

Teoria dei Numeri

AlpT (@freaknet.org)

March 12, 2007

Copyright ©2007 Andrea Lo Pumo aka AlpT <alpt@freaknet.org>. All rights reserved.

This document is free; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This document is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this document; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Contents

1	Anelli Noetheriani	1
1.1	Proprieta'	1
2	Residuo quadratico	2
2.1	Simbolo di Legendre	2
3	Somma di quadrati	3
4	Primi in $\mathbb{Z}[i]$	4
5	Primi infiniti	5
6	Riemman	6
7	Reciprocita' quadratica	6
7.1	Teorema di reciprocita' di Gauss	7

1 Anelli Noetheriani

Un anello si dice Noetheriano se vale una delle seguenti condizioni:

1. Vale la c.c.a.f per gli ideali, cioè la seguente catena

$$I_1 \subseteq I_2 \subseteq \dots$$

si stabilizza. Ovvero, a partire da un certo punto in poi, tutti gli ideali sono uguali.

2. Ogni famiglia di ideali ammette l'elemento massimale
3. Ogni ideale dell'anello è finitamente generato

(0)1. Dimostriamo $1 \Rightarrow 2$

ASSUME: X poset, non vuoto, in cui vale la c.c.a.f

PROVE: Esiste $y_n \in X : y_n$ è massimale

PROOF:

LET: $Y_1 \subseteq X, Y_1 \neq \emptyset \quad y_1 \in Y_1$

CASE: y_1 è massimale

□

CASE: y_1 non è massimale

$$\exists Y_2 \subseteq X, Y_2 \neq \emptyset \quad y_2 \in Y_2$$

$$y_2 > y_1$$

CASE: y_2 è massimale

□

CASE: y_2 non è massimale

...Procedendo in questa maniera formiamo la seguente catena:

$$y_1 < y_2 < y_3 < \dots$$

ma per Hp, si stabilizza, quindi esiste un y_n che è maggiore di tutte le altre y_i con $i < n$ e inoltre, tutti gli elementi y_m , con $m > n$, sono tali che $y_m = y_n$. □

Theorem 1.1. *Il teorema della base di Hilbert afferma che:*

$$A \equiv \text{Noeth} \Rightarrow A[x] \equiv \text{Noeth}$$

Come corollario, dato il campo K :

$$K \equiv \text{Noeth} \Rightarrow K[x] \equiv \text{Noeth} \Rightarrow K[x, y] \equiv \text{Noeth} \Rightarrow \dots$$

1.1 Proprietà

1. A anello Noetheriano è un UFD se vale la seguente proprietà:

$$\forall a \in A, a \equiv \text{irriducibile} \Rightarrow a \equiv \text{primo}$$

Questa è un immediata conseguenza della caratterizzazione degli UFD.

2. $PID \Rightarrow \text{Noeth}$

Infatti, ogni PID è finitamente generato.

2 Residuo quadratico

Sia $p \neq 2$ primo, e sia $a \in \mathbb{Z}_p^*$

$$x^2 = a \pmod{p}$$

distinguiamo due casi:

CASE: Ammette soluzione $\pm x_0$

preso $y \in \mathbb{Z}_p^* \setminus \{\pm x_0\}$ l'equazione $yy' = a$, dove y' e' l'incognita, ammette sempre soluzione ($\mathbb{Z}_p$ e' un campo). L'insieme $\mathbb{Z}_p^* \setminus \{\pm x_0\}$ e' formato da $p-3$ elementi, quindi esistono $\frac{p-3}{2}$ coppie yy' tali che $yy' = a$. Allora se moltiplichiamo tutte le coppie tra loro otteniamo $a^{\frac{p-3}{2}}$. Riassumendo tutto quello che abbiamo trovato:

$$\prod_{x \in \mathbb{Z}_p^*} x = -x_0^2 a^{\frac{p-3}{2}} = -a^{\frac{p-1}{2}}$$

In questo caso diremo che a e' un residuo quadratico modulo p , e utilizzeremo il simbolo di Legendre:

$$\left(\frac{a}{p}\right) = 1$$

CASE: Non ammette soluzione

In questo caso, per ogni $y \in \mathbb{Z}_p^*$ esiste un $y' : yy' = a$, quindi esistono $\frac{p-1}{2}$ coppie yy' , e moltiplicandole tutte tra loro otteniamo:

$$\prod_{x \in \mathbb{Z}_p^*} x = a^{\frac{p-1}{2}}$$

In questo caso diremo che a non e' un residuo quadratico modulo p .

