Capitolo 1

Introduzione

1.1 La collana "I quaderni della Settimana Matematica"

La collana "I quaderni della Settimana Matematica" è una iniziativa editoriale del Dipartimento di Matematica dell'Università di Pisa che si è sviluppata nell'ambito del Piano Nazionale Lauree Scientifiche.

Ogni volume della Collana prende spunto dai contenuti e dai materiali raccolti negli anni nei laboratori attivati durante la Settimana Matematica, lo stage rivolto a studenti di scuola secondaria superiore che si tiene ogni anno presso il Dipartimento di Matematica dell'Università di Pisa, all'interno delle iniziative previste per il Piano Nazionale Lauree Scientifiche.

L'iniziativa editoriale è rivolta in particolare ad insegnanti di scuola superiore ed è finalizzata a fornire ai docenti interessati un possibile strumento di lavoro. I volumi della Collana infatti propongono ipotesi di possibili percorsi didattici su aspetti che coinvolgono strumenti matematici rilevanti per l'istruzione secondaria e suggeriscono attività di classe che possono stimolare una didattica di tipo laboratoriale, capace di coniugare la conoscenza di determinati contenuti matematici con competenze fondamentali quali quelle di problem solving, argomentazione e modellizzazione. Le attività suggerite possono anche stimolare competenze più generali, parimenti importanti, come quella di saper affrontare una discussione tra pari, di lavorare in gruppo, di sostenere o criticare costruttivamente un'ipotesi di lavoro.

Le finalità del progetto editoriale sono perfettamente in linea, per tutti i livelli scolari, con le nuove Indicazioni (per il primo ciclo e per i percorsi liceali) e Linee Guida (per gli istituti tecnici e professionali). Già nel 2007[1] si sottolineava come uno degli obiettivi fondamentali del nostro sistema scolastico fosse l'acquisizione dei saperi e delle competenze chiave di cittadinanza, articolate in quattro assi culturali principali: asse dei linguaggi, matematico, scientifico-tecnologico e storico-sociale. E per quanto riguarda l'asse matematico, si specificava che: "*finalità dell'asse matematico è l'acquisizione al termine dell'obbligo d'istruzione delle abilità necessarie per applicare i principi e i processi matematici di base nel contesto quotidiano della sfera domestica e sul lavoro, nonché per seguire e vagliare la coerenza logica delle argomentazioni proprie e altrui in molteplici contesti di indagine conoscitiva e di decisione*".

In continuità con tale impostazione, le nuove Indicazioni per il primo ciclo[2] descrivono la competenza matematica come segue: "*La competenza matematica è l'abilità di sviluppare e applicare il pensiero matematico per risolvere una serie di problemi in situazioni quotidiane. Partendo da una solida padronanza delle competenze aritmetico-matematiche, l'accento è posto sugli aspetti del processo e dell'attività oltre che su quelli della conoscenza. La competenza matematica comporta, in misura variabile, la capacità e la disponibilità a usare modelli matematici di pensiero (pensiero logico e spaziale) e di presentazione (formule, modelli, schemi, grafici, rappresentazioni)*".

Si richiede quindi, tra le altre cose, che i nostri studenti acquisiscano la capacità di utilizzare la matematica per leggere, rappresentare ed interpretare la realtà. Ad esempio, nelle Indicazioni Nazionali per i percorsi liceali[3] si richiede che "*al termine del percorso didattico lo studente avrà approfondito i procedimenti caratteristici del pensiero matematico (definizioni, dimostra-*

[1] Decreto Ministeriale 22-8-2007 n.139, sull'adempimento dell'obbligo di istruzione.

