Stage di CAMPOBASSO - 2012.

Titolo nota 23/02/2012

1. Aritmetica

1 non è primo.

2, 3, 5, 7, 11, 13, 17, 19, 23

2012	2
1006	2
503	503
1	

$2012 = 2^2 \cdot 503$

Divisibilità per 2 $\Leftrightarrow$ finisce con 2, 4, 6, 8, 0

Divisibilità per 5 $\Leftrightarrow$ finisce con 0, 5

Divisibilità per 4 $\Leftrightarrow$ finisce con un mult. di 4 (le 2 cifre)

28 256 716

Divisibilità per 10, 100, 1000, ... $\Leftrightarrow$ termina con 1, 2, 3, ... zeri.

---

a è un numero tra 0 e 99

100k + a NUMERI CHE TERMINANO PER a

$$\frac{100k+a}{4} = 25k + \frac{a}{4}$$

↑ $\frac{a}{4}$

E' INTERO $\Leftrightarrow$ a E' DIV. per 4

TROVARE TUTTI I QUADRATI TRA 0 e 2012^{2012}

CHE FINISCONO PER 26.

se $n^2 = 100k + 26$

allora 2 DIVIDE n^2

ma 4 NON DIVIDE n^2

e questo è ASSURDO.

$12 = 2^2 \cdot 3$

$12 \cdot 3 = 36 = 6^2$

$100k + 27 = n^2$

Oss: Divisibilità per 2

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14

Divisibilità per 7

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14

×	P	D
P	P	P
D	P	D

×	M	N
M	M	M
N	M	N

+	P	D
P	P	D
D	D	P

+	M	N
M	M	N
N	N	?

QUANDO a, b (NON MULTIPLI DI 3) HANNO $a+b$ MULTIPLO DI 3?

$$\frac{a+b}{3} = \frac{a}{3} + \frac{b}{3} = \frac{3\cdot k + r}{3} + \frac{3h+s}{3} =$$

$$= k + \frac{r}{3} + h + \frac{s}{3} = k+h+\frac{r+s}{3}$$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

0	1	2	3	4	5	6
D	L	Π	Π	G	V	S

↑

$6 + 18$

$=$

$2 \cdot 7 + 4$

$6 + 4 = 10 = 7 + 3$

a CONGRUO A b MODULO m

se 1.) m DIVIDE $a - b$

2.) $a = Km + b$

3.) a, b HANNO LO STESSO RESTO SE DIVISI PER m

1) $\Rightarrow$ $a - b = Km \Rightarrow a = km + b$ 2)

2) $\frac{a}{m} = \frac{Km + b}{m} = k + \frac{b}{m} \Rightarrow$ STESSO RESTO 3)

3) se HANNO LO STESSO RESTO, allora $a - b$ HA RESTO 0 1)

$$a \equiv b \mod m$$

ED: $2 \equiv 16 \mod 7$

$22 \equiv 71 \mod 7$ $+$

$24 \equiv 87 \mod 7$ $=$??

