

Un approccio alla teoria dei numeri in I liceo
basato sulla crittografia per stimolare la curiosità
dell'allievo e migliorare la qualità
dell'apprendimento

Christian Ferrari

8 maggio 2009

Sommario

In questo testo presentiamo una sperimentazione didattica volta a stimolare e migliorare l'apprendimento dei rudimenti della teoria dei numeri, sfruttando il potenziale interesse degli allievi per un tema di matematica applicata: la crittografia a chiave pubblica RSA. L'obiettivo è quello di presentare \mathbb{Z}_n con la sua particolare aritmetica e le diverse basi numeriche così da implementare il protocollo di crittografia RSA. L'aspetto della sicurezza è affrontato studiando alcune caratteristiche dei numeri primi. Un ruolo importante è assunto dai software Maple ed Excel, che permettono sia di scoprire proprietà aritmetiche interessanti, sia di implementare alcuni semplici algoritmi e simulare un reale protocollo crittografico. La sperimentazione è monitorata sia attraverso l'apprendimento degli allievi, sia sui loro commenti sull'attività svolta.

Indice

1	Introduzione	3
2	La costruzione del percorso didattico	4
2.1	Contestualizzazione del percorso nel corso di prima liceo	4
2.2	Riflessioni sugli aspetti disciplinari	5
2.3	Considerazioni di carattere storico	7
2.4	Obiettivi	8
3	Lo svolgimento del percorso didattico	8
3.1	La fase di scoperta	9
3.2	La fase di messa a punto	9
3.3	Il ruolo del software Maple	10
3.4	Traccia dello svolgimento delle attività	11
4	Oltre il percorso didattico proposto	11
4.1	Un complemento interessante per la prima liceo	12
4.2	Crittografia e teoria dei numeri negli studi liceali	12
4.3	Crittografia e teoria dei numeri nella didattica in generale	13
5	La valutazione del percorso didattico	13
5.1	Valutazione dell'apprendimento degli allievi	13
5.2	Valutazione da parte degli allievi	16
6	Conclusione	16
	Bibliografia	19
A	Materiale didattico	20
A.1	Scheda per la fase di scoperta	20
A.2	Scheda di esercizi	25
A.3	Scheda per l'attività sulla fattorizzazione	29
A.4	Presentazione beamer riassuntiva	31
B	Materiale per la valutazione	32
B.1	Valutazione sommativa	32
B.2	Analisi della valutazione sommativa	33
B.3	Questionario di valutazione	36
B.4	Risultati del questionario di valutazione	38

1 Introduzione

L'obiettivo principale del mio intervento didattico, che descriverò nel presente lavoro di documentazione, è quello di affrontare alcuni aspetti elementari della teoria dei numeri dal punto di vista della crittografia. In particolare saremo interessati al protocollo di crittografia a chiave pubblica scoperto nel 1977 dai tre matematici R. Rivest, A. Shamir e L. Adleman al Massachusetts Institute of Technology (MIT) [16], che ha preso universalmente il nome di crittografia RSA. Questo sistema è alla base della maggior parte dei sistemi di protezione dell'informazione, dalle carte bancarie ad Internet, ed è quindi diventato un prodotto commerciale della matematica [28] di alto valore aggiunto.

Dal punto di vista pedagogico-didattico, l'interrogativo alla base di questo lavoro è il seguente: "Può un'attività di matematica applicata fungere da catalizzatore per l'apprendimento di alcuni concetti elementari della teoria dei numeri?" Chiaramente questa domanda può essere estesa a molti argomenti trattati nel corso di matematica liceale e non solo alla teoria dei numeri.

La scelta di questo tema scaturisce dalla considerazione che la crittografia implementata sulla teoria dei numeri, o più genericamente la necessità di scambiare dati in modo sicuro, è certamente un argomento che può suscitare interesse nei liceali. Infatti nasconde un qualcosa di misterioso che può fungere da elemento scatenante per stimolare la curiosità degli allievi. D'altronde, gli scambi di informazione segreta sono sempre stati di fondamentale importanza nella società, sia civile sia militare [19]. All'inizio del XXI secolo, quando la tecnologia legata all'informazione ha cominciato ad avanzare sempre più velocemente, la possibilità di scambiare informazione in modo sicuro è diventata una necessità di primaria importanza non solo nell'ambito militare ma anche in quello civile, toccando tutti. A tale riguardo la crittografia coglie un aspetto a mio avviso molto importante, ossia che la matematica non è una disciplina fine a se stessa, ma è presente anche nella "vita di tutti i giorni", benché a volte in modo nascosto. La crittografia permette quindi di mostrare come la matematica sia uno strumento utile ed efficace per svolgere determinati compiti importanti nel mondo tecnologico: vi è in questo una spendibilità culturale della matematica, aspetto, questo, che purtroppo è spesso trascurato.

