Teoria dei Numeri 1

Titolo nota 02/09/2013

Naturali = $\mathbb{N} = \{0, 1, 2, \dots\}$

Interi $\mathbb{Z}$ $\{\dots, -2, -1, 0, 1, 2, \dots\}$

Un intero a divide un intero b

(e si scrive $a \mid b$)

se esiste un intero k t.c. $b = ka$

Oss: $a \mid b \Rightarrow |a| \leq |b|$

$|b| = |k| \cdot |a| \geq |a|$

Fatto essenziale: $a \mid b$ $a \mid c$

$a \mid b \cdot c$ $a \mid b + c$

$a \mid k \cdot b$

Quindi $a \mid hb + kc$

Numero primo p è divisibile solo per $\pm 1, \pm p$ e non è ± 1

p è primo se e solo se $p \mid a \cdot b$
$\Rightarrow p \mid a$ oppure $p \mid b$

Supponiamo $a \mid p$, cioè $p = a \cdot b$
In particolare $p \mid a \cdot b$; WLOG
(= senza perdita di generalità) $p \mid a$

$|a| \leq |p| \leq |a| \Rightarrow a = \pm p$

Teorema fondamentale dell'Aritmetica

Ogni intero ≥ 2 si scrive in maniera unica come prodotto di primi (con ripetizioni)

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

$$m = q_1^{b_1} \cdot \cdots \cdot q_h^{b_h}$$

Quand'è che $m \mid n$?

1) Tutti i q_i devono dividere anche n

A meno dell'ordine, $p_1 = q_1, \dots, p_h = q_h$

2) $b_1 \le a_1, \dots, b_h \le a_h$ $\boxed{h \le k}$

Massimo comun divisore

Dati a, b interi, il massimo comun divisore - che si scrive (a,b) - è il più grande intero che divida entrambi

Algoritmo di Euclide

$d = (a,b)$

$c \mid a$ e $c \mid b \iff c \mid a$ e $c \mid a-b$

$$(144, 27) = (144-27, 27) = (144-27\cdot 2, 27)$$
$$= \dots = (9, 27) = (27 - 3\cdot 9, 9)$$
$$= (0, 9) = 9$$

Es. $(a^2+a+1, a+1) = 1$?

Coprimi

a, b sono coprimi se $(a,b) = 1$

$$(a^2+a+1, a+1) = (a^2+a+1 - a(a+1), a+1)$$
$$= (1, a+1) = 1$$

Identità di Bézout

Esiste sempre una scrittura di (a,b) come combinazione (a coeff. interi) di a e b

$$9 = 144h + 27k$$
$$h = 1, \quad k = -5$$

$$(44, 17) = 1$$

$$44 = 17 \cdot 2 + 10 \qquad (17, 10)$$
$$17 = 10 \cdot 1 + 7 \qquad (10, 7)$$
$$10 = 7 \cdot 1 + 3 \qquad (7, 3)$$
$$7 = 3 \cdot 2 + 1 \qquad (3, 1) = 1$$

$$1 = 7 - 3 \cdot 2 = 7 - 2 \cdot (10 - 7) =$$
$$= -2 \cdot 10 + 3 \cdot 7 = -2 \cdot 10 + 3 \cdot (17 - 10)$$
$$= 3 \cdot 17 - 5 \cdot 10 = 3 \cdot 17 - 5 \cdot (44 - 2 \cdot 17) =$$
$$= -5 \cdot 44 + 13 \cdot 17$$

Diofantee lineari in due variabili

$$44x + 17y = 5$$

$$44x - 72y = 5$$ ha grossi problemi ad avere soluzioni

$$44x + 17y = 1$$

$$44 \cdot (5x) + 17(5y) = 5$$

In generale $ax + by = c$, dove a, b, c sono interi fissati ed x, y le incognite hanno soluzioni se e solo se $(a,b) \mid c$

Ex Quali sono TUTTE le soluzioni?