$a \equiv b \mod m$

$c \equiv d \mod m$

$\Rightarrow$) $a+c \equiv b+d \mod m$

) $a-c \equiv b-d \mod m$

) $ac \equiv bd \mod m$

$$2012^{2012} + 2011^{2011}$$

$2012 \equiv 2 \mod 3$

$2011 \equiv 1 \mod 3$

$2012^2 \equiv 2012 \cdot 2012 \equiv$

$\equiv 1 \pmod 3$

$2012^3 \equiv 2012^2 \cdot 2012 \equiv$

$\equiv 1 \cdot 2 \equiv 2 \mod 3$

$2012^{2012} \equiv 1 \mod 3$

$2011^{2011} \equiv (1)^{2011} \equiv 1 \mod 3$

$\Rightarrow$ NO, È CONGRUO A 2 mod 3

a) $2^7 + 3^7 + 5^7 \mod 7$

b) $500^{500} + 200^{200} \mod 11$

c) $1 + 7^4 + 49^4 + 9^4 + 81^4 \mod 5$

a) $2^7 + 5^7 = (2+5)(\ldots) = 7 \cdot (\ldots)$

$\Rightarrow 2^7 + 5^7 \equiv 0 \mod 7$

$a^3 + b^3 = (a+b)(\_\_\_\_)$

$a^5 + b^5 = (a+b)(\_\_\_\_\_)$

$a^7 + b^7 = (a+b)(\ldots\ldots\ldots)$

	0	1	2	3	4	5	6	7
3^7	1,	3,	2,	6,	4,	5,	1,	3

$\Rightarrow 2^7 + 5^7 + 3^7 \equiv 3 \mod 7$

	0	1	2	3	4	5	6	7	8
2^7	1,	2,	4,	1,	2,	4,	1,	2,	4
5^7	1,	5,	4,	6,	2,	3,	1,	5	

b) $500^{500} + 200^{200} \mod 11$

$5^{500} + 2^{200} \mod 11$

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

$$(5^{500}) \equiv (5^5)^{100} \equiv 1^{100} \mod 11$$

n	0	1	2	3	4	5	6	7	8	9	10
2^n	1,	2,	4,	8,	5,	10,	9,	7,	3,	6,	1

$$2^{200} \equiv (2^{10})^{20} \equiv 1^{20} \equiv 1 \mod 11$$

$$500^{500} + 200^{200} \equiv 2 \mod 11$$

c) $1 + 7^4 + 49^4 + 9^4 + 81^4 \mod 5$

$$1 + 1 + 1 + 1 + 1 \equiv 0 \mod 5$$

n	0	1	2	3	4
7^n	1,	7,	4,	3,	1

$\mod 5$

$$49^4 = (7^2)^4 = (7^4)^2 \equiv 1^2 \mod 5$$

$$9 \equiv 4 \equiv -1 \mod 5 \qquad 81^4$$

$$9^4 \equiv (-1)^4 \equiv 1 \mod 5$$

$$2x \equiv 3 \mod 23$$

$$2x - 3 \equiv 0 \mod 23$$

$$2x \equiv 3 \mod 23$$

$$12 \cdot 2x \equiv 12 \cdot 3 \mod 23$$

$\downarrow$

$x \equiv 13 \mod 23$

$23k + 13$ k intero

$2x \equiv 19 \mod 23$

$x \equiv 12 \cdot 19$

$x \equiv 228 \equiv 21 \mod 23$

"$\frac{1}{3}$" $\longrightarrow 5$

Es: $3x \equiv 4 \mod 7$ $\quad x \equiv 20 \equiv 6 \mod 7$

"$\frac{1}{5}$" $\longrightarrow 9$

$5x \equiv 2 \mod 11$ $\quad x \equiv 2 \cdot 9 \equiv 7 \mod 11$

$7x \equiv 8 \mod 13$ $\quad x \equiv 16 \equiv 3 \mod 13$

$2 \cdot 7 = 14$

Fatto: SE IL MODULO E' PRIMO, OGNI NUMERO $\not\equiv 0$ HA UN INVERSO.

SE IL MODULO NON E' PRIMO, HANNO UN INVERSO SOLO I NUMERI COPRIMI CON IL MODULO.

↳ RELATIVAMENTE PRIMI

↳ SENZA FATTORI COMUNI

$2^n \mod 7$

1, 2, 4, 1, 2, 4, 1, 2, 4

$$2^{3007} \equiv 2^1 \mod 7$$

$3^n \mod 7$

1, 3, 2, 6, 4, 5, 1

6

$3004 = 6 \cdot 500 + 4$

$3^{3004} = (3^6)^{500} \cdot 3^4$

$$3^{3004} \equiv 3^4 \mod 7$$

PICCOLO TEO di FERMAT

Teo: SE p è PRIMO e a NON è DIV. per p

allora $$a^{p-1} \equiv 1 \mod p.$$

Cor: Se p è PRIMO

allora: $$a^p \equiv a \mod p$$

$x^5 + 11y = 3$ (??)

$y = \frac{3 - x^5}{11}$ $\quad 3 - x^5 \equiv 0 \mod 11$

So che $x^{10} \equiv 1 \mod 11$ se 11 non divide x.

$(x^5)^2 \equiv 1 \mod 11 \qquad z^2 \equiv 1 \mod 11$

Voglio che 11 divida $z^2 - 1 = (z+1)(z-1)$

$\Rightarrow$ 11 divide $z+1 \qquad z \equiv -1 \equiv 10 \mod 11$

oppure

11 divide $z-1 \qquad z \equiv 1 \mod 11$

$\Rightarrow x^5 \equiv \begin{cases} 1 \\ -1 \\ 0 \end{cases} \mod 11 \Rightarrow 3 - x^5 \equiv \begin{cases} 2 \\ 4 \\ 3 \end{cases} \mod 11$

$\Rightarrow$ l'eq. è impossibile.

Es: $x^3 + y^3 = 7004$

$z = x^3 \qquad z^2 = x^6 \equiv 1 \quad (7)$

$z^2 - 1 \equiv 0 \mod 7$

7 divide $(z+1)(z-1) \Rightarrow \begin{cases} z \equiv -1 \\ z \equiv 1 \end{cases} \mod 7$

$x^3 \equiv \begin{cases} 1 \\ -1 \\ 0 \end{cases} \qquad y^3 \equiv \begin{cases} 1 \\ -1 \\ 0 \end{cases} \qquad x^3 + y^3 \equiv \begin{cases} 2 \\ 1 \\ 0 \\ -1 \\ -2 \end{cases} \qquad 7004 \equiv 4 \mod 7$

$$100k + 27 = n^2$$

$\downarrow$ $\quad$ $\downarrow$

$0 \quad 3 \pmod 4$

$$n^2 \equiv 3 \pmod 4$$

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

non c'è nessun quadrato che ha resto 3.