Nelle prossime sezioni esamineremo in primo luogo la costruzione del percorso didattico e in seguito ne descriveremo lo svolgimento. La contestualizzazione di quanto sviluppato al di là del corso di prima liceo è l'oggetto di alcune ulteriori considerazioni. L'analisi sul "terreno" del percorso proposto, con lo scopo di monitorare l'intervento didattico, sarà debitamente illustrata. In sede di conclusione, alla luce dell'esito ottenuto, si farà una riflessione critica sul lavoro svolto.

2 La costruzione del percorso didattico

In questa sezione, dopo la contestualizzazione del percorso didattico nel quadro del corso di prima liceo, analizzeremo gli argomenti di carattere disciplinare necessari alla crittografia RSA e i concetti generali soggiacenti, in relazione alla loro importanza nel percorso formativo liceale; particolare attenzione sarà data ai possibili ostacoli all'apprendimento. Tutto ciò permetterà di motivare le scelte didattiche. Si faranno alcune considerazioni storiche e si espliciteranno gli obiettivi del percorso costruito.

2.1 Contestualizzazione del percorso nel corso di prima liceo

Consideriamo il contesto del corso di prima liceo nel quale è stata inserita la serie di attività didattiche proposte (ulteriori considerazioni di carattere più generale sono sviluppate nella sezione 4). Se analizziamo il piano degli studi liceali [22] o il piano di sede del Liceo di Locarno [23], notiamo che tra i campi di studio figura la voce *Numeri*, che concretamente nella pratica professionale coincide con la sistemazione chiara e precisa delle proprietà fondamentali degli insiemi numerici. Partendo dall'insieme dei numeri naturali, si percorrono, per estensione, l'insieme dei numeri relativi, quello dei numeri razionali e infine quello dei numeri reali. Questo percorso, che richiede circa tre settimane, permette di parificare le competenze degli allievi in entrata al liceo, anche se si tratta di argomenti già affrontati nella scuola media. La necessità di provvedere a questa parificazione non permette, per ragione di tempo, di affrontare aspetti di carattere più profondo dal punto di vista disciplinare inerenti gli insiemi numerici, in particolare i numeri naturali e relativi che toccano diverse tematiche interessanti. Senza la necessità di un formalismo eccessivamente complesso, diverse questioni di primaria importanza per quella parte della matematica che si occupa dei numeri, ossia l'aritmetica o più generalmente la teoria dei numeri, restano così all'oscuro degli allievi. A tal proposito diversi temi interessanti, e con un grado di approfondimento superiore a quanto svolto nel corso tradizionale [9], possono essere trovati nella pubblicazione della Commissione Romana di Matematica intitolata *Algèbre* [4]. Il percorso proposto si inserisce quindi molto bene come modalità in grado di completare la formazione degli allievi sul fronte dell'aritmetica, senza nel contempo prolungare eccessivamente la parte iniziale di parificazione sopra menzionata. Considerando il fatto che la maggior parte di quanto proposto trova spazio nel laboratorio di matematica, la collocazione temporale non è influenzata e quindi permette al corso tenuto a classe riunita di avanzare secondo una tempistica accettabile. A tal proposito non va infatti dimenticato che, nel limite del possibile, il corso di matematica dovrebbe essere minimamente coordinato con il resto delle discipline scientifiche, in modo particolare con la fisica. Un allungamento dello studio degli insiemi numerici secondo uno schema d'insegnamento formale non è da ritenere idoneo, per ragioni di tempo, ma anche per ragioni di modalità didattica. La teoria dei numeri, che a prima vista potrebbe sembrare arida, può essere presentata in modo più accattivante, per esempio, come applicazione alla crittografia.

2.2 Riflessioni sugli aspetti disciplinari

Per poter strutturare in modo adeguato il percorso didattico, è di fondamentale importanza analizzare gli aspetti disciplinari coinvolti nel progetto. Infatti lo studio della crittografia RSA non è un tema che fa capo a un unico aspetto disciplinare, ma ne coinvolge parecchi; per questo motivo, prima di cominciare la progettazione dell'attività da svolgere in classe, è importante focalizzare tutti gli elementi necessari; questo permette inoltre di identificare sin dall'inizio le maggiori difficoltà. A tal proposito è utile descrivere sommarariamente la struttura del protocollo che verrà studiato.

Alice e Bob vogliono scambiare messaggi segreti, per questo necessitano di un sistema di protezione dell'informazione. Visto e considerato che si trovano a grande distanza, e che non è sensato che si incontrino, lo scambio di una chiave condivisa per mezzo della quale è possibile codificare in modo sicuro i messaggi è impossibile. Un protocollo di questo tipo è noto come crittografia a chiave privata o crittografia simmetrica, metaforicamente corrisponde alla situazione in cui Alice e Bob (e solo loro) possiedono la stessa chiave per chiudere una cassaforte nella quale viene inserito il messaggio. Vista la situazione, essi devono ricorrere alla crittografia a chiave pubblica o crittografia asimmetrica, che metaforicamente corrisponde alla situazione seguente: Bob (che sarà il destinatario) invia ad Alice una cassaforte con due aperture e una chiave monouso (chiamata chiave pubblica); la mittente, dopo aver inserito il messaggio, chiude la cassaforte e invia il tutto a Bob, che avendo la chiave della seconda apertura (chiamata chiave privata), può accedere al messaggio.

