Teoria dei Numeri 1

Note Title 9/3/2016

Kirill Kuzmin

$-3, -2, -1, 0, 1, 2, 3, \ldots$

negativi

positivi

non negativi

$b \geq 2$ Si possono scrivere in base b

$$2016 = 2 \cdot 1008 =$$

$$= 2 \cdot 2 \cdot 504 = 2 \cdot 2 \cdot 2 \cdot 252 =$$

$$= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 126 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 63 =$$

$$= 2^5 \cdot 3^2 \cdot 7$$

I numeri come 2, 3, 5, 7, 11 etc. che non sono rappresentabili come prodotto di numeri più piccoli sono detti "primi"

I numeri primi sono infiniti

a, b interi $a \mid b$ se $b = k \cdot a$

" "a divide b"

Primi: > 1 che hanno come divisori positivi solo 1 e se stesso.

Ogni numero si può scrivere come prodotto di primi IN MODO UNICO

$2016 = 2^5 \cdot 3^2 \cdot 7$ $\quad 2015 = 5 \cdot 13 \cdot 31$

2017 è primo

Altro modo di definire i primi

Esempio: mn pari, allora m pari oppure n pari

$2 \mid mn$, allora $2 \mid m$ o $2 \mid n$

Questo vale per ogni primo p:

$p \mid mn$ allora $p \mid m$ o $p \mid n$

$10 \mid 4 \cdot 25$ ma $10 \nmid 4$ e $10 \nmid 25$

10 non è primo.

$1 \mid$ intero $\quad$ intero $\mid 0$

$2 \mid 2016$

$2^5 \| 2016$ ← divide esattamente

$\downarrow$

① $2^5 \mid 2016$

$2^6 \nmid 2016$

$10 \nmid 2016$

a, b interi $\quad b > 0$

$a = 2016 \quad b = 10$

$a = qb + r$ — resto $2016 = 0 \cdot 10 + 2016$

$q = 0 \quad r = a$

c'è un'unica scrittura per cui $0 \le r \le b-1$

$$2016 = 201 \cdot 10 + 6$$

Divisione euclidea

Resto

Quando $b \mid a$? Quando il resto è 0

Massimo Comun Divisore

$d = MCD(a,b) = (a,b)$

$a = 102$
$b = 30$

$d \mid a \qquad d \mid b$

Massimo: se $c \mid a$, $c \mid b$, allora $c \mid d$

$MCD(102,30) = 6$

$MCD(a,b) = MCD(a+b,b) = MCD(a-b,b)$

$a = bq + r$ divisione euclidea

$= MCD(b,r)$

Come si calcola
Modo 1: Fattori primi in comune
Modo 2: Algoritmo di Euclide

a	b	
102	30	
1	0	102
0	1	30
1	−3	12
−2	7	6
5	−17	0

$102 = 3 \cdot 30 + 12$

$12 = 102 - 3 \cdot 30$

$30 = 2 \cdot 12 + 6$

$6 = 30 - 2 \cdot 12$

$6 = -2 \cdot 102 + 7 \cdot 30$

Teorema di Bézout

$MCD(a,b) = ha + kb$

Come ottenere le altre coppie?

$$MCD(a,b) = ha + kb = ha + kb + n\frac{ab}{MCD(ab)} - n\frac{ab}{MCD(a,b)}$$

$$= \left(h + n\frac{b}{(a,b)}\right)a + \left(k - n\frac{a}{(a,b)}\right)b$$

$$G = (-2 + n\cdot 5)102 + (7 - n\cdot 17)30$$

Quando $MCD(a,b) = 1$ ↔ primi tra loro, coprimi, relativamente primi

Succede quando non hanno fattori primi in comune

$a = 3 \quad b = 5 \qquad 1 = 2\cdot 3 + (-1)\cdot 5$

Diofantee (dovete cercare soluzioni intere)

