7)$)

Fatto: Se $MCD(a,b) = 1$, allora esistono x, y interi tali che

$$ax + by = 1$$

es: •) 7, 13 $\quad 2 \cdot 7 - 13 = 1$

•) 8, 25 $\quad -3 \cdot 8 + 25 = 1$

es: •) 2, 4 $\quad 2x + 4y = 2(x + 2y) \neq 1$

•) a, b, $MCD(a,b) = d > 1 \Rightarrow a = d \cdot a' \quad b = d \cdot b'$

$$ax+by = d\cdot a'x + d\cdot b'y = d(a'x+b'y) \neq 1$$

Algoritmo per l'MCD: $MCD(1024, 257)$

$1024 : 257 = 3 \quad r = 253$

$1024 = 3\cdot 257 + 253 \longrightarrow 253 = 1024 - 3\cdot 257$

$MCD(1024, 257) = MCD(257, 253)$

$257 : 253 = 1 \quad r = 4 \longrightarrow 4 = 257 - 253$

$MCD(257, 253) = MCD(253, 4)$

$253 : 4 = 63 \quad r = 1 \longrightarrow 253 = 63\cdot 4 + 1$

$MCD(253, 4) = MCD(4, 1) = 1$

$1 = 253 - 63\cdot 4 =$

$= 253 - 63(257 - 253) =$

$= 64\cdot 253 - 63\cdot 257 =$

$= 64\cdot(1024 - 3\cdot 257) - 63\cdot 257 =$

$= 64\cdot 1024 - 257(64\cdot 3 + 63) =$

$= 64\cdot 1024 - 255\cdot 257$

$x \qquad\qquad y$

Algoritmo Euclideo

64 · 3 = 192
63
255

se $MCD(a,b)=1$, allora $ax+by=1$

$$ax \equiv 1 \quad (b)$$ ← x si chiama Inverso modulo b di a

es: inverso di 7 mod 13 = 2

$2 \cdot 7 - 13 = 1$

inverso di 8 mod $25 = -3 \equiv 22 \quad (25)$

es: $257x \equiv 48 \quad (1024)$ $\quad MCD(1024, 257)=1$

Trovo due numeri α, β t.c. $1024\alpha + 257\beta = 1$

$\alpha = 64$, $\beta = -255$

$\Leftarrow$

$-255 \cdot 257 \equiv 1 \quad (1024)$

$-255 \cdot 257 x \equiv -255 \cdot 48 \quad (1024)$

$1 \quad x \equiv -976 \quad (1024)$

$x \equiv 48 \quad (1024)$

$$\begin{array}{r} {\scriptstyle 4} \\ 255 \cdot \\ 48 = \\ \hline 2040 \\ 1020 \\ \hline 12240 \end{array}$$

Riflessione: Cos'è $\frac{1}{3}$? $\frac{1}{3}$ è il numero che moltiplicato per 3 fa 1

$\Rightarrow$ modulo 7 $\frac{1}{3}$ "è" 5

$3x \equiv 2 \pmod 7$ $\qquad$ $x \equiv \frac{2}{3} \pmod 7$

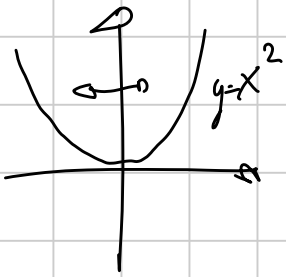
$MCD(3,7)=1 \Rightarrow$ "esiste" $\frac{1}{3}$ che è $5 \bmod 7$

$$\frac{2}{3} \equiv 2 \cdot \frac{1}{3} \equiv 2 \cdot 5 \equiv 10 \equiv 3 \pmod 7$$

Quando n^2+1 è mult. di 7?