Le necessità matematiche per realizzare un tale protocollo crittografico nella versione RSA sono le seguenti:

- possibilità di codificare un testo in un numero;
- possibilità di cifrare il messaggio da inviare con la chiave pubblica e di decifrarlo con la chiave privata;
- garanzia che il messaggio inviato nella forma cifrata non sia (facilmente) decifrabile da un'eventuale spia.

Questi aspetti di ordine pratico sono realizzati grazie alla teoria dei numeri, sfruttando i seguenti aspetti disciplinari:

- differenti *basi numeriche*, per codificare un testo in un numero che fungerà da messaggio da cifrare e decifrare;
- *aritmetica modulare*, quale elemento di base per cifrare e decifrare il messaggio;
- *complessità computazionale*, quale aspetto legato alla sicurezza del sistema utilizzato.

Sommarariamente ecco quindi gli elementi indispensabili. È ora necessario approfondire questi concetti e la loro applicazione alla crittografia RSA, così da scorgere gli aspetti di dettaglio necessari all'apprendimento dell'intero protocollo. Ecco quindi l'essenza del protocollo RSA.

1. Bob sceglie due numeri primi p e q con i quali calcola $n = pq$ e la funzione di Euler $\varphi(n) = (p - 1)(q - 1)$. Egli sceglie inoltre un numero

$e < \varphi(n)$ coprimo a $\varphi(n)$ (ossia tale che $\text{MCD}(e, \varphi(n)) = 1$) e calcola poi un numero d tale che $ed \equiv 1 \pmod{\varphi(n)}$ (d è l'inverso di e in $\mathbb{Z}_{\varphi(n)}$ la cui esistenza è garantita dalla condizione di coprimalità vista sopra). La coppia (n, e) costituisce la chiave pubblica che Bob invia ad Alice.

2. Alice trasforma il messaggio in un numero (decimale) M tale che $M < n$. Per effettuare questa operazione essa associa a ogni lettera di un alfabeto prescelto un numero, la sequenza di numeri associati al messaggio va poi trasformata nel numero decimale M . Alice infine cifra il messaggio che viene inviato a Bob calcolando

$$C \equiv M^e \pmod{n} .$$

3. Bob decifra il messaggio grazie alla chiave privata (n, d) calcolando

$$C^d \pmod{n} \equiv M .$$

La sicurezza di questo metodo di crittografia sta nella difficoltà di determinare d conoscendo solo n e non la sua fattorizzazione $n = pq$.

Vediamo quindi apparire diversi concetti dell'aritmetica, quali: numero primo, numeri coprimi (e quindi massimo comun divisore), funzione $\varphi(n)$ di Euler, trasformazione in diverse basi numeriche, calcolo modulo n , inverso modulo n , potenze modulo n , fattorizzazione in numeri primi, difficoltà di fattorizzazione. Possiamo ora strutturare i vari concetti da mettere in gioco, identificando i punti critici.

Concetti disciplinari

- *I numeri naturali e i numeri relativi*: numeri primi, fattorizzazione in numeri primi di un numero naturale (teorema fondamentale dell'aritmetica), divisione euclidea in \mathbb{Z} , difficoltà di fattorizzazione, test di primalità.
- *Il massimo comun divisore, il teorema di Bézout e gli algoritmi di Euclide*: metodi di calcolo del massimo comun divisore nel caso di grandi numeri tramite algoritmi, numeri coprimi.
- *Gli anelli \mathbb{Z}_n e la loro aritmetica*: congruenza e classi di resto, addizione, moltiplicazione, potenze e algoritmo di Legendre, inversi e algoritmi di calcolo, alcune proprietà degli elementi di \mathbb{Z}_n inerenti l'esistenza dell'inverso, il piccolo teorema di Fermat, la funzione $\varphi(n)$ di Euler, il teorema di Euler.
- *Basi numeriche*: notazione posizionale, numeri in base differente da 10, definizione di alfabeti e trasformazione di un testo in un numero e viceversa.

Gli aspetti di carattere generale presenti nei concetti disciplinari sopracitati sono da ricondurre al concetto di *algoritmo* e a quello di *complessità computazionale*. Il primo è inerente il calcolo del massimo comun divisore grazie all'algoritmo di Euclide, al calcolo dell'inverso modulo n basato sul teorema di Bézout e sull'algoritmo di Euclide esteso e al calcolo rapido delle potenze in \mathbb{Z}_n con l'algoritmo di Legendre. Il secondo riguarda il problema

della fattorizzazione in numeri primi di un numero con molte cifre.