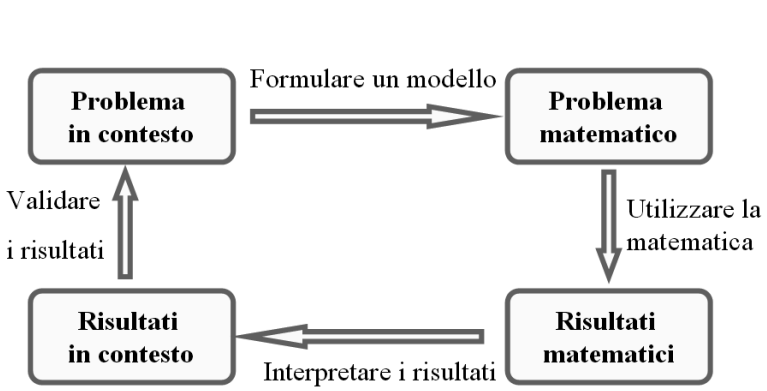
[2] Indicazioni Nazionali per il curricolo della scuola dell'infanzia e del primo ciclo d'istruzione, Miur - Settembre 2012

[3] Schema di regolamento recante "Indicazioni nazionali riguardanti gli obiettivi specifici di apprendimento concernenti le attività e gli insegnamenti compresi nei piani degli studi previsti per i percorsi liceali di cui all'art. 10, comma 3, del d.P.R. 15 marzo 2010"

zioni, generalizzazioni, formalizzazioni), conoscerà le metodologie elementari per la costruzione di modelli matematici in casi molto semplici ma istruttivi.

Il processo di matematizzazione richiesto è abitualmente schematizzata in quello che è noto come “ciclo di matematizzazione” nel quadro di riferimento teorico delle prove OCSE-PISA (vedi figura 1.1).

Figura 1.1: Il ciclo di matematizzazione - Framework OCSE-PISA 2012



Il ciclo di matematizzazione consta dunque di quattro fasi distinte:

1. il passaggio dalla situazione di problema reale al modello matematico
2. il lavoro sul modello matematico (cercare una soluzione del problema matematico)
3. l’interpretazione dei risultati matematici nel mondo reale
4. la verifica e validazione dei risultati rispetto al problema reale da cui si era partiti

È piuttosto evidente come nella scuola italiana a qualsiasi livello scolare, gli studenti siano messi di fronte quasi esclusivamente ad attività inerenti al lavoro sul modello matematico. È opportuno sottolineare le difficoltà oggettive che si presentano nell’affrontare, a livello di scuola secondaria, attività che coinvolgano tutte le fasi del ciclo di matematizzazione: la realtà è molto complessa e gli strumenti matematici che si acquisiscono durante il ciclo

secondario di istruzione sono comunque limitati. È necessario dunque trovare argomenti adatti, ovvero che siano legati a problematiche interessanti e che possano permettere di introdurre o consolidare argomenti matematici accessibili agli studenti e rilevanti per l'istruzione secondaria.

Uno dei primi obiettivi della presente Collana è proprio legato alla scelta degli argomenti, scelti appositamente per la loro rilevanza, per la possibilità di essere trattati con importanti strumenti matematici accessibili a studenti di scuola superiore e sperimentati con successo con i ragazzi nell'ambito della manifestazione che dà il nome alla Collana.

Oltre agli argomenti, i volumi della Collana, appunto ispirati dai laboratori della Settimana Matematica, vogliono essere un possibile modello di *laboratorio matematico* e quindi fornire idee e spunti anche metodologici. Le Indicazioni Nazionali per i percorsi liceali e le Linee Guida per gli istituti tecnici e professionali richiamano l'importanza dell' "*uso costante del laboratorio per l'insegnamento delle discipline scientifiche*". Questo richiamo rappresenta un elemento di continuità tra le Indicazioni per il secondo ciclo e quelle per il primo ciclo, che esplicitano cosa si intenda e quali siano le finalità del laboratorio nello specifico della matematica: "*In matematica, come nelle altre discipline scientifiche, è elemento fondamentale il laboratorio, inteso sia come luogo fisico sia come momento in cui l'alunno è attivo, formula le proprie ipotesi e ne controlla le conseguenze, progetta e sperimenta, discute e argomenta le proprie scelte, impara a raccogliere dati, negozia e costruisce significati, porta a conclusioni temporanee e a nuove aperture la costruzione delle conoscenze personali e collettive*".