Diofantee

$$3x^2 = 141y^5 + 5$$

$$3x^2 - 141y^5 = 5$$

$$\| \quad 3(x^2 - 47y^5)$$

No! Perché $3 \nmid 5$ (3 non divide 5)

Fattorizzazioni algebriche forniscono fattorizzazioni aritmetiche

$$x^2 - y^2 = 7$$

$$(x-y)(x+y) = 7 \longrightarrow x+y \mid 7$$

Wlog $x \geq 0$, $y \geq 0$

$$x+y = \begin{cases} 1 \\ 7 \end{cases} \quad \begin{matrix} \Rightarrow x-y = 7 \\ \Rightarrow x-y = 1 \end{matrix}$$

Soluzione $x = \pm 4$, $y = \pm 3$

$5p + 4q = n^2$, n intero e p primo

$$5p = (n+7)(n-7)$$

$\pm 1, \pm 5, \pm p, \pm 5p$

$n+7 = p$, $n-7 = 5$

$n+7 = 5p$, $n-7 = 1$

Ex $m^3 - n^3 = 7004 = 2^2 \cdot 17 \cdot 103$

Risolvere $p^x = x^y$

1) x è una potenza di p

$$x = p^a$$

2) $$p^{p^a} = p^{ay} \Rightarrow p^a = a \cdot y$$

3) $$a \mid p^a \Rightarrow a = p^b$$

$$p^{p^b} = p^b \cdot y \Rightarrow y = p^{p^b - b}$$

Ex $p^b - b \geq 0$ per ogni p primo, $b \geq 0$

Congruenze

Che giorno sarà fra 400 giorni?

$400 = 57 \cdot 7 + 1$

$400 \rightsquigarrow 50 \rightsquigarrow 1$

Def Diciamo che a e b sono congrui modulo n se lasciano lo stesso resto nella divisione per n

Si denota $a \equiv b \pmod{n}$

$a \equiv b \ (n)$

ed è equivalente a dire che $n \mid (a-b)$

$400 \equiv 50 \equiv 1 \pmod{7}$

1) $a \equiv b \pmod{n} \Rightarrow a + k \equiv b + k \ (n)$

2) $a \equiv b \ (n) \Rightarrow ha \equiv hb \ (n)$

3) $a \equiv b \ (n)$ $c \equiv d \ (n) \Rightarrow ac \equiv bd \ (n)$

$400 \equiv 1 \ (7) \Rightarrow 400 \cdot 400 \equiv 1 \cdot 1 \equiv 1 \ (7)$

Cosa vogliamo? $n \mid ac - bd =$

$= c(a-b) - bd + bc =$

$$= c\underbrace{(a-b)}_{\text{multiplo di } n} + b\underbrace{(c-d)}_{\text{multiplo di } n}$$

Rappresentanti privilegiati $= \{0, 1, 2, \ldots, n-1\}$

Un'altra scelta possibile è

$$\{-3, -2, -1, 0, 1, 2, 3\}$$

Resto della divisione di 398^2 per 400?

$$398 \equiv -2 \pmod{400}$$

$$398^2 \equiv (-2)^2 \equiv 4$$

ACHTUNG: COSA NON FUNZIONA?

$6 \equiv 2 \pmod 4$ $\qquad 4 \mid 6-2$

$\Downarrow$ (non funziona)