Va notato che alcuni dei concetti elencati nei primi due punti sono già a conoscenza degli allievi, perché marginalmente trattati nella scuola media e poi ripresi nel capitolo iniziale del corso di prima liceo. Benché possano quindi essere considerati come dei prerequisiti, essi andranno comunque ripresi così da garantirne l'assimilazione da parte di tutti.

Difficoltà

Percorrendo i concetti esposti sopra, si possono intravedere alcune difficoltà legate agli anelli \mathbb{Z}_n e alla trasformazione di un numero da una base all'altra. Queste difficoltà sono da ricondurre al fatto che sono temi nuovi, un po' particolari e che escono apparentemente dalla "realtà quotidiana" degli allievi, e non a una loro difficoltà intrinseca. Con una presentazione adeguata e riconducibile a casi concreti, queste difficoltà possono essere superate senza troppe difficoltà.

La vera difficoltà è invece da ricondurre al concetto e il calcolo dell'inverso modulo n di un dato elemento. Da una parte, anche se l'elemento in questione differisce dall'elemento neutro additivo, l'inverso in \mathbb{Z}_n non esiste necessariamente; dall'altra il calcolo esplicito dell'inverso, quando esiste, non è di semplice esecuzione. Particolare attenzione deve quindi essere prestata a questo aspetto, che tuttavia non può essere omissivo.

Infine è possibile che alcuni allievi manifestino difficoltà in relazione all'utilizzo dei software Excel e Maple, difficoltà che può essere sormontata affiancando agli allievi in difficoltà allievi che padroneggiano il mezzo informatico.

Oltre alle difficoltà sopramenzionate, vi è un aspetto che, se trascurato, può generare difficoltà di tipo computazionale; si tratta del calcolo di una potenza in \mathbb{Z}_n quando l'esponente è un numero assai grande. A tal riguardo è quindi necessario fornire agli allievi un algoritmo in grado di evitare di calcolare esplicitamente $a^b \bmod n$.

2.3 Considerazioni di carattere storico

La storia della matematica permette di affrontare lo studio di determinati argomenti in modo interessante (pensiamo ad esempio alle equazioni polinomiali), e in particolare mostra agli allievi come la matematica, spesso vista come scienza statica e "fuori del tempo", è invece esattamente l'opposto, ossia una scienza in continua evoluzione sviluppata da personaggi più o meno autorevoli. Nel contesto di questo percorso didattico non si intende utilizzare la storia come filo conduttore, ma è comunque interessante mostrare agli allievi alcuni aspetti storici relativi in particolare ai numeri primi. A tale scopo gli aspetti storici vanno introdotti come complementi di informazione, mostrando che l'interesse per i numeri primi risale all'antica Grecia, i più antichi studi sui numeri primi sono infatti contenuti negli *Elementi* di Euclide (composti tra il IV e il III secolo a.C.). Vanno poi citati i lavori di Pierre de Fermat e di Marin Mersenne, che ripresero lo studio dei numeri primi nel XVII secolo. A proposito di Mersenne è interessante citare il fatto che egli si interessò ai numeri primi nella forma $2^p - 1$, con p primo, numeri che oggi sono chiamati in suo onore primi di Mersenne. Infatti il più grande numero primo conosciuto (a

ottobre 2008 [27]) è proprio il numero di Mersenne $M_{43112609} = 2^{43112609} - 1$. Vanno pure sottolineati i risultati ottenuti da Eulero nel corso del XVIII secolo e da Gauss sul volgere del secolo. Infine è interessante notare come i numeri primi restarono confinati nell'ambito della matematica pura fino agli anni settanta, quando fu sviluppato il concetto di crittografia a chiave pubblica; forse la cosa più sorprendente della crittografia RSA sta nel fatto che il protocollo si basa su proprietà matematiche dei numeri relativi conosciute a partire dal XVIII secolo, o addirittura dal XVII secolo con i lavori di Fermat, anche se la potenza di calcolo necessaria per la concretizzazione pratica allora non era disponibile.

A proposito della crittografia è interessante affrontare anche una delle tecniche più antiche: il cifrario concepito da Giulio Cesare. Questo ha almeno tre vantaggi dal punto di vista formativo: permette di mostrare come la problematica della sicurezza dell'informazione sia molto antica, di esercitare l'aritmetica modulare in \mathbb{Z}_{26} , ciò che necessita la messa in corrispondenza delle lettere dell'alfabeto a numeri, e di mostrare un sistema elementare di crittografia a chiave privata.

