TEORIA DEI NUMERI

Titolo nota 14/02/2014

$5p+49$

→ Fattorizzazione

→ divisibilità

Problema

$$5p+49 = n^2 \qquad 5p = n^2-49 = (n+7)(n-7)$$

1	-1
5	-5
p	-p
5p	-5p

$n-7$	$n+7$			
1	5p	⇝	$n=8$,	$5p=15$ ⇝ $\boxed{p=3}$
5	p	⇝	$n=12$	$\boxed{p=19}$
p	5	⇝	$n-2$	$p=-9$
5p	1	⇝	$n=-6$	negativo si mono

(negativi) (+4)

$a \mid b$ "a divide b" $3 \mid 18$

$3 \mid 6$ $\quad 6 \mid 18 \Rightarrow 3 \mid 18$

$a \mid b$ $\quad b \mid a \Rightarrow a = \pm b$

$3|a \quad 3|b \quad 3|a+b \quad 3|a+57b$

$3|a-b$

$4 \overset{?}{|} 2014 \iff 4 \mid 2914 - 2000$

$d|a \quad d|b \Rightarrow d|a+b$

$\mcd(b, b^2+1) = 1$

$d|b \quad d \mid b^2+1 \Rightarrow d \mid b^2+1-b\cdot b = 1$

$\mcd(a,b) = 1$

$\mcd(a+b, a^2+b^2) = \begin{cases} 1 \\ 2 \end{cases}$

$= \mcd(a+b, a^2+b^2-(a+b)(a-b)) =$

$= \mcd(a+b, a^2+b^2-a^2+b^2) = \mcd(a+b, 2b^2)$

$d|a+b \quad d|2, \quad d|b^2$

$p \mid a+b$, $p \mid b^2$ $\quad p \mid b^2 \Rightarrow p \mid b$

$p \mid a+b$, $p \mid b$ $\Rightarrow$ $p \mid a$

... continua da sopra $\quad \mathrm{mcd}(a+b,\ 2b^2) = \mathrm{mcd}(a+b,\ 2)$

$\text{mostro}_1 + \text{mostro}_2 = \text{mostro}_3$

d divide $\qquad$ d divide

$\Rightarrow$ d divide anche mostro_2

ES: $3x^2 - 2y^2 = 1998$

$y = 3 \cdot z$

$3x^2 - 2 \cdot 9z^2 = 1998$ $\qquad$ (3, 666)

$x^2 - 6z^2 = 666$ $\qquad x = 6w$

$36w^2 - 6z^2 = 666$ $\qquad$ (6, 1, 111)

$6w^2 - z^2 = 111$ $\qquad$ (2, 3, 37)

$6w^2 - 9v^2 = 111$

$2w^2 - 3v^2 = 37$ serve un'altra idea

$d = \text{mcd}(78, 385)$

$$\underbrace{a \cdot 78}_{d} - \underbrace{b \cdot 385}_{d} = 1$$

$\text{mcd}(2003, 3002)$

$$3 \cdot 2003 - 2 \cdot 3002 = 5$$

Teo: se $\text{mcd}(p, q) = d$, allora riesco a trovare Teorema di Bézout

$$ap - bq = d$$

$\text{mcd}(91, 21) = \text{mcd}(91 - 4 \cdot 21, 21) = \text{mcd}(7, 21) =$

$= \text{mcd}(21 - 3 \cdot 7, 7) = \text{mcd}(0, 7)$

$91 : 21 = 4$

$91 = 4 \cdot 21 + 7$

Algoritmo di Euclide

Che giorno della settimana sarà il 25 Aprile 2023?

14/2/2014 Venerdì

+15	1° Marzo 2014
+31	1° Aprile 2014
+24	25 Aprile 2014
+9·365+2	25 Aprile 2023

$15+31+24+9\cdot365+2$ giorni ⊛

$\quad\|\quad\|\quad\|\quad\|$

$14+1 \quad 28+3 \quad 3 \quad (7+2)\cdot365 = 7\cdot365+2\cdot365 =$

$2(7\cdot52+1)$

⊛ ha lo stesso resto nella divisione per 7 di

$1+3+3+2\cdot1+2=4$ Martedì

Congruenze $a \equiv b \pmod m$ vuol dire "a ha lo stesso resto di b nella divisione per m"