Le attività scelte, ma anche la struttura dei volumi di questa Collana, sono dunque pensate appositamente per favorire la discussione, le congetture e le argomentazioni anche tra pari. Per questo ogni sezione dei volumi propone uno o più problemi da cui far scaturire una discussione in cui l'insegnante assuma il ruolo di moderatore/guida, ma in cui siano gli allievi per primi a mettersi in gioco, a porsi domande, a congetturare risposte. In questo modo anche gli strumenti matematici in gioco vengono sempre introdotti non dall'alto, come argomento imposto dal programma, ma come risposta ad un'esigenza scaturita "dal basso", ovvero dai ragazzi stessi, che ne sentono il bisogno per risolvere un problema che li ha coinvolti e sul quale

si sono confrontati.

Questo approccio permette una modellizzazione matematica non predeterminata, costruita in base alle scelte del gruppo classe, e costituisce un interessante occasione per concentrarsi sull'individuazione degli obiettivi (il perché) prima che sulla loro realizzazione (il come), favorendo la condivisione di senso nell'attività matematica.

In questo "laboratorio in aula", quindi, il docente avrà la possibilità di costruire e valutare attivamente abilità e competenze nei suoi ragazzi, sia disciplinari che trasversali, mentre questi ultimi avranno l'importantissima occasione di sperimentare una matematica "nuova", meno ingessata, che prova a dare risposte a problemi scaturiti dal basso, in cui sono possibili spesso diverse risposte e nel quale hanno un ruolo il proprio intuito e il proprio pensiero.

Un'ultima annotazione sul percorso: sia per eventuali specifiche esigenze dell'insegnante sia per lo spirito laboratoriale del percorso stesso, non avrebbe senso imporre un rigido ordine sequenziale dei contenuti e delle attività. L'organizzazione sequenziale dei contenuti è dovuta soltanto ad esigenze di stampa: ogni docente ovviamente è libero di organizzare il percorso che preferisce, a seconda degli interessi propri e della classe, e della discussione tra gli alunni. Per aiutare nella scelta, è presente in ogni volume uno schema che indica le connessione tra le varie parti e dei possibili percorsi tenendo conto anche degli eventuali pre-requisiti.

1.2 Crittografia

L'esigenza di rendere nascosto il contenuto di un certo messaggio a chiunque non sia né il mittente né il destinatario è presente fin dall'antichità. La necessità di possedere metodi sicuri e efficienti per cifrare un testo è sempre stata una priorità per governanti e strateghi. I motivi possono essere i più disparati: diplomazia, guerre, interessi. Il denominatore comune è la sfida continua tra chi vuole mantenere segreto il messaggio (il crittografo) e chi vuole svelarne il contenuto (il crittanalista).
È importante tenere presente che questa sfida non è sempre tra "buoni" e "cattivi: quando si vuole comunicare i dati della propria carta di credito

per un acquisto o una transazione di denaro riteniamo importante usare un sistema di cifratura a prova di crittanalista. Tuttavia quando si pensa ai movimenti e alle comunicazioni, per esempio, di gruppi criminali, capiamo l'importanza che le forze dell'ordine riescano a decifrare le comunicazioni segrete di chi può minare la sicurezza di altre persone.

La scelta dell'argomento, come sottolineato nella sezione precedente, è dunque tutt'altro che casuale. La sicurezza nello scambio di informazioni riservate, siano essi codici bancari o mail personali, è un tema molto delicato e rilevante nell'esperienza di vita quotidiana di tutti noi, e sicuramente anche in quella dei ragazzi di scuola superiore. Parlare di crittografia permette inoltre di mettere in gioco diversi aspetti del ragionamento matematico: osservazione, ricerca di regolarità e capacità di analizzare e generalizzare. Tutto questo in un contesto e con un obiettivo del quale tutti possono cogliere l'importanza: rendere certe informazioni incomprensibili a chi intercetti il messaggio.