2.4 Obiettivi

Gli obiettivi di questo percorso didattico possono essere riassunti nel modo seguente. Da una parte si vuole migliorare la formazione degli allievi nel quadro dell'aritmetica e, nel contempo, come già esplicitato nel titolo, si vuole stimolare la curiosità degli allievi verso un aspetto della matematica applicata a una situazione del "mondo reale". I due obiettivi chiaramente sono intrecciati; in particolare il secondo dovrebbe fungere da catalizzatore per il primo. Come terzo obiettivo vi è pure quello di iniziare gli allievi al software Maple e di rafforzare le loro competenze con il software Excel, questo per mostrare loro che la matematica può essere svolta anche con l'ausilio del mezzo informatico. Ciò è di grande importanza sia per i corsi di approfondimento che seguiranno, sia per integrare l'informatica nel quadro del corso di matematica così come auspicato dalla politica informatica di sede.

3 Lo svolgimento del percorso didattico

Lo svolgimento del percorso didattico si articola nelle due fasi descritte qui di seguito. Da notare che, dal punto di vista del materiale didattico, la fase di scoperta è stata gestita con una scheda quale filo conduttore. Mentre nella fase di messa a punto si è preferito utilizzare la lavagna affiancata dal beamer, solo dopo il consolidamento dei concetti fondamentali è stata distribuita una presentazione beamer riassuntiva. Per i dettagli si rinvia il lettore all'allegato A, in cui è possibile trovare il materiale didattico consegnato agli allievi. Questo materiale è pure messo a disposizione degli allievi nella pagina di matematica del sito web [24].

3.1 La fase di scoperta

Lo scopo della fase di scoperta è di incuriosire gli allievi verso la crittografia RSA, così da motivarli per lo studio dell'aritmetica che sta alla sua base. Questa fase è quindi molto superficiale dal punto di vista matematico; sono infatti presentate le linee generali della crittografia RSA grazie all'ausilio di esempi semplici svolti con il software Maple, che in prima battuta gioca quindi il ruolo di "scatola nera". Gli allievi devono "scoprire che funziona" senza però capire i dettagli dei passaggi matematici messi in atto. Dopo questa prima attività, è fondamentale sintetizzare in modo chiaro le diverse fasi del protocollo di crittografia RSA, in modo tale che quando saranno approfonditi, tutti abbiano in chiaro perché si studiano determinati aspetti dell'aritmetica. In particolare la fase di scoperta permette di sollevare tre problemi computazionali fondamentali dell'aritmetica modulare che rendono evidente la necessità di uno studio più approfondito dell'aritmetica: il calcolo delle potenze $a^b \bmod n$, il calcolo del massimo comun divisore tra due numeri grandi, il calcolo dell'inverso in \mathbb{Z}_n . Questi tre aspetti dovranno fungere da catalizzatore per lo studio dell'aritmetica modulare.

Al termine di questa fase, gli allievi devono poi esercitarsi su una parte del protocollo con esempi *ad hoc* proposti dal docente, in altre parole su esempi in cui le difficoltà saranno appositamente contenute ma permetteranno di scorgere le tre problematiche sopraelencate. Dal punto di vista dell'aritmetica, questa fase permette di avvicinare l'aritmetica modulare attraverso esempi semplici, come pure di cominciare a capire la necessità di tradurre il testo in un numero. Questa prima fase è gestita prevalentemente nel laboratorio di matematica.

3.2 La fase di messa a punto

Quando gli allievi cominciano a capire "come funziona" il protocollo di crittografia RSA, sono coinvolti in diverse attività volte ad apprendere gli elementi di matematica fondamentali atti al controllo di tutte le fasi sintetizzate in precedenza. Esse sono gestite nel laboratorio di matematica ed in parte nel corso a classe riunita; quest'ultima modalità è utilizzata in particolare quando vengono ripresi alcuni concetti di base già parzialmente studiati nel capitolo sugli insiemi numerici o nei momenti di sintesi. Ecco alcuni dettagli inerenti le possibili difficoltà menzionate alla fine della sezione 2.2.

Per introdurre gli insiemi \mathbb{Z}_n e l'aritmetica modulare, si sfruttano situazioni concrete quali l'aritmetica dell'orologio o quella del calendario della settimana; questo approccio didattico è assai diffuso [5, 10, 20]. Infine è pure interessante la strutturazione dei numeri relativi secondo lo schema proposto da [3] così da facilitare la classificazione degli elementi in \mathbb{Z} nelle classi di resto.

Per gli aspetti legati alle operazioni in \mathbb{Z}_n , un'entrata in materia sfruttando un percorso di scoperta, basato sulla costruzione esplicita delle tavole di addizione e di moltiplicazione [12], si rivela particolarmente adeguato. Questo ha il vantaggio di "visualizzare" tutte le operazioni e scoprire interessanti caratteristiche degli insiemi \mathbb{Z}_n , così da poter formulare delle congetture che, in un secondo tempo, andranno poi enunciate come teoremi.