$\Updownarrow$ $10 \equiv 24 \pmod 7$ $24-10$ è multiplo di 7

Alternativamente: $m \mid b-a$

Cose comode:

(*)
$$\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d \pmod m \\ a \cdot c \equiv b \cdot d \pmod m \end{cases}$$

$$8^{350} + 9 \cdot 6^{15} \equiv 1 + 2 \cdot (-1) \equiv -1 \pmod 7$$

8^{350}: $8 \equiv 1$, $8 \cdot 8 \cdot 8 \cdot \dots \cdot 8 \equiv 1 \cdot 1 \cdot 1 \cdot \dots \cdot 1 = 1$

$9 \equiv 2$

$6^{15} \equiv (-1) \cdot (-1) \cdot \dots \cdot (-1) = -1$

no

$5^{15} \equiv 5^{1} \pmod 7$

$$\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d \pmod m \\ a \cdot c \equiv b \cdot d \pmod m \end{cases}$$

$m \mid b-a$

$m \mid d-c$

$m \mid (a+c)-(b+d)$ $\quad$ $m \mid (b-a)+(d-c)$

Tesi: $m \mid b\cdot d - a\cdot c$

$$b\cdot d - a\cdot c = b\cdot d - b\cdot c + b\cdot c - a\cdot c =$$

$$= \underbrace{b(d-c)}_{\text{mult. di } m} + \underbrace{c(b-a)}_{\text{mult. di } m}$$

D + D = P

D : resto 1 nella div. 2 $\equiv 1 \pmod 2$

P : resto 0

$$1+1 \equiv 2 \equiv 0 \pmod 2$$

$$3795268 \cdot 3986213 \equiv 8\cdot 3 \pmod{10}$$

$3795268 \equiv 8$, $3986213 \equiv 3$

$3 \mid \underbrace{abcde} \iff 3 \mid a+b+c+d+e$

$$10^4\cdot a + 10^3\cdot b + 10^2\cdot c + 10\cdot d + e \equiv a+b+c+d+e$$

($10^4 \equiv 1^4$, $10^3 \equiv 1^3$, $10^2 \equiv 1^2$, $10 \equiv 1$)

mod 9 stessa cosa

mod 11

$7 \mid 3582 \iff 7 \mid 358 - 2 \cdot 2 \iff 7 \mid 354 \iff 7 \mid 35 - 24$

(esercizio: dimostrare che funziona)

$14 \equiv 4 \pmod{10}$

$7 \not\equiv 2$

$10 \mid 14 - 4 = 2(7-2)$

$\not\Downarrow$

$10 \mid 7 - 2$

Quando posso semplificare?

solo se $\mathrm{mcd}(k, m) = 1$

$ka \equiv kb \pmod{m}$ (*)

$\Downarrow$

$a \equiv b \pmod{m}$

$21 \equiv 51 \pmod{10}$

$\Downarrow$

$7 \equiv 17$

(*) dim: $m \mid ka - kb$ $\quad m \mid k(a-b)$

$20000000\ldots00014$ è un quadrato perfetto?

Cosa succede ai quadrati mod 4?

$a \equiv$ 0, 1, 2, 3

$a \cdot a \equiv$ $0 \cdot 0 \equiv 0$, $1 \cdot 1 \equiv 1$, $2 \cdot 2 \equiv 0$, $3 \cdot 3 \equiv 1$

Tutti i quadrati perfetti sono $\equiv$ a 0 oppure 1 modulo 4

Allora $20000\ldots014 \equiv 2$ non è un quadrato

$2w^2 - 3v^2 = 37$

guarda mod 3:

$2w^2 - 3v^2 \equiv 37 \pmod 3$

$2w^2 \equiv 1 \pmod 3$

$w \equiv$ 0, 1, -1

w^2: $0 \cdot 0 \equiv 0$, $1 \cdot 1 \equiv 1$, $(-1)\cdot(-1) \equiv 1$

impossibile

$2 \cdot w^2$: $2 \cdot 0 \equiv 0$, $2 \cdot 1 \equiv 2$, $2 \cdot 1 \equiv 2$

3, 4, 5, 8, 9 → provare moduli piccoli

→ provare moduli che "fanno sperire un pezzo"