L'argomento permette di toccare alcuni contenuti significativi della matematica, in particolare dell'aritmetica e dunque dell'ambito "Numeri", inclusi negli obiettivi specifici di apprendimento per la matematica fin dal primo biennio della scuola superiore; ad esempio l'algoritmo euclideo per il calcolo del massimo comun divisore, esplicitamente richiamato nelle Indicazioni Nazionali per i percorsi liceali: "*Lo studio dell'algoritmo euclideo per la determinazione del MCD permetterà di approfondire la conoscenza della struttura dei numeri interi e di un esempio importante di procedimento algoritmico*".

Infine la crittografia si presta bene ad essere trattata all'interno di un laboratorio matematico, partendo prima dai problemi per cercare poi le eventuali diverse soluzioni matematiche, discuterne e confrontarne l'efficacia, provare a trovare soluzioni sempre migliori. Il lavoro sulla crittografia offre un'occasione importante di lavorare su competenze trasversali quali congetturare, argomentare, validare e confutare ipotesi; inoltre permette anche di descrivere in maniera coinvolgente lo sviluppo storico del problema, sottolineando i rapporti tra metodi, scoperte matematiche e il contesto storico, tecnologico e scientifico, e dunque di lavorare anche con l'obiettivo di mostrare la matematica come un prodotto culturale, in cui prove ed errori

sono all'ordine del giorno, e non uno statico sapere immutabile indipendente dal contesto.

Oltre a rappresentare un'applicazione a tutto tondo della matematica, la crittografia è una fonte ricchissima di aneddoti, legami storici e incursioni nella letteratura, il che rende l'attività adattissima alla creazione di percorsi multidisciplinari, attinenti con storia e letteratura, oltre che informatica e discipline tecniche e informatiche. Percorsi non fini a se stessi, ma che integrano, rafforzandole, le conoscenze e i punti di vista provenienti da saperi diversi.

Questo volume fa riferimento al lavoro svolto nell'ambito del laboratorio de "la Settimana Matematica" dal titolo "Crittografia", coordinato dalla professoressa Patrizia Gianni. Un ringraziamento particolare va dunque a Patrizia Gianni per l'idea, i materiali e il supporto a questa iniziativa. Il materiale è stato in parte testato anche in un'altra esperienza con studenti della scuola superiore: l'iniziativa *Scienze?...Al Dini!* proposta dal Liceo Scientifico "Ulisse Dini" di Pisa.

1.3 I percorsi possibili

I percorsi possibili da realizzare con il materiale contenuto nel presente volume sono molteplici ed adattabili in base al livello ed agli interessi del gruppo classe: la mappa a fine capitolo ne propone alcuni possibili (indicati dalle frecce tratteggiate).

I percorsi possono dosare in proporzioni diverse due aspetti essenziali dei contenuti di questo volume:

- gli aspetti **storici**, in particolare inerenti l'evoluzione dei metodi crittografici nel corso dei secoli (anzi, dei millenni!), evoluzione che dipende dalla contemporanea evoluzione dei metodi per decrittare i messaggi cifrati, in una specie di singolare competizione tra chi nasconde il messaggio e chi riesce a decifrarlo;

- gli aspetti più puramente **matematici**, in particolare l'illustrazione degli strumenti matematici utilizzati in crittografia e dei teoremi (tra cui diversi di aritmetica) e delle dimostrazioni che spiegano e giustifi-

cano perché tali strumenti funzionino in maniera efficiente rispetto all'obiettivo di crittare in maniera sicura. Tali aspetti possono spingersi, fino ad arrivare alla dimostrazione - o quantomeno alla giustificazione - dell'algoritmo di uno dei metodi crittografici più importanti e più usato negli ultimi decenni: RSA.