Per la difficoltà inerente l'inverso modulo n , la proposta di calcolarlo in modo sistematico mediante un algoritmo, congiuntamente con la classificazione

di \mathbb{Z} come proposto in [3], è probabilmente la soluzione meno complicata, a condizione di esercitarla con una certa determinazione. Un elemento di motivazione per superare questa difficoltà sta nel fatto che per “rompere” il codice RSA, o per creare una chiave segreta, è proprio necessario calcolare l’inverso modulo n ; questo si rivela quindi un elemento fondamentale per le attività che seguono. Infine il problema delle potenze in \mathbb{Z}_n può essere risolto presentando un algoritmo di calcolo rapido delle potenze (algoritmo di Legendre), sfruttando la scrittura dell’esponente come somma di potenze di 2 (ossia la sua scrittura binaria).

In entrambi i casi, l’implementazione degli algoritmi con il software Excel è importante, infatti, essendo obbligati a “programmare” gli algoritmi, gli allievi devono aver capito questo concetto generale, nonché il dettaglio del calcolo specifico inerente il problema affrontato.

Per quel che concerne le differenti basi numeriche, la base 60 dei secondi e dei minuti può essere di aiuto; vi è anche la possibilità di introdurre il sistema binario così da mostrare il sistema numerico utilizzato nei computer e applicare concretamente la scomposizione in base 2 di un numero nel quadro dell’algoritmo di Legendre.

Segnaliamo infine che una breve introduzione ai logaritmi permette di affrontare la quantificazione del numero di cifre di un numero dato e di inquadrare meglio il problema della complessità computazionale della fattorizzazione in numeri primi. Concretamente si presenta il logaritmo in base a con la stessa identica procedura utilizzata per introdurre la radice n -esima.

Terminato l’insegnamento dei concetti matematici necessari alla crittografia RSA, viene ripreso il protocollo precedentemente abbozzato mostrando come i dettagli appresi si rivelano essenziali. Quale attività finale gli allievi svolgono un’attività-gioco utilizzando il protocollo di crittografia RSA per scambiarsi messaggi.

3.3 Il ruolo del software Maple

Il ruolo fondamentale del software Maple è quello di indagare sul problema della difficoltà di fattorizzare i numeri in numeri primi con il crescere del numero di cifre. Grazie ai comandi di Maple, è infatti possibile ottenere velocemente numeri primi con molte cifre, come pure procedere alla fattorizzazione in numeri primi di grandi numeri visualizzando il tempo di calcolo. Gli allievi possono cercare una relazione tra il numero di cifre e il tempo di calcolo, inserendo i dati ottenuti dall’“esperienza informatica” nel software Excel. Questa attività, ispirata da [12], permette infine di stimare il tempo di calcolo richiesto per fattorizzare un numero con molte cifre come quelli realmente utilizzati nei protocollo di crittografia RSA; interessante è il confronto di questo valore con l’età presunta dell’Universo.

3.4 Traccia dello svolgimento delle attività

La fase di scoperta è stata organizzata nel modo seguente.

1. *Introduzione alla crittografia*: la crittografia e la differenza tra crittografia a chiave privata e crittografia a chiave pubblica.
2. *Esempio storico*: il cifrario di Cesare per avvicinarsi a \mathbb{Z}_n quale esempio di crittografia a chiave privata.
3. *Introduzione al protocollo RSA con Maple*: è presentata una simulazione con il software Maple così da permettere una sintesi delle fasi del protocollo.
4. *Iniziazione al protocollo RSA*: vengono presentati esempi semplici poi affrontati dagli allievi.

La fase di messa a punto è invece stata articolata come segue.

1. *L'aritmetica modulare e gli insiemi \mathbb{Z}_n* : sulla base degli elementi già parzialmente messi in campo nella fase di scoperta si definisce \mathbb{Z}_n con la sua particolare aritmetica. Viene ripreso il concetto di divisione euclidea e particolare importanza è data alla questione delle potenze e dell'inverso; come complemento e obiettivo di sviluppo gestito nell'ottica della differenziazione, sono presentati alcuni concetti legati alle strutture algebriche.
2. *Dal testo al numero e viceversa*: utilizzando alcune idee già messe in campo precedentemente, si affronta il problema delle diverse basi numeriche e la possibilità di associare un numero intero a una stringa di testo e viceversa.
3. *Alcune proprietà dei numeri primi e la sicurezza della crittografia RSA*: vengono ripresi alcuni concetti già incontrati all'inizio dell'anno scolastico e in seguito sono approfonditi aspetti della teoria dei numeri primi in relazione alla sicurezza della crittografia RSA; per analizzare il problema è introdotto il concetto di logaritmo. Come obiettivo di sviluppo, sempre nell'ottica della differenziazione, si abbozza il concetto di test di primalità.
4. *RSA in sintesi con i nuovi elementi dell'aritmetica*: si formalizza il protocollo di crittografia RSA grazie alla nuova matematica appresa e vengono svolte attività-gioco supportate dai software Excel e Maple. Come obiettivo di sviluppo, sempre nell'ottica della differenziazione, si approfondisce la questione della firma digitale.