$$\left(\frac{a}{p}\right) = -1$$

2.1 Simbolo di Legendre

Come abbiamo visto prima:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ e' un residuo quadratico modulo } p \\ -1 & \text{se non lo e'} \end{cases}$$

Una formula (non ottimale) per calcolare il simbolo di Legendre e':

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$$

Nota: siamo sempre in $\mathbb{Z}_p$

CASE: a e' un residuo quadratico modulo p

come abbiamo visto prima:

$$\prod_{x \in \mathbb{Z}_p^*} x = -a^{\frac{p-1}{2}}$$

ma e' anche vero che

$$\prod_{x \in \mathbb{Z}_p^*} x = (p-1)! = -1 \quad [\text{thm di Wilson}]$$

quindi

$$-a^{\frac{p-1}{2}} = -1 \Rightarrow a^{\frac{p-1}{2}} = 1 = \left(\frac{a}{p}\right)$$

CASE: a non e' un residuo quadratico modulo p
 procedendo come prima arriviamo a:

$$a^{\frac{p-1}{2}} = -1 = \left(\frac{a}{p}\right)$$

□

3 Somma di quadrati

$x^2 + 1 = 0$ ha soluzioni in $\mathbb{Z}_p \Leftrightarrow p = 4k + 1$
 (0)2. Dim. $\Leftrightarrow$

$$\begin{aligned} x^2 + 1 = 0 &\Leftrightarrow \left(\frac{-1}{p}\right) = 1 \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \\ (-1)^{\frac{p-1}{2}} = 1 &\Leftrightarrow \frac{p-1}{2} = 2k, k \in \mathbb{Z} \\ p-1 = 4k & \end{aligned}$$

□

Questo e' una dimostrazione alternativa (e molto piu' elegante) a quella usata in un passo del paragrafo "somma di quadrati" che negli appunti di Algebra I: fenix.olocolors.org/~alpt/appunti/algebraI/algebraI.pdf

Dato $n \in \mathbb{Z}$, e la sua fattorizzazione

$$n = 2^t q_1^{m_1} q_2^{m_2} \dots q_r^{m_r} p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$$

dove

$$t \geq 0, \quad \forall i \ q_i = 1 \ (\mathbb{Z}_4), \quad p_i = 3 \ (\mathbb{Z}_4)$$

allora

$$n = a^2 + b^2 \Leftrightarrow \forall i, n_i \in 2\mathbb{N}$$

(0)3. Dimostriamo solo $\Rightarrow$, dato che la dimostrazione per $\Leftarrow$ e' stata gia' fatta negli appunti di Algebra I

ASSUME: 1. $n = a^2 + b^2$
 2. $n = 2^t q_1^{m_1} q_2^{m_2} \dots q_r^{m_r} p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$
 3. $t \geq 0, \quad \forall i \ q_i = 1 \ (\mathbb{Z}_4), \quad p_i = 3 \ (\mathbb{Z}_4)$

PROVE: $n_i \in 2\mathbb{N}$

PROOF:

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

$$d/a \Rightarrow a = \lambda d \Rightarrow a^2 = \lambda^2 d^2 \Rightarrow d^2/a^2$$

$$d/b \Rightarrow b = \mu d \Rightarrow b^2 = \mu^2 d^2 \Rightarrow d^2/b^2$$

$$d^2/a^2, d^2/b^2 \Rightarrow d^2/n$$

$$n = d^2 m$$

$$\frac{n}{d^2} = m = \frac{a^2}{d^2} + \frac{b^2}{d^2} = \lambda^2 + \mu^2$$

ASSUME: $p = 4h + 3 : p/d$

(1)1. Dimostreremo che p compare con esponente pari nella decomposizione di n facendo vedere che $p \nmid m$

ASSUME: Per assurdo p/m

PROVE: assurdo

PROOF: Come abbiamo visto prima, $m = \lambda^2 + \mu^2$, con $MCD(\lambda, \mu) = 1$.