$\longrightarrow x\cdot 3 + y\cdot 5 = 2016$

$(2 - n\cdot 5)3 + (-1 + n\cdot 3)5 = 1$

$x = 2016(2 - n\cdot 5) \qquad y = 2016(-1 + n\cdot 3)$

n intero qualunque

$x\cdot 102 + y\cdot 30 = 9$

$x\cdot 102 + y\cdot 30 = 4$

In generale $ax+by=c$ ha soluzione se e solo se $MCD(a,b) \mid c$

$$x^2 - y^2 = 9$$

$$(x+y)(x-y) = 9 = 3^2$$

$x+y$	$x-y$
9	1 →
3	3
1	9
-1	-9
-3	-3
-9	-1

$x+y=9$
$x-y=1$ OK
$x=5$
$y=4$

$$x^2 - y^2 = 14$$

$$(x+y)-(x-y) = 2y$$

$$14 = (x+y)(x-y)$$

$x+y$	$x-y$	
14	1 →	$x=7{,}5$ $y=6{,}5$
7	2 →	No NO!
⋮	⋮	

In generale un numero 2 dispari NON si può scrivere come differenza di quadrati

---

$$xy + x + y + 1 = 11 + 1$$

$$(x+1)(y+1) = 12 = 2^2 \cdot 3$$

$$xy + x + y + 1 = 12$$

$x+1$	$y+1$	
12	1 →	$x=11$ $y=0$
6	2 →	$x=5$ $y=1$
⋮	⋮	

$xy + x + y = 11$

$xy + x = 11 - y$

$x(y+1) = 11 - y$

$x = \boxed{\frac{11-y}{y+1}}$ → quando è intero?

$\frac{-y+11}{y+1} = \frac{-y-1+12}{y+1} = -1 + \boxed{\frac{12}{y+1}}$

INTERO se e solo se intero, e questo sappiamo farlo

Congruenze

m intero ≥ 2

$a \equiv a' \pmod m$ se

"a è congruo ad a' modulo m"

$m \mid a - a'$ se e solo se a ed a' danno lo stesso resto divis: per m

Che giorno della settimana sarà il 3 settembre 2017?

domenica

sabato +1

$365 = 52 \cdot 7 + 1$

3 settembre 2015 era giovedì

sabato −2

$a \equiv a' \pmod m$

$b \equiv b' \pmod m$

Allora $a+b \equiv a'+b' \pmod m$

$a-b \equiv a'-b' \pmod m$

$ab \equiv a'b' \pmod m$

$(a+b) - (a'+b') = (a-a') + (b-b')$

$a-a'$: divisibile per m ; $b-b'$: divisibile per m

$ab - a'b' = ab - ab' + ab' - a'b' = a(b-b') + b'(a-a')$

$a(b-b')$: divisib per m ; $b'(a-a')$: divisib per m

$0, 1, \dots, m-1$

significa

numero $\equiv 0 \pmod 3$ divisibile per 3

$\equiv 1 \pmod 3$ dà resto 1 diviso per 3

Se so che $a \mid b$ e conosco i resti della divisione di a e di b per m riesco a trovare il resto di $\frac{b}{a}$?

Risposta: NON sempre

$m=2$ $6/2 = 3$ $8/2 = 4$

NON si può se $MCD(m,a) > 1$

Se $MCD(m,a) = 1$ sì

$m=5$ $36 : 3 = 12$ $36 = 3 \cdot 12$

mod 5: 1 3 $\boxed{2}$

$3 \cdot 2 = 6 \equiv 1 \pmod 5$

$1 = 2 \cdot 3 - 1 \cdot 5$

Trovare $\frac{b}{a}$ modulo m se $b \equiv 1 \pmod m$ e a è coprimo con m

$1 = ka + hm$

k è detto "inverso di a modulo m"