4 Oltre il percorso didattico proposto

In questa sezione analizziamo la localizzazione del percorso didattico proposto nel contesto più ampio degli studi liceali; particolare riguardo è dato alle ricadute di questo progetto per gli allievi e alle possibilità di reinvestimento di quanto proposto. Infine è pure interessante contestualizzare quanto svolto nel quadro delle esperienze didattiche svolte in altre sedi o in altre scuole.

4.1 Un complemento interessante per la prima liceo

Il percorso proposto può essere coordinato con un'altra attività di laboratorio inerente la crittografia. Infatti, secondo il piano di sede del liceo di Locarno [23], tra i campi di studio figura pure la voce *Elementi di statistica*, che viene trattata appunto nel contesto del laboratorio. Vediamo come: tra le diverse attività inerenti la statistica che il docente può proporre vi è la crittoanalisi, che si presta molto bene come complemento alla crittografia RSA proposta in questo progetto. Infatti tra i vari metodi crittografici la sostituzione monoalfabetica o polialfabetica è di particolare interesse dal punto di vista matematico, proprio perché grazie all'analisi statistica delle frequenze è possibile decifrare il testo codificato secondo queste tecniche. L'attività presentata qui riguarda *la crittografia e la teoria dei numeri*, si potrebbe pensare a un'attività simile per *la crittoanalisi e la statistica*. Le due attività permetterebbero di mostrare le due facce della *crittologia*, quella dei creatori di cifrari (la crittografia) e quella dei solutori di cifrari (la crittoanalisi). Per completare la visione storica dell'argomento, l'assegnazione della lettura del libro di Simon Singh *Codici e segreti* [19] permetterebbe agli allievi di venire a conoscenza della lunga lotta tra creatori e solutori di cifrari e come questo aspetto abbia influenzato anche il corso della storia.

4.2 Crittografia e teoria dei numeri negli studi liceali

Oltre alla prima liceo, l'aritmetica non trova più spazio nel piano base della formazione liceale, quindi la teoria dei numeri resta confinata a poche proprietà essenzialmente già incontrate nella scuola media. Credo invece che uno spazio invece molto interessante, ma scarsamente utilizzato, nel quale è possibile sviluppare maggiormente la teoria dei numeri e la crittografia, sia l'opzione complementare di matematica, collocata nel secondo biennio. È facilmente immaginabile proporre quale filo conduttore del corso il tema *informazione e matematica*, nel quale, come primo tema, si affronta la teoria dei numeri, in modo chiaramente più approfondito che in prima liceo, così da ottenere un "pacchetto" *crittografia e teoria dei numeri*; in seguito si approfondisce l'argomento *crittoanalisi e statistica*. Dopodiché, sempre in relazione alla teoria dei numeri e marginalmente agli aspetti crittografici, si studia il tema dei *codici correttori*, un altro campo in cui la matematica si applica nella nostra vita quotidiana; infatti senza questi codici il trasferimento di dati numerici (CD, ...) non sarebbe utilizzabile. Infine si potrebbe collegare il concetto di informazione a quello di probabilità analizzando casi elementari della *teoria di Shannon*.

Vediamo quindi che la teoria dei numeri e la crittografia offrono molte attività realizzabili al liceo, che possono senz'altro essere gestite con successo nell'opzione complementare di matematica. Il vantaggio delle tematiche sopra elencate sta nel fatto che spesso i prerequisiti sono quelli della prima liceo; inoltre esse sono legate a aspetti della matematica che, sebbene in modo nascosto, fanno parte della nostra vita quotidiana sempre più tecnologica. Mi risulta, a tal proposito, che solamente al liceo di Lugano 1 [17] è stata proposta un'attività in questa direzione, mentre diverse sono le proposte di lavori di maturità in quest'ambito. Anche nel quadro dell'opzione specifica fisica e applicazioni della matematica, il tema crittografia potrebbe trovare

un collocamento appropriato; infatti lo sviluppo della fisica quantistica ha portato alla creazione di un protocollo di *crittografia quantistica* [8, 18]; di conseguenza una trattazione della crittografia da più punti di vista sarebbe sicuramente interessante per l'allievo. Infine, considerando il rafforzamento del concetto dell'interdisciplinarietà sancito dalla piccola riforma dell'ORM, si potrebbe pensare di sperimentare un'opzione complementare a cavallo tra matematica e fisica quantistica moderna (non quindi una versione ristretta dell'opzione specifica fisica e applicazioni della matematica) avente quale filo conduttore il concetto di informazione.

Considero quindi che quanto sviluppato in questo lavoro offra numerosi spunti per nuove attività didattiche.

