Introduzione al corso AL420-Numeri Algebrici

Stefania Gabelli

a.a. 2010/2011

I sei libri dell'Arithmetica di Diofanto (circa 250 A.C.), miracolosamente scampati alla distruzione della biblioteca di Alessandria, sono stati tra gli ultimi libri dei matematici greci ad essere tradotti in latino. In esso venivano affrontati più di cento problemi aritmetici che avevano per soluzione numeri interi. Questo tipo di problemi vengono oggi chiamati *Problemi Diofantei*.

Pierre de Fermat (1601-1665), il precursore della moderna Teoria dei Numeri, usava annotare le sue osservazioni in margine alla sua copia dell'Arithmetica (una traduzione di Bachet, del 1621). Molte di queste acute annotazioni consistevano nell'enunciazione di vari teoremi, che Fermat asseriva di aver provato, ma di cui purtroppo non dava alcuna dimostrazione.

Agli inizi dell'800 tutti i problemi posti da Fermat erano stati risolti, in positivo o in negativo, tranne quello che viene oggi conosciuto come l'*Ultimo Teorema di Fermat*. In relazione ad alcuni quesiti riguardanti il Teorema di Pitagora (*Libro 2, Questione 8: dividere un quadrato dato in due quadrati*), Fermat scrisse di aver trovato una sorprendente dimostrazione del seguente fatto:

Teorema 1 (Ultimo Teorema di Fermat, 1637) *Per $n \geq 3$, non esistono dei numeri interi a, b, c diversi da zero tali che*

$$a^n + b^n = c^n;$$

ovvero l'equazione

$$X^n + Y^n = Z^n$$

non ha soluzioni intere non banali.

Nonostante la semplicità dell'enunciato, questo problema si è rivelato essere uno tra i più difficili di tutti i tempi. Nel tentativo di dimostrarlo, sono stati introdotti molti nuovi concetti e metodi che hanno apportato grande ricchezza alla matematica moderna, favorendone lo sviluppo e la diversificazione. Nel corso dei secoli la congettura di Fermat è stata dimostrata per valori sempre più grandi di n, ma è stata definitivamente risolta soltanto nel 1994, circa 350 anni dopo la sua formulazione, da A. Wiles, con il contributo di R. Taylor.

La dimostrazione dell'Ultimo Teorema di Fermat è una delle più grandi conquiste matematiche del secolo scorso; in essa si fa uso di tutte le tecniche più recenti e sofisticate, accessibili soltanto a pochi specialisti. È perciò molto probabile che la congettura di Fermat sia stata una geniale intuizione basata su un errore di ragionamento.

Il Teorema di Fermat è evidentemente falso per $n = 2$, perché, come era già noto ad Euclide, esistono (infiniti) triangoli rettangoli con lati di lunghezza intera ed inoltre il Teorema di Pitagora ci assicura che, se i cateti hanno lunghezza uguale ad a e b e l'ipotenusa ha lunghezza uguale a c, allora $a^2 + b^2 = c^2$; dunque la terna di numeri interi (a, b, c) è soluzione dell'equazione $X^2 + Y^2 = Z^2$. Le terne di questo tipo, come ad esempio $(2, 3, 5)$ oppure $(5, 12, 13)$, si dicono *terne pitagoriche*.

Per dimostrare il Teorema di Fermat per $n > 2$, ci si può ridurre facilmente a considerare il caso in cui $n = 4$ oppure $n = p$, con p un numero primo dispari.

Per convincersene, basta ricordare che ogni numero naturale si può scrivere in modo unico come prodotto di numeri primi (*Teorema Fondamentale dell'Aritmetica*); dunque ogni numero intero maggiore di 2 è un multiplo di 4 oppure di un numero primo $p > 2$. Inoltre, se il teorema è vero per un numero naturale m, è vero anche per tutti i suoi multipli km. Infatti, per $k, m \geq 1$, se l'equazione

$$X^{km} + Y^{km} = Z^{km}$$

ha soluzioni non banali, posto $U = X^k$, $V = Y^k$, $W = Z^k$, l'equazione

$$U^m + V^m = W^m$$

ha soluzioni non banali.