$3 \equiv 1 \pmod 4$ $\qquad 4 \mid \frac{6-2}{2}$

$3 \equiv 1 \pmod 2$ $\qquad \frac{4}{2} \mid \frac{6-2}{2}$

$4 \cdot 7 \equiv 88 \pmod{15}$

$\Downarrow$

$7 \equiv 22 \pmod{15}$

Potenze

Funziona: $a \equiv b \ (n) \Rightarrow a^k \equiv b^k \ (n)$

NON funziona: $h \equiv k \pmod n$

$$\Rightarrow \quad 2^h \equiv 2^k \pmod n$$

FALSISSIMO

$$1 \equiv 6 \pmod 5 \quad \not\Rightarrow \quad 2^1 \equiv 2^6 \ (5)$$

$$2 \not\equiv 64 \ (5)$$

Applicazione alle Diofantee

$$3x^2 = 141y^2 + 2$$

Uguaglianza $\Longrightarrow$ congruenza

Idea: far sparire variabili

$$0 \equiv 3x^2 \equiv 141y^2 + 2 \pmod 3$$
$$\equiv 0 \cdot y^2 + 2 \pmod 3$$

$$2^x - 5y^2 = 64$$

Modulo 2: $-5y^2 \equiv 0 \pmod 2$

$y^2 \equiv 0 \pmod 2$

y è pari

Modulo 5: $2^x \equiv 4 \pmod 5$

$x=0$	$2^x = 1 \equiv 1 \ (5)$
1	$2^1 \equiv 2$
2	$2^2 \equiv 4$
3	$2^3 \equiv 3$
4	$2^4 \equiv 1$
5	$2^5 \equiv 2^4 \cdot 2 \equiv 2 \ (5)$

+ periodicità di periodo 4

Quindi $x = 2 + 4k$, quindi x è pari

$$x^2 + y^2 = z^4 + 6$$

Quadrati sono belli modulo 8

$0^2 \quad 1^2 \quad 2^2 \equiv 4 \quad 3^2 \equiv 1 \pmod 8$

$4^2 \equiv 0 \ (8) \qquad 5^2 \equiv 1 \pmod 8 \qquad 6^2 \equiv 4 \ (8)$

$7^2 \equiv (-1)^2 \equiv 1 \ (8)$

$a \equiv 0, 1, 2, 3, \dots, 7 \pmod 8$

$a^2 \equiv 0^2, 1^2, \dots, 7^2 \ (8)$

$x^2 + y^2 = z^4 + 6$

Cosa può fare x^2+y^2 mod 8 ?

0, 1, 4, 5, 2

Cosa fa z^4 ?

$z^4 \equiv (z^2)^2 \equiv$ 1^2 (8) se z dispari; 0 (8) se z pari

Cosa fa z^4+6 ? 6 o 7

Caso fortunato

Lavorando modulo n, ho trovato una cosa della forma

$$a \cdot (\underbrace{\text{roba contente incognite}}) \equiv b \ (n)$$

Quindi voglio sapere se si può risolvere

$$ax \equiv b \pmod{n}$$

$\Leftrightarrow n \mid (ax - b)$ $\Leftrightarrow$ esiste un intero y tale che $ax - b = y \cdot n$

$\Leftrightarrow$ la diofantea $\circledast$ $ax \pm ny = b$ si risolve $\Leftrightarrow$ $(a, n) \mid b$

(a meno di cambiare il segno di y)

E come trovo la soluzione?

La soluzione di $\circledast$ è esattamente la soluzione della congruenza:

se guardo $ax + ny = b$ modulo n

trovo $ax \equiv b \pmod{n}$

Ex L'equazione $8x \equiv 7 \pmod{15}$ quante soluzioni ha?