$n^2+1 \equiv 0 \pmod 7$

n	n^2+1
-3	3
-2	5
-1	2
0	$0+1=1$
1	$1+1=2$
2	$4+1=5$
3	$9+1 \equiv 3$



n	n^3 (7)
0	0
1	1
2	1
3	-1
-3	1
-2	-1
-1	-1

$(-3)^3 = -(3)^3$

-1

$3^n + 1 \equiv 2 \pmod 7$ $\qquad$ $3^1 + 1 \equiv 4 \pmod 7$

$3^{n+7} = 3^n \cdot 3^7$

$3^8 + 1 \equiv \pmod 7$

$\equiv 2^4 + 1 \equiv (-3)^2 + 1 \equiv 3$ $\neq$

$3^7 \equiv 1 \pmod 7$

(7)

n	3^n+1
0	2
1	4
2	3
3	0
4	5
5	6
6	2
7	4
8	3
9	0
10	5
11	6
12	2

6

$n = 0 + 6k$

$3^6 + 1 \equiv 2$

$3^6 \equiv (3^2)^3 \equiv 2^3 \equiv 8 \equiv 1$

Ex: mod 5

n	2^n
0	1
1	2
2	4
3	3
4	1
5	
6	

4

$2^5 = 2^4 \cdot 2 \equiv 2^0 \cdot 2 \equiv 2^1$

mod 5

n	4^n
0	1
1	4
2	1
3	4
4	1

2

Fatto: Se il modulo è primo (p)

le potenze si ripetono con periodo che

divide $p-1$

n	2^n (7)
0	1
1	2
2	4
3	1

] 3

mod 13

12, 6, 4, 3, 2, 1

$(-1)^n$ 1^n

Trovare x, y naturali t.c. $3^x - 2^y = 1$

$3 - 2 = 1$

$9 - 8 = 1$

mod 3

$-2^y \equiv 1$

y	2^y	-2^y
0	1	$\not\equiv 2$
1	2	$\not\equiv 1$
2	1	$\not\equiv 2$

$y = 1 + 2k$

y dispari

mod 2

$3^x \equiv 1$

$1^x \equiv 1$ $\forall x$

$x, y \geq 2$

mod 4

$3^x \equiv 1 \quad (4)$

$(-1)^x \equiv 1 \quad (4)$ x pari

$x = 2h \qquad y = 2k+1$

$$\boxed{3^{2h} - 2^{2k+1} = 1}$$

$$3^{2h} - 1 = 2^{2k+1}$$

$$(3^h - 1)(3^h + 1) = 2^{2k+1}$$

$$\| \qquad \| \qquad b > a$$

$$2^a \qquad 2^b$$

$$2^b - 2^a = 2$$

$$2^{b-1} - 2^{a-1} = 1$$

$$a - 1 = 0 \Rightarrow \boxed{a = 1}$$

$$b - 1 = 1$$

$$\boxed{b = 2}$$

$$1$$

$$2^{b-1} - 1 = 1$$

$$3^h + 1 = 4$$

$$3^h - 1 = 2$$

$$2 \cdot 3^h = 6$$

$$3^h = 3 \Rightarrow h = 1$$

$$\boxed{x = 2h = 2}$$

$$\boxed{y = 3}$$

$$3m^2 + 2m - 1 = 0 \qquad (13)$$

$$3x^2 + 2x - 1 = 0 \qquad 3(x+1)\left(x - \frac{1}{3}\right)$$

$$x = \frac{-2 \pm \sqrt{4 + 12}}{6} =$$

$$= \frac{-2 \pm \sqrt{16}}{6} = \frac{-2 \pm 4}{6} = \begin{matrix} -1 \\ \frac{1}{3} \end{matrix}$$

$$3n^2+2n-1 \equiv 3\left(n+1\right)\left(n-\frac{1}{3}\right) \equiv$$

$$\equiv 3(n+1)(n-9) \quad (13)$$

13 divide $3\cdot(n+1)\cdot(n-9)$

$\Downarrow$

13 divide $(n+1)(n-9)$

$\Downarrow$

13 divide $n+1$

oppure

13 divide $n-9$

En caltivo:

$$(x^4-1) \equiv 0 \quad (8)$$

$$(x-1)(x+1)(x^2+1)$$

1, 7, 3, 5

$$(3^2-1)\cdot(3+1)^4\cdot(9+1)^{10}$$

$$80 \equiv 0 \ (8)$$

En + caltivo: $x^2+1 \equiv 0 \quad (13)$

$x = 5+13k$

$x = 8+13k$

$x^2+1 \equiv 0 \ (p)$

$$x^2+1 \equiv x^2+27 \equiv \boxed{x^2-25}$$

$$\equiv x^2-12 \equiv x^2+14 \quad (13)$$

si risolve sempre se $p \equiv 1 \ (4)$

Esercizi: 1) Risolvere: (i) $x^4 - 1 \equiv 0 \quad (16)$

(ii) $13^n + 17^n \equiv 0 \quad (5)$

(iii) $6n^2 - n - 1 \equiv 0 \quad (17)$

2) Trovare (Tutti i naturali) x, y, z t.c. $3^x + 4^y = 5^z$

3) Risolvere: (i) $n^2 \equiv n+1 \quad (11)$

(ii) $n^2 \equiv n+1 \quad (31)$

1) (i) $x^4 - 1 \equiv 0 \quad (16)$ • x deve essere dispari

$x = 1, 3, 5, 7, 9, 11, 13, 15$

$(x-1)(x+1)(x^2+1)$

$x-1$, $x+1$ sono PARI e CONSECUTIVI

$\Rightarrow$ uno dei due è $\equiv 0 \ (4)$

$2 \quad 2 \quad 2$

2

$8 \cdot 2 = 16 \Rightarrow (x-1)(x+1)$ è mult. di 8

$\Rightarrow x^4 - 1 \equiv 0 \ (16) \quad \forall x$ dispari

(ii) $13^4 + 17^4 \equiv 0 \quad (5)$

$3^n + 2^n \equiv 0 \quad (5)$

$n = 1 + 4k, \ 3 + 4k$

n	2^n	3^n	+
0	1	1	2
1	2	3	0
2	-1	4	3
3	3	2	0
4	1	1	2

4

$(-2)^n + 2^n \equiv 0 \ (5)$ → n pari $(-2)^n = 2^n$

$2 \cdot 2^n \equiv 0 \ (5)$ mai

$\Leftarrow$

n dispari → n dispari $(-2)^n = -2^n$

$-2^n + 2^n \equiv 0 \ (5)$

(iii) $6n^2 - n - 1 \equiv 0 \ (17)$

$6\left(n - \frac{1}{2}\right)\left(n + \frac{1}{3}\right) \equiv 0 \ (17)$

$\frac{1}{2}$ = n. che moltiplicato per 2 fa $1 \equiv 9 \ (17)$

$\frac{1}{3}$ = n° che molt. per 3 fa $1 \equiv 6 \ (17)$

$6(n-9)(n+6) \equiv 0 \ (17)$

17 è primo $\Rightarrow$ $\underline{n \equiv 9}$ $n \equiv -6 \equiv \underline{11} \ (17)$

3) $n^2 \equiv n+1 \ (11) \ [0 \ (31)]$

$n^2 - n - 1 = 0$ → $n = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$

mod 11

n	n^2
0	0
1	1
2	4
3	9
4	5

mod 11 "$\sqrt{5} \equiv \pm 4$"

$n \equiv \frac{1 \pm 4}{2} \equiv (1 \pm 4)6$ → 30, → -18

5	3
$-5 \equiv 6$	3
7	5
8	9
9	4
10	1
11	0

$n \equiv 8, 4 \quad (11)$

mod 31 $\quad \pm 6 \equiv \sqrt{5}$ mod 31

$\frac{1}{2} \equiv 16 \mod 31$

$n \equiv (1 \pm 6) \cdot 16 \quad (31)$

2) $3^x + 4^y = 5^z$

mod 3 $\rightarrow$ z pari

mod 4 $\rightarrow$ x pari

$z = 2b \quad x = 2a$

$4^y = 5^{2b} - 3^{2a} = (5^b + 3^a)(5^b - 3^a)$

distano $2 \cdot 3^a$

$\Rightarrow \begin{cases} 5^b + 3^a = 2^h \\ 5^b - 3^a = 2^k = 2 \end{cases}$

$MCD(2^q, 2^k) = 2$

$5^b = 3^a + 2 \qquad 2 \cdot 3^a + 2 = 2^h$

$3^a + 1 = 2^{h-1}$

$3^a - 2^{h-1} = -1$

$h-1$ pari

$2^{h-1} - 1$

$$\begin{cases} 5^b + 3^a = 2^q \\ 5^b - 3^a = 2 \end{cases}$$

$$2 \cdot 5^b = 2^q + 2$$

$$5^b = 2^{q-1} + 1$$