Un metodo per dimostrare la congettura nel caso $n = 4$ si trova già negli scritti di Fermat e probabilmente Fermat pensava erroneamente che questo stesso metodo potesse essere impiegato per risolvere il caso generale. Effettivamente questa tecnica è stata poi usata da L. Euler per dimostrare nel 1770, seppure in modo incompleto, il caso $n = 3$; ma si è rivelata inefficace per valori superiori.

Euler ebbe la fondamentale idea di ampliare il concetto di numero intero, lavorando con dei particolari numeri complessi che vengono oggi chiamati *interi algebrici*. Per illustrarne l'utilità in relazione alla congettura di Fermat, è necessario considerare le radici complesse n-sime dell'unità.

Un numero complesso ζ è una radice n-sima dell'unità se $\zeta^n = 1$. Le radici n-sime dell'unità sono dunque le soluzioni complesse dell'equazione $X^n - 1 = 0$. Esse sono tutte distinte e, nel piano complesso, si dispongono ai vertici di un poligono regolare di n lati, centrato nell'origine e con un vertice in 1 .

Se p è un numero primo, una proprietà molto utile è il fatto che le radici p-esime sono tutte esprimibili come potenze di una qualsiasi di esse diversa da 1. Cioè, se $\xi \neq 1$ è una radice p-esima, allora tutte e sole le radici p-esime sono:

$$1, \xi, \xi^2, \xi^3, \ldots, \xi^{p-1}.$$

Con l'aiuto delle radici p-esime dell'unità, l'equazione di Fermat si può fattorizzare linearmente:

$$X^p + Y^p = (X+Y)(X+\xi Y)(X+\xi^2 Y)\ldots(X+\xi^{p-1}Y) = Z^p.$$

Sostituendo alle indeterminate X, Y, Z dei numeri interi a, b, c, otteniamo una fattorizzazione in numeri complessi:

$$a^p + b^p = (a+b)(a+\xi b)(a+\xi^2 b)\ldots(a+\xi^{p-1}b) = c^p$$

dove i fattori $a + \xi^i b$ sono del tipo:

$$a_0 + a_1\xi + a_2\xi^2 + \ + a_{p-1}\xi^{p-1},$$

con $a_0, a_1, \ldots, a_{p-1}$ numeri interi.

L'insieme di tutti i numeri interi si indica con $\mathbb{Z}$ e l'insieme dei numeri complessi sopra definiti si indica con $\mathbb{Z}[\xi]$. Per ogni primo p ,

$$\mathbb{Z}[\xi] = \{a_0 + a_1\xi + \cdots + a_{p-1}\xi^{p-1}; a_i \in \mathbb{Z}\}$$

è un anello commutativo integro; esso si chiama l'anello degli *interi ciclotomici* ed è un particolare anello di *interi algebrici*.

Il termine anello è dovuto al fatto che le radici n-sime dell'unità si dispongono su una circonferenza, mentre il termine ciclotomico (che deriva dal greco e significa che taglia il cerchio) è dovuto al fatto che esse tagliano tale circonferenza in n archi uguali.

Nel 1847 G. Lamè presentò all'Accademia di Parigi una sua dimostrazione dell'Ultimo Teorema di Fermat. Essa si basava sul fatto che nell'anello degli interi ciclotomici valesse un teorema analogo al Teorema Fondamentale dell'Aritmetica, ovvero sul fatto che ogni intero ciclotomico si potesse fattorizzare in modo essenzialmente unico nel prodotto di interi ciclotomici irriducibili. Come fu osservato da J. Liouville, tale supposizione non aveva nessun fondamento: infatti E. Kummer, venuto a conoscenza del problema sollevato da Liouville, gli scrisse che essa era in realtà del tutto falsa. Il più piccolo numero primo per il quale fallisce il teorema di fattorizzazione unica in $\mathbb{Z}[\xi]$ è 23.

Kummer dimostrò tuttavia che in certi casi il teorema di fattorizzazione unica poteva essere ripristinato per gli interi ciclotomici introducendo dei *numeri ideali*. Questo permetteva di provare il Teorema di Fermat per quasi tutti i numeri primi minori di 100.