quadrati mod 8 fanno $\begin{cases} 0 \\ 1 \\ 4 \end{cases}$

Potenze e moduli mod 7

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	...
0	X	0	0	0	0	0	0	0	0	0	0	...
1	1	1	1	1	1	1	1	1	1	1	1	
2	1	2	4	1	2	4	1	2	4	1	2	...
3	1	3	2	6	4	5	1	3	2	6	4	...
4	1	4	2	1	4	2	1	4	2	1		...
5	1	5	4	6	2	3	1	5	4	6	2	...
$-1 \equiv 6$	1	6	1	6	1	6	1	6	1	6	1	...
7	1	0	0	0	0							
8	1	1	1	1								
9	1	2	4	1	2	4	1	2	4			
⋮												

si ripete quello sotto

$2^4 \equiv 2^3 \cdot 2^1 \equiv 2^1 \equiv 2$

$2^5 \equiv 2^3 \cdot 2^2 \equiv 4$

$4^2 \equiv 2$

$4^3 \equiv 4^2 \cdot 4 \equiv 2 \cdot 4 \equiv 1$

Le potenze si ripetono ogni 6!

$$59 \equiv \dots \pmod 7$$

$$59 \equiv 3^{59} \equiv 3^5 \equiv \boxed{5}$$

Teo: (Fermat) Se p è primo, allora $a^p \equiv a \pmod p$ per tutti gli a

Teo: p primo, i quadrati prendono $\frac{p+1}{2}$

Tutti i "periodi" delle potenze (es: le potenze di 2 hanno periodo 3, le potenze di 6 hanno periodo 2 mod 7) sono divisori di $p-1$

Es: esistono due quadrati la cui differenza fa 2014?

$$m^2 - n^2 = 2014$$

$$(m+n)(m-n)$$ vediamo modulo qualcosa

mod 4: $m^2 \equiv \begin{cases} 0 \\ 1 \end{cases}$ $n^2 \begin{cases} 0 \\ 1 \end{cases}$

$$m^2 - n^2 \equiv \begin{cases} m^2 \equiv 0 \quad n^2 \equiv 0 \rightsquigarrow m^2 - n^2 \equiv 0 \\ m^2 \equiv 0 \quad n^2 \equiv 1 \rightsquigarrow m^2 - n^2 \equiv -1 \\ m^2 \equiv 1 \quad n^2 \equiv 0 \rightsquigarrow m^2 - n^2 \equiv 1 \\ m^2 \equiv 1 \quad n^2 \equiv 1 \rightsquigarrow m^2 - n^2 \equiv 0 \end{cases}$$

$$m^2 - n^2 = 2013$$

$$(m+n)(m-n) = 2013 = 3 \cdot 11 \cdot 61$$

$m-n$	$m+n$
1	$3\cdot11\cdot61$
3	$11\cdot61$
11	$3\cdot61$
61	$3\cdot11$
33	⋮
$3\cdot61$	⋮
$11\cdot61$	
$3\cdot11\cdot61$	
-1	
-3	
-11	
⋮	

8 div. positivi

$$\begin{cases} m-n=11 \\ m+n=3\cdot61 \end{cases}$$

$$2m = 11+3\cdot61 \qquad m=\frac{11+3\cdot61}{2}$$

$$2n = 3\cdot61-11 \qquad n=\frac{3\cdot61-11}{2}$$

→ In ognuno di questi casi fa $D \pm D$ e m, n vengono interi (potrebbero venire negativi)

Ognuno dei 16 casi porta a una soluzione (distinta)

$m^2-n^2=2015$ è uguale, bisogna fattorizzare 2015 è tutto dispari lo stesso

$$(n+1)^2-n^2 = 2n+1$$

$$(1008)^2-(1007)^2 = 2015$$

$n=1007$

$(1007)^2-(1006)^2$

Quanti divisori (positivi) (inclusi 1 e lui stesso) ha $N=2^{15}3^{18}5^{16}$?

Per ogni $0 \le a \le 15$, $0 \le b \le 18$, $0 \le c \le 16$

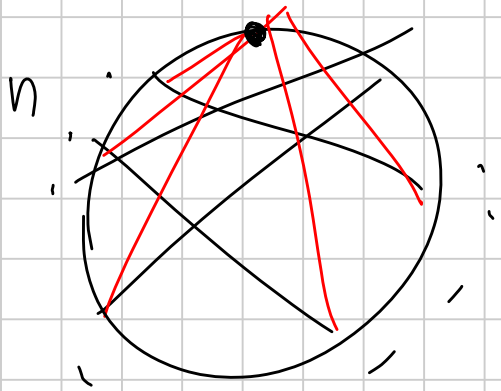
$$2^a 3^b 5^c \mid N$$

16 scelte per a
19 per b
17 per c

$16 \cdot 19 \cdot 17$

In generale $N = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}$ (p_k primi distinti)