$a^{-1} \pmod m$

$27 : 3 \mod 5$ è

$2 \cdot (3^{-1} \pmod 5) \equiv 2 \cdot 2 \pmod 5 = 4$

---

modulo 4 $\quad 6/2 = 3 \quad 10/2 = 5 \equiv 1$

$a, a^2, a^3, \dots \pmod m$

$a, a^2, a^3, \dots, a^k, \dots, a^{k+h} \equiv a^k \pmod m$

$a^{k+h} \equiv a^k \pmod m$

$a^{k+h+1} \equiv a(a^{k+h}) \equiv a \cdot a^k \equiv a^{k+1} \pmod m$

$a^{k+h+2} \equiv a^{k+2} \pmod m$

Mod 24, potenze di 2

$2, 4, 8, 16, 8, 16, 8, \dots$

$3^{2016} \equiv 3^4 \equiv 1 \pmod{10}$

$3, 9, 7, 1, 3, 9, 7, 1$

perché $2016 \equiv 4 \pmod 4$ è il periodo delle potenze di 3 modulo 10

$a \bmod 3$	$a^2 \bmod 3$
0	0
1	1
2	1

$a \bmod 4$	$a^2 \bmod 4$
0	0
1	1
2	0
3	1

$x^2 - y^2$ non può essere 2 · dispari $\equiv 2 \pmod 4$

$0 - 0 \equiv 0$

$0 - 1 \equiv -1 \equiv 3$

$1 - 0 \equiv 1$

$1 - 1 \equiv 0$

$a^2 \bmod 5$ può essere solo $0, 1, -1 \equiv 4$

$a^4 \bmod 5$ può essere solo $0, 1$

$a^2 \bmod 8$ può essere solo $0, 4, 1$

$a^4 \bmod 16$ solo $0, 1$

$a^3 \bmod 7$ può essere solo $0, 1, -1 \equiv 6$

$a^3 \bmod 9$ $0, 1, -1 \equiv 8$

Base: 38, 40, 42, 51, a desiderio

Altri: 6, 8, 9, 10

$$7 = q_1^2 + q_2^2 + q_3^2$$

q_1, q_2, q_3 razionali

Soluzioni agli esercizi

38 Se $p \mid ab$ allora $p \mid a$ o $p \mid b$

VERO (DEF)

Se $p^2 \mid ab$ allora $p^2 \mid a$ oppure $p^2 \mid b$

NO: se $p \| a$ e $p \| b$ è Falso

$p \mid a-b$, allora $p \mid a+b$ Falso

vero se $p=2$

Se $p^2 \mid a^3$, allora $p^6 \mid a^6$

$p \mid p^2$ $p \mid a \cdot a \cdot a$ allora $p \mid a$ VERO

Se $p^2 \mid b^3$, allora $p^2 \mid b$ FALSO

$p \mid (a,b)$ $p \mid (a^2, ab)$

$= a \cdot (a,b)$ (ESERCIZIO)

VERO

$\frac{n+3}{n+1} = \frac{n+1+2}{n+1} = 1 + \frac{2}{n+1}$ Intero se $n+1 \mid 2$

$\frac{15-3n}{2n^2+1}$ $\frac{2n^2+1}{-3n+15} = (an+b) + \frac{c}{-3n+15}$

$n \leq -4$ } se succede questo, il VA del NUM
$n \geq 6$ } è più piccolo del VA del DEN