Troviamo almeno una soluzione

$$8x \equiv 6 \quad (15)$$

$\Leftrightarrow \quad 15 \mid 8x-6 \quad \Leftrightarrow \quad 8x-6 = -15y$

$\Leftrightarrow \quad 8x+15y = 6$

$(8,15) \mid 6 \qquad$ OK

$15 = 8 + 7$

$8 = 7 + 1$

$1 = 8 - 7 = 2 \cdot 8 - 15$

$\times 6 \quad \hookrightarrow \quad 12 \cdot 8 - 6 \cdot 15 = 6$

$\hookrightarrow \quad 12 \cdot 8 \equiv 6 \pmod{15}$

$M = n^4 + n^3 + n^2 + n + 1$

$n \in \mathbb{Z}^+$, trovare n affinché

M sia quadrato perfetto

Diofantee lineari in 2 variabili: tutte le soluzioni

$$ax + by = c$$

$$az + bw = c$$

$$a(x-z) + b(y-w) = 0$$

$$a(x-z) = -b(y-w)$$

Wlog $(a,b) = 1$. $\quad a \mid b(y-w)$

$\Downarrow$ perché $(a,b)=1$

$a \mid (y-w)$

$$\Rightarrow \begin{cases} \boxed{w = y + ka} \\ a(x-z) = -b(-ka) \end{cases}$$

$$\Rightarrow x - z = kb \Rightarrow \boxed{z = x - kb}$$

$$mn + 2m - n - 8 = 0$$

$$(m-1)(n+2) - 6$$

$$(m-1)(n+2) = 6$$

$$x^3 - y^3 = 7004$$
$$7005$$

Osservazione $(x+3)^3 = x^3 + 9x^2 + 27x + 27$

$$\equiv x^3 \pmod 9$$

$0^3 \equiv 0 \quad 1^3 \equiv 1 \quad 2^3 \equiv -1 \ (9)$

$7005 \equiv 12 \equiv 3 \ (9)$

Quindi $x^3 - y^3 \equiv 3 \pmod 9$ non ha soluzioni

$$7004 = (x-y)(x^2+xy+y^2)$$

$x \geq 0,\ y \geq 0$

$$(x-y)^2 + 3xy \geq (x-y)^2$$

$$8000 > 7004 \geq (x-y)^3 \Rightarrow 20 > x-y$$

Lavorando modulo 2 (mah...) trovo

$$x \equiv y \ (2)$$

Possono essere entrambi pari?

Se sì, $8 \mid x^3 - y^3 = 7004$, il che non è vero. Quindi $x \equiv y \equiv 1 \ (2)$, e

$x - y \equiv 0 \pmod 4$, siccome

x^2+xy+y^2 è dispari

$$4 \mid (x-y) \mid 7004 = 4 \cdot 17 \cdot 103$$

E $x - y < 20$. Mmmh...

$x^2 + 3y = 2$ modulo 3

$x^2 \equiv 2 \pmod 3$

ma x^2 è 0 o 1 modulo 3, assurdo

$3^y - x^2 = 41$

Parità: x è pari

Mod 4: $3^y \equiv 1 \pmod 4$

$\Rightarrow y$ è pari

$\Rightarrow$ scrivo $y = 2a$,

$(3^a - x)(3^a + x) = 41$

$3^y - 2^x = 41$

Se $x \equiv 1$ non è interessante

Altrimenti $2^x \equiv 0 \pmod 4$, da cui

$$3^y \equiv 1 \pmod 4$$

$\Rightarrow$ y è pari

$$-2^x \equiv 2 \pmod 3$$

$$2^x \equiv 1 \pmod 3 \Rightarrow x \text{ pari}$$

$4^x - 2^y = 4094$ $\qquad$ $4096 - 2 = 4094$

$0 - 2^y \equiv 2 \mod 4$

$\Rightarrow y \leq 1$

(Esercizio 42)

$4^x + 4^y + 4^z = 9 \cdot \text{qualcosa} + 1$

Per parità, uno tra x, y, z è zero, diciamo z.

$4^x + 4^y = \text{numerone} = 2^3 \cdot \text{dispari}$

Quindi x e y non possono essere entrambi ≥ 2, e poi casi...

Altrimenti, contraddizione modulo 3

IMO 2009/1

Sia n un intero >0 e $a_1, \dots, a_k$ $(k \geq 2)$ interi distinti in $\{1, \dots, n\}$

Supponiamo che $n \mid a_i(a_{i+1} - 1)$ per $i = 1, \dots, k-1$.

Tesi: $n \nmid a_k(a_1 - 1) \iff a_1 a_k \not\equiv a_k$

$$a_i \cdot a_{i+1} \equiv a_i \mod n$$

$$a_1 a_2 \equiv a_1 \quad (n)$$

$$a_2 a_3 \equiv a_2 \quad (n) \to a_1 a_2 a_3 \equiv a_1 a_2 \equiv a_1$$

$$a_3 a_4 \equiv a_3 \quad (n)$$

$$a_1 a_2 a_3 a_4 \equiv a_1 a_2 a_3 \equiv a_1 a_2 \equiv a_1$$

a_1:

$$\begin{cases} a_1 a_2 \dots a_k \equiv a_1 \pmod n \\ a_1 a_k \equiv a_k \pmod n \end{cases}$$

Se per assurdo ↑ fosse vera, $a_k \equiv a_1 \ (n)$

Ma $a_1, \dots, a_k \in \{1, \dots, n\}$ e sono distinti, assurdo!