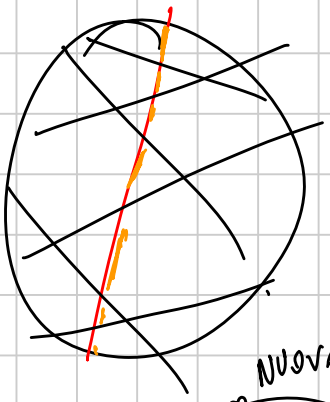
ha $(a_1+1)(a_2+1)\cdots(a_k+1)$

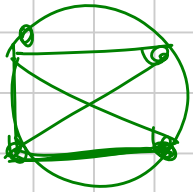


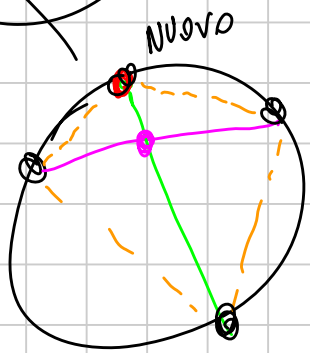
Aggiungo 1 punto a n già presenti

Aggiungo n nuovi segmenti

Ogni ~~nuovo segmento incontra tutti gli~~ $\binom{n}{2}$ ~~segmenti~~ che c'erano prima

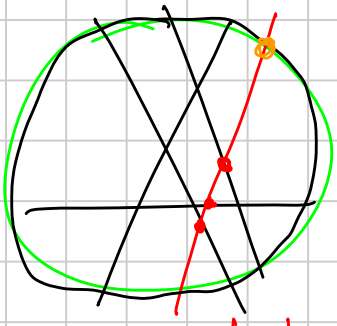






Scelgo 1 nuovo e 3 vecchi

Creo $\binom{n}{3}$ nuovi punti di intersez.



k intersezioni $\Rightarrow$ $k+1$ nuove regioni

una per segmento + 1 per intersezione

$$A_{n+1} - A_n = \binom{n}{3} + n = \text{polinomio di grado } 3 \text{ in } n$$

$$p(n+1) - p(n) = \text{grado } d-1$$

$$p(x) = a_n \binom{x}{0} + a_{n-1} \binom{x}{1} + a_{n-2} \binom{x}{2} + \dots + a_0 \binom{x}{n}$$

$$\binom{x+1}{n} - \binom{x}{n} = \binom{x}{n-1}$$

$$ax^4+bx^3+cx^2+dx+e = p(x)$$

$$\begin{cases} p(1) \\ p(2) \\ p(3) \\ p(4) \\ p(5) \\ \vdots \end{cases}$$

Partite da 1, 2, 3, 4, 5

$$m^2 - n^2 = \boxed{2012}$$

$2012 = 2 \cdot 2 \cdot \underbrace{503}_{\text{primo!}}$

---

① $p+1 = n^3$ $\qquad p = n^3 - 1 = (n-1)(n^2+n+1)$

(A)	1	p
(B)	p	1
	-1	$-p$ (se $n \geq 0$)
	$-p$	-1 ($n^2+n+1 \geq 0$)

(A): $\begin{cases} n-1 = 1 \\ n^2+n+1 = p \end{cases}$ $\quad n=2$ $\quad \boxed{p=7}$

(B) $\begin{cases} n-1 = p \\ n^2+n+1 = 1 \end{cases}$ $\Leftrightarrow$ $n < 0$ $\quad p=-1$ entrambe p non acc.