In una sua fondamentale memoria del 1871, R. Dedekind osservò poi che la funzione dei numeri ideali di Kummer poteva essere svolta più generalmente in tutti gli anelli di interi algebrici da particolari sottoinsiemi, che egli chiamò ancora *ideali*.

Gli ideali, come i numeri, si possono addizionare e moltiplicare. Dedekind dimostrò che in ogni anello di interi algebrici un ideale si può sempre fattorizzare in modo unico nel prodotto di ideali primi, anche nei casi in cui il teorema di fattorizzazione unica fallisce per gli elementi.

Senza entrare nei dettagli, facciamo un esempio per illustrare questo fatto.

Esempio 1 Diamo per scontato che il dominio

$$\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5}; a, b \in \mathbb{Z}, i^2 = -1\}$$

sia un anello di interi algebrici. Alcuni elementi di questo anello si possono fattorizzare in modi differenti nel prodotto di elementi irriducibili, ad esempio:

$$21 = 3 \cdot 7 = (1 + 2i\sqrt{5})(1 - 2i\sqrt{5}).$$

Passando agli ideali, abbiamo:

$$\langle 21\rangle = \langle 3\rangle\langle 7\rangle;$$

ma gli ideali $\langle 3\rangle$ e $\langle 7\rangle$ non sono primi. Infatti la loro fattorizzazione in ideali primi è:

$$\langle 3\rangle = \langle 3, 1 + 2i\sqrt{5}\rangle\langle 3, 1 - 2i\sqrt{5}\rangle; \quad \langle 7\rangle = \langle 7, 1 + 2i\sqrt{5}\rangle\langle 7, 1 - 2i\sqrt{5}\rangle.$$

Dunque l'unica fattorizzazione dell'ideale $\langle 21\rangle$ in ideali primi è:

$$\langle 21\rangle = \langle 3, 1 + 2i\sqrt{5}\rangle\langle 3, 1 - 2i\sqrt{5}\rangle\langle 7, 1 + 2i\sqrt{5}\rangle\langle 7, 1 - 2i\sqrt{5}\rangle.$$

La formalizzazione delle proprietà degli anelli di interi algebrici e dei polinomi a coefficienti numerici ha portato all'inizio del 1900 al concetto astratto di *anello*.

Negli anni '20, ci sono stati enormi progressi nello studio degli anelli commutativi, soprattutto ad opera di maestri quali Emmy Noether ed Emil Artin.

E. Noether ha caratterizzato tra l'altro gli anelli commutativi in cui, come negli anelli di interi algebrici, ogni ideale non nullo è prodotto di ideali primi. Questi anelli vengono oggi chiamati *Domini di Dedekind*.

La classe dei Domini di Dedekind è l'intersezione di due classi fondamentali di anelli, gli Anelli Noetheriani e gli Anelli di Prüfer. Gli Anelli Noetheriani (che prendono il nome da E. Noether) sono gli anelli che intervengono in Geometria Algebrica ed hanno il loro prototipo negli anelli

di funzioni algebriche. Gli Anelli di Prüfer, (che prendono il nome da H. Prüfer) sono gli anelli che intervengono nella Teoria Algebrica dei Numeri ed hanno il loro prototipo negli anelli di valutazione.

In questo corso ripercorremo le tappe di questa evoluzione del pensiero matematico.

Dopo avere brevemente richiamato le proprietà dei campi di numeri (ampliamenti finiti del campo dei numeri razionali) e delle estensioni intere di anelli, studieremo gli anelli di interi algebrici (definiti come la chiusura integrale di $\mathbb{Z}$ in un campo di numeri), specialmente gli anelli di interi quadratici e ciclotomici. Affronteremo in particolare il problema della fattorizzazione e mostreremo che gli anelli di interi algebrici sono domini di Dedekind. Infine illustreremo la dimostrazione di Lamè e mostreremo perché, come osservato da Kummer, essa funziona per i così detti primi regolari.

Alcune parti del programma potranno essere svolte più o meno approfonditamente, in relazione alla preparazione e all'interesse degli studenti.