Allora,

$$p/m \Leftrightarrow m = \lambda^2 + \mu^2 = 0 \pmod{p}$$

Poiche' $(\lambda, \mu) = 1$, p non puo' dividere contemporaneamente λ e μ , e inoltre non puo' neanche dividerne uno solo, infatti, se supponiamo per assurdo che divide λ abbiamo:

$$\lambda^2 + \mu^2 = \mu^2 = 0 \pmod{p}$$

e quindi dividerebbe anche μ , che e' assurdo perche' $(\lambda, \mu) = 1$. Quindi $\lambda, \mu \neq 0 \pmod{p}$. Poiche' $\mathbb{Z}_p$ e' un campo, $\exists c : \mu = \lambda c$. Sostituendo la b :

$$\lambda^2 + \mu^2 = \lambda^2 + (\lambda^2 c^2) = \lambda^2(1 + c^2) = 0 \pmod{p}$$

e poiche' $\lambda \neq 0$, ci riduciamo a

$$1 + c^2 = 0 \pmod{p}$$

ma questo e' assurdo, perche' $c^2 = -1$ ammette soluzione se e solo se p e' della forma $4k + 1$ (lo abbiamo dim. al paragrafo 3) □

□

Theorem 3.1. *Un numero n e' somma di tre quadrati se e solo se non e' del tipo $4^n(8k + 7)$*

Theorem 3.2. *Ogni numero intero e' somma di 4 quadrati.*

Theorem 3.3. *Ogni numero e' somma di 9 cubi.*

In realta', escludendo solo 23 e 239, tutti gli altri interi si possono scrivere come somma di 8 cubi.

Theorem 3.4. *Indichiamo con $G(3)$ il numero di cubi necessari a scrivere tutti i numeri interi positivi, tranne un insieme finito di essi, come somma di cubi. Esiste questo teorema:*

$$4 \leq G(3) \leq 7$$

4 Primi in $\mathbb{Z}[i]$

Proposition 4.1.

$$\pi \in \mathbb{Z}[i] \text{ primo} \Rightarrow \exists z \in \mathbb{Z} : \pi/z$$

PROOF:

$$|\pi| = \pi \bar{\pi} = n \in \mathbb{Z} \Rightarrow \pi/n$$

□

Proposition 4.2. *Dato $\pi \in \mathbb{Z}[i]$*

$$|\pi| \text{ primo} \Rightarrow \pi \text{ primo}$$

PROOF: Per assurdo $\pi = \lambda\mu$ con λ, μ non invertibili.

$$|\pi| = |\lambda||\mu|$$

ma $|\pi|$ e' primo e quindi irriducibile, e quindi o $|\lambda|$ o $|\mu|$ e' un invertibile. Supponiamo che lo sia $|\lambda|$, cioe' $|\lambda| = 1$, ma questo implicherebbe che λ stesso e' un invertibile in $\mathbb{Z}[i]$ il che e' un assurdo contro ipotesi. □

Proposition 4.3. Dato un $p \in \mathbb{Z}$ analizziamo 3 casi:

1. $p = 2$:

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

Si dice che 2 e' ramificato.

$(1 + i)$ e' primo in $\mathbb{Z}[i]$.

2. $p = 4k + 1$:

$$p = a^2 + b^2 = (a + ib)(a - ib)$$

$a + ib, a - ib$ e' una coppia di primi coniugati in $\mathbb{Z}[i]$.

Si dice che p e' decomposto.

3. $p = 4h + 3$:

p resta primo in $\mathbb{Z}[i]$.

Si dice che p e' inerte.

5 Primi infiniti

Proposition 5.1. Esistono infiniti primi della forma $4k + 3$.

ASSUME: Per assurdo che $A = \{p_1, \dots, p_n\}$ sia l'insieme finito dei primi $4k + 3$.

PROOF: Consideriamo il numero $q = 4p_1 \cdot p_2 \cdot p_3 \cdots p_n + 3$ e consideriamo la sua fattorizzazione: $q = q_1 q_2 \dots q_t$. Poiche' prodotti di numeri congrui 1 modulo 4 sono chiusi rispetto al prodotto

$$(4k + 1)(4h + 1) = 4(5h + k) + 1$$

deve esistere almeno un q_i congruo 3 modulo 4 per fare in modo che q sia pure congruo 3 (lo e' per costruzione). Se $q_i \in A$, cioe' se $q_i = p_j$, avremmo:

$$q_i/q, \quad q/4p_1 \cdot p_2 \cdot p_3 \cdots p_n \Rightarrow q_i/3$$

Il che e' impossibile, quindi $q_i \notin A$, ma allora abbiamo trovato un primo della forma $4k + 3$ che non appartiene in A , ed ecco l'assurdo. $\square$

Proposition 5.2. Esistono infiniti primi della forma $4k + 1$.

ASSUME: Per assurdo che $A = \{p_1, \dots, p_n\}$ sia l'insieme finito dei primi $4k + 1$.