$n = -3, -2, \dots, 5$ Finiti casi, provare tutti

$|15 - 3n| \leq (2n^2+1)$

---

51 $\dots\dots\dots 02$

qualcosa $\cdot 100 + 2 = 2(qc \cdot 50 + 1)$ dispari

modulo 4: $0 + 2 \equiv 2$

$n = p_1^{h\alpha_1} \cdots p_k^{h\alpha_k}$ → NON è una potenza

---

6 $p^4 - q^4$ $p > q \geq 10$ primi

Sia M il MCD cercato

Sia r un primo >10

Perché $r \nmid M$? $p > r$ $q = r$

$p^4 - r^4$ non è divisibile per r

~~2, 3, 5, 7~~

13, 11 $13^4 - 11^4 \mod 7$

$(-1)^4$ $(-3)^4$

$1 - 4 \equiv -3$

$x^4 \mod 5$ può essere solo 1, ~~0~~

$p^4 - q^4$ ha un fattore 5

$(13^4 - 11^4) = (13^2 + 11^2)(13+11)(13-11)$

290 NO 5 NO 5

↑ un solo fattore 3

$5 \| M$

$p^4 - q^4$ $\qquad 3 \mid M$

$1 - 1 \equiv 0 \pmod 3$

$p^4 - q^4$ $\qquad 16 \mid M$

$1 - 1 \equiv 0 \pmod{16}$

$17^4 - 13^4 = (17^2 + 13^2)(17+13)(17-13)$

$30 \qquad 4$

un solo fattore 2, sempre

mod 4: $p^2 \equiv 1$, $q^2 \equiv 1$, $p^2 + q^2 \equiv 2$

3 fattori 2

$M = 2^4 \cdot 3 \cdot 5$

---

8 $\quad MCD(100 + n^2,\ 100 + (n+1)^2)$

$n > 0$ intero

$= MCD(100 + n^2,\ 2n + 1)$

Se $\quad a \mid 100 + n^2, \quad a \mid 2n + 1$

Allora $\quad a \mid 200 + 2n^2 \qquad a \mid 2n^2 + n$

e quindi $\quad a \mid n - 200, \quad a \mid 2n - 400$

e perciò $\quad a \mid 401$ $\qquad 401$ è primo

$401 \mid 2n + 1 \qquad n = 200$

$200^2 + 100 = 100(1 + 400)$ $\qquad$ OK

$(200+1)^2 + 100 = 100 + 200^2 + 2\cdot 200 + 1$

ok 401 ok

$y^2 = x^5 - 4$ Modulo 11

x^5 modulo 11 assume valori $0, 1, -1$

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

$x^5 - 4$ può fare solo $6, 7, 8$

NON esistono soluzioni modulo 11, e quindi nemmeno negli interi.

$7 = a_1^2 + a_2^2 + a_3^2$

$7d^2 = a^2 + b^2 + c^2$

$-d^2 \equiv a^2 + b^2 + c^2 \pmod 8$

0 Residui 1 quadratici 4 mod 8

0
-1
4

3 dispari: NO

$1 + 1 + 0$ 4 2 disp, 1 pari NO

1 dispari: NO

3 pari ok! e allora anche d è pari

$7(2d')^2 = (2a')^2 + (2b')^2 + (2c')^2$

dividi per 4

$7d'^2 = a'^2 + b'^2 + c'^2$

Continuo a dividere i numeri per 2

NO! per la discesa infinita

Si può fare anche senza stando attenti ai dati iniziali

---

(9) $f(0)=0 \quad f(1)=0 \quad f(2n)=2f(n)+1 \quad f(2n+1)=2f(n)$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
f(n)	0	0	1	0	3	2	1	0	7	6	5	4	3	2	1	0

0	1	10	11	100	101	110	111
0	0	1	0	11	10	01	00

$f(\_0\_1\_) = (\_\_1\_\_0\_\_)$

$f(2n) = f(\underbrace{1\ \text{stringa}}_{n \text{ in base } 2}\ 0) = 2(\overline{\text{stringa}}) + 1$

$\overline{\text{stringa}}\ 0 + 1$

ok

$\overline{\text{stringa}}\ 1$

$f(2n+1) = f(\underbrace{1\ \text{stringa}}_{n \text{ in base } 2}\ 1) = 2(\overline{\text{stringa}}) = \overline{\text{stringa}}\ 0$

Fatto 1: Ad ogni passaggio perdo ALMENO una cifra binaria

Questo basta per (2)

$a_{2002} = f^{2002}(m) = \underbrace{f(f(f\ldots f(m)\ldots))}_{2002 \text{ volte}}$ NOTAZIONE

NON SEMPRE $\sin^2(x) = (\sin x)^2$

ATTENZIONE ALLE NOTAZIONI !!!

$f^{2002}(m) = 0$

$f^{2001}(m) \neq 0$ ha almeno 1 cifra binaria

$f^{2000}(m)$ ha almeno 2 cifre binarie

m ha almeno 2002 cifre binarie

$m = 101010\_\_\_\_\_10$ (2002 cifre)

$r(m) = 10101\_\_\_\_\_01$

$r^2(m) = 1010\_\_\_\_\_10$

$10 = 2 \quad 1010 = 2^3+2 \quad 101010 = 2^5+2^3+2$

$m = 2^{2001} + 2^{1999} + \_\_\_ + 2^3 + 2 =$

$= 2\left(\sum_{i=0}^{1000} 2^{2i}\right) = 2 \cdot \frac{4^{1001}-1}{3}$