Entrambi gli aspetti appaiono importanti e possono appunto essere dosati a seconda dei propositi del docente: gli aspetti storici, la contestualizzazione del problema (la sicurezza nelle comunicazioni) e la ricerca di una sua soluzione (attraverso strumenti matematici), come detto nel paragrafo precedente, offrono allo studente l'occasione di riflettere sul ruolo che hanno le scienze e la matematica nella vita quotidiana dell'uomo e di vedere la matematica come prodotto culturale. Gli aspetti matematici possono contribuire a mostrare agli allievi l'importanza pratica della dimostrazione (sicurezza che non ci siano eccezioni ad esempio) e anche le applicazioni di strumenti matematici di base (come ad esempio la fattorizzazione o il calcolo del massimo comun divisore) a problemi concreti e rilevanti.

L'idea che dovrebbe accomunare tutti i percorsi dovrebbe essere quella di partire inizialmente dal problema: inviare messaggi che anche se intercettati non possano essere compresi (o meglio siano molto difficile da comprendere). A partire dal problema gli studenti sono stimolati sia a forzare messaggi cifrati con metodi semplici che possono far riferimento a cifrari storici, sia a inventarsi metodi di cifratura è discuterne la complessità e l'efficacia (ad esempio nella possibilità di scambiarsi in modo sicuro la chiave di cifratura), cercandone debolezze e punti di forza.

In un secondo momento, mostrata la vulnerabilità dei metodi classici (e presumibilmente anche di quelli proposti dagli allievi) si passa alla crittografia moderna spiegando, in un contesto in cui sono già discussi e condivisi le problematiche e gli obiettivi del crittare, come l'uso dei numeri e lo sviluppo dei calcolatori hanno rivoluzionato il modo di fare crittografia, rendendo necessario lo sviluppo di adeguati e specifici strumenti informatici e matematici. Questo tipo di discorso può essere spinto, per gli studenti più interessati, fino ad aspetti molto complessi.

Se si arriva a trattare RSA si suggerisce di dedicare almeno un incon-

tro alla presentazione dell'idea di crittografia a chiave pubblica (come ci si arriva, cosa significa,...) e alla descrizione di RSA, comprensiva di un esempio numerico, come quello svolto nella parte dei contenuti. Solo dopo che i passaggi dell'algoritmo saranno ben chiari si potrà passare alla loro dimostrazione. Infatti, il passaggio dai cifrari storici all'algoritmo RSA presenta alcune difficoltà intrinseche di cui è bene tenere conto nell'organizzazione del percorso.

A parte le difficoltà tecniche nel caso in cui si decida di affrontare la dimostrazione del funzionamento di RSA, la cosa di per sé importante è far apprezzare l'idea che sta dietro a RSA e che lo differenzia dai cifrari storici.

In primo luogo il passaggio da una chiave simmetrica a una asimmetrica: mittente e destinatario usano chiavi differenti, ma non solo, addirittura una delle due chiavi è pubblica e non segreta!

In secondo luogo è il destinatario che fornisce al mittente la chiave con cui crittare il messaggio da inviare. Non è un dettaglio di poco conto: significa che ognuno di noi può crearsi una chiave propria, nell'eventualità di essere il destinatario di un messaggio segreto. Questo fa sì che, inoltre, un'unica chiave (anzi, una coppia di chiavi) vada bene per qualsiasi comunicazione rivolta a un certo destinatario: infatti non ha importanza chi sia chi manda il messaggio, dato che in ogni caso l'unico in grado di decifrarlo, una volta trasformato con la chiave di crittazione (pubblica), sarà il destinatario, cioè colui che possiede la chiave di decrittazione (privata).

Infine RSA tratta di numeri: si passa dal sostituire una lettera con un'altra (seguendo, è vero, un procedimento preciso e reversibile, ma che coinvolge pur sempre lo scambio di lettere) al manipolare numeri, che magicamente tornano fuori dopo passaggi aritmetici diversi e apparentemente senza senso.