LET: 1. $B = \{3, 5, 7, \dots, p\}$ in modo tale che $A \subseteq B$

$$2. n = 3^2 5^2 7^2 \dots p^2 + 2^2$$

n e' somma di quadrati e' quindi e' della forma $4k + 1$, allora tutti i suoi fattori primi sono pure nella forma $4k + 1$, perche' prodotti di numeri congrui 1 modulo 4 sono chiusi rispetto al prodotto:

$$(4k + 1)(4h + 1) = 4(5h + k) + 1$$

Se un $p_i \in A$ fosse un fattore di n avremmo che:

$$p_i/n, \quad p_i/3^2 5^2 7^2 \dots p^2 \Rightarrow p_i/2^2$$

il che e' impossibile, quindi ogni fattore primo di n deve essere della forma $4k + 1$ ma non deve appartenere ad A . Assurdo. $\square$

Theorem 5.3. Teorema di Dirichlet.

$$MCD(a, b) = 1 \Rightarrow \{ak + b \mid k \in \mathbb{Z}\} \text{ contiene infiniti primi}$$

Theorem 5.4. *Teorema dei numeri primi.*

$$\pi(x) \approx \frac{x}{\log x} \Leftrightarrow \lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

dove $\pi(x)$ e' il numero di primi minori o uguali a x .

6 Riemman

Questa e' la famosa funzione di Riemman:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

per $s > 1$ converge.

Questa funzione puo' anche essere definita $\forall s \in \mathbb{C}$.

L'Ipotesi di Riemann afferma che tutti gli zeri di questa funzione si trovano in

$$\left\{ \frac{1}{2} + iy, y \in \mathbb{R} \right\}$$

Eulero ha dimostrato che

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

7 Reciprocita' quadratica

Il simbolo di Legendre $\left(\frac{d}{p}\right)$ con $p \nmid a$ si puo' interpretare come la seguente composizione di omomorfismi:

$$\mathbb{Z} \setminus p\mathbb{Z} \longrightarrow \mathbb{Z}_p^* \longrightarrow \frac{\mathbb{Z}_p^*}{(\mathbb{Z}_p^*)^2}$$

dove $(\mathbb{Z}_p^*)^2$ e' l'insieme dei elementi quadrati in $\mathbb{Z}_p$.

$\frac{\mathbb{Z}_p^*}{(\mathbb{Z}_p^*)^2} = \{1, -1\}$, proprio perche' un elemento in $\mathbb{Z}_p^*$ puo' essere o un quadrato, e quindi diventa equivalente a 1 oppure non esserlo, e quindi diventa equivalente a -1 .

Da queste osservazioni seguono queste due proprieta':

1. $d = d' \pmod{p} \Rightarrow \left(\frac{d}{p}\right) = \left(\frac{d'}{p}\right)$. Ovviamente se d e' uguale a d' , allora avranno lo stesso simbolo di Legendre.
2. $\left(\frac{dd'}{p}\right) = \left(\frac{d}{p}\right) \left(\frac{d'}{p}\right)$. Questo proprio perche' $\left(\frac{d}{p}\right)$ e' un omomorfismo.

7.1 Teorema di reciprocita' di Gauss

Dati p, q primi dispari

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p'q'} \quad p' = \frac{p-1}{2}, \quad q' = \frac{q-1}{2}$$

Possiamo usare questo teorema per calcolare velocemente il simbolo di Lagrange.

Ecco un esempio: vogliamo calcolare $\left(\frac{13}{29}\right)$, per gauss: $\left(\frac{13}{29}\right)\left(\frac{29}{13}\right) = (-1)^{6 \cdot 14} = 1$

allora abbiamo due casi: $\left(\frac{13}{29}\right) = \left(\frac{29}{13}\right) = \pm 1$

consideriamo $\left(\frac{29}{13}\right)$ che e' uguale a $\left(\frac{3}{13}\right)$ perche' $29 \equiv 3 \pmod{13}$.

Reiteriamo: $\left(\frac{3}{13}\right)\left(\frac{13}{3}\right) = (-1)^{2 \cdot 6} = 1$

allora abbiamo due casi: $\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \pm 1$

consideriamo $\left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$. Quindi poiche' $\left(\frac{13}{3}\right) = 1$ e poiche' $\left(\frac{3}{13}\right)\left(\frac{13}{3}\right) = 1$

deduciamo che $\left(\frac{3}{13}\right) = 1$. Ma poiche' prima avevamo visto che $\left(\frac{29}{13}\right) = \left(\frac{3}{13}\right) = 1$,

e poiche' $\left(\frac{13}{29}\right)\left(\frac{29}{13}\right) = 1$, concludiamo che $\left(\frac{13}{29}\right) = 1$