$\frac{15n+2}{20n+3}$ È sempre vero che

$$\mathrm{mcd}(15n+2, 20n+3) = 1 ?$$

Se trovassi a, b tali che

$$a(15n+2) - b(20n+3) = 1$$

allora avrei vinto

$a=4, b=3$ $\quad -4(15n+2) + 3(20n+3) = -8+9 = +1$

$n = 2014$

$$\mathrm{mcd}(n+1,\ n^{16}+1) =$$

$$= \mathrm{mcd}(n+1,\ n^{16}+1 - \underbrace{(\dots)}_{n^{16}-1}(n+1)) \quad (*)$$

È vero che $n^{16}-1$ è multiplo di $n+1$?

$$n^{16}-1 = (n^8+1)(n^8-1) = (n^8+1)(n^4+1)(n^4-1) =$$

$$\dots (n^8+1)(n^4+1)(n^2+1)(n+1)(n-1)$$

$$(*) = \mathrm{mcd}(n+1,\ n^{16}+1-(n^{16}-1)) = \mathrm{mcd}(n+1, 2)$$

$n = 2014$

$6^{54} \equiv ?$ mod $2, 3, 5, 7$

mod 2: $6^{54} \equiv 0^{54} \equiv 0 \equiv 2$

mod 3: $6^{54} \equiv 0^{54} \equiv 0 \equiv 3$

mod 5: $6^{54} \equiv 1^{54} \equiv 1$

mod 7 $6^{54} \equiv (-1)^{54} \equiv 1$

anche: sappiamo che $x^6 \equiv 1$ per ogni $x \not\equiv 0$

$6^{54} \equiv (6^6)^9 \equiv 1^9 \equiv 1$

$2012 = 2 \cdot 2 \cdot 503$

$m^2 - n^2 = 2012$

$(m+n)(m-n) = 2 \cdot 2 \cdot 503$

$2^{(2)} \cdot 503^{(1)}$

ha $(2+1)(1+1) = 6$ div. positivi

$m-n$	$m+n$	
1	$4 \cdot 503$	no!
2	$2 \cdot 503$	✗
4	503	
503	4	
$2 \cdot 503$	2	✗
$4 \cdot 503$	1	
-1		
-2	$-2 \cdot 503$	✗
-4		
-503		
$-2 \cdot 503$	-2	✗
$-4 \cdot 503$		

$$\begin{cases} m-n = a \\ m+n = b \end{cases} \Rightarrow \begin{cases} m = \frac{a+b}{2} \\ n = \frac{b-a}{2} \end{cases}$$

$$\begin{cases} m-n = 1 \\ m+n = 4 \cdot 503 \end{cases}$$

$m = \frac{4 \cdot 503 + 1}{2}$ ✗ ops! non intero

$n = \frac{4 \cdot 503 - 1}{2}$

solo 4 soluzioni

Quanti sono le sol. di $\longrightarrow$

$\longrightarrow$ $m^2 - n^2 = 2^{15} 3^{16}$?

$$\begin{cases} m-n = d \\ m+n = \dfrac{2^{15}3^{16}}{d} \end{cases}$$

Ognuno accettabile a patto che siano entrambi pari

divisori di $2^{15}3^{16}$: $2^a 3^b$

$0 \le a \le 15 \quad 0 \le b \le 16$

divisori di $2^{15}3^{16}$ che vanno bene?

$0 < a < 15 \quad 0 \le b \le 16$

occhio

divisori negativi $2 \cdot 14 \cdot 17$ soluzioni

E se voglio solo $m \ge 0, \ n \ge 0$?

Le soluzioni vengono a quadruple

$$\begin{cases} m, n \\ -m, -n \\ -m, n \\ -n, m \end{cases}$$

Tutte? Quasi!

ci sono quelle con $m=0$ oppure $n=0$

$$\begin{cases} m^2 = 2^{15}3^{16} \\ -n^2 = 2^{15}3^{16} \end{cases}$$

ma non è un quadrato...

Quali sono i numeri che hanno un numero dispari di divisori?
(positivi)

$$N = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

$$\#\text{divisori} = (a_1+1)(a_2+1)(a_3+1)\cdots(a_k+1)$$

tutti i fattori devono essere dispari

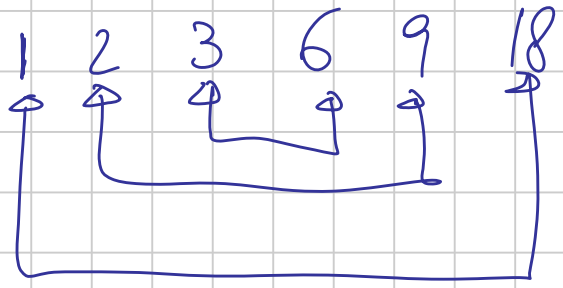
$\Rightarrow$ tutti gli a_i devono essere pari

$\Rightarrow$ N quadrato perfetto

N Accoppio i divisori:

$d \longleftrightarrow \frac{n}{d}$

18



solo!