4.3 Crittografia e teoria dei numeri nella didattica in generale

Altri autori si sono dedicati alla crittografia nel quadro dell'insegnamento liceale. La crittografia, quale tema di matematica, sta entrando in modo sempre più importante nei curricula di studio liceali della vicina penisola, dove le esperienze didattiche in tale direzione si stanno moltiplicando. Esse vanno da interventi intensivi concentrati su poche giornate [1, 12] ad attività didattiche organizzate in diverse unità separate [25, 26]. A livello svizzero l'attenzione verso la crittografia è stata concretizzata con la pubblicazione da parte della Commissione Romanda di Matematica di un quaderno destinato al corso Fisica e Applicazioni della Matematica [15]. È pure interessante osservare che attività semplici di crittografia RSA sono state proposte anche nella scuola media [7]. Le esperienze a livello liceale sopraccitate sono state spesso finalizzate a un approfondimento dell'argomento tale da indirizzare l'attività didattica a classi di terza e quarta liceo, mentre nel presente lavoro ci si è focalizzati sulle classi di prima liceo. In questo progetto lo scopo per l'allievo è quindi focalizzato sullo "scoprire che funziona" e "come funziona" senza la pretesa di dimostrare il teorema RSA che spiega il "perché funziona", aspetto, questo, che può essere affrontato in un corso di approfondimento.

5 La valutazione del percorso didattico

Da un punto di vista operativo, la valutazione del percorso didattico è stata effettuata con lo scopo di verificare le competenze di aritmetica e crittografia apprese dagli allievi (sapere e saper fare) come pure di valutare come gli allievi hanno percepito e vissuto questo soggetto (saper essere).

5.1 Valutazione dell'apprendimento degli allievi

La valutazione del grado di apprendimento degli allievi è stata gestita tramite una valutazione sommativa (vedi allegato B.1), nella quale si sono volute monitorare sia le competenze di crittografia RSA, sia quelle relative alla teoria dei numeri. Essa è stata costruita in modo da poter valutare ogni singolo obiettivo. Considerato il fatto che l'attività proposta è molto particolare, non è possibile eseguire una valutazione per confronto, ossia che attesti un miglioramento partendo da una situazione di partenza data.

Qui di seguito sono riportate le tabelle riassuntive in cui sono elencati gli obiettivi e il tasso di riuscita, come pure due grafici che illustrano il risultato d'assieme della classe. Maggiori dettagli possono essere trovati nell'analisi della valutazione sommativa riportata nell'allegato B.2.

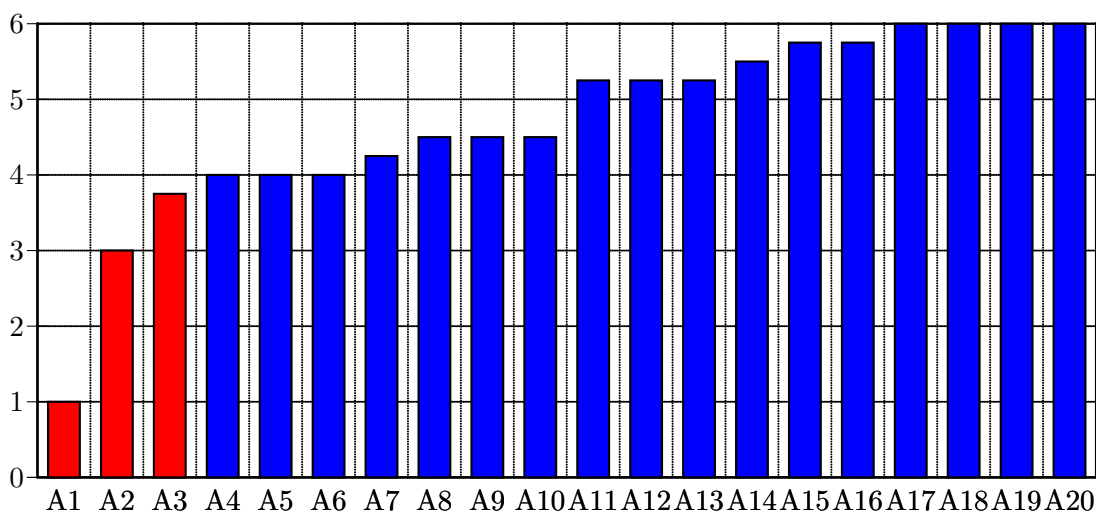
Competenze di crittografia RSA

Obiettivo	% Tasso di riuscita
Generazione chiave pubblica	86
Generazione chiave privata	65
Lunghezza minima chiave	71
Possibilità di sezionare il testo	70
Conversione testo \rightarrow numero	74
Conversione numero \rightarrow testo	68
Ciframento	70
Deciframento	65
Sicurezza di RSA	79
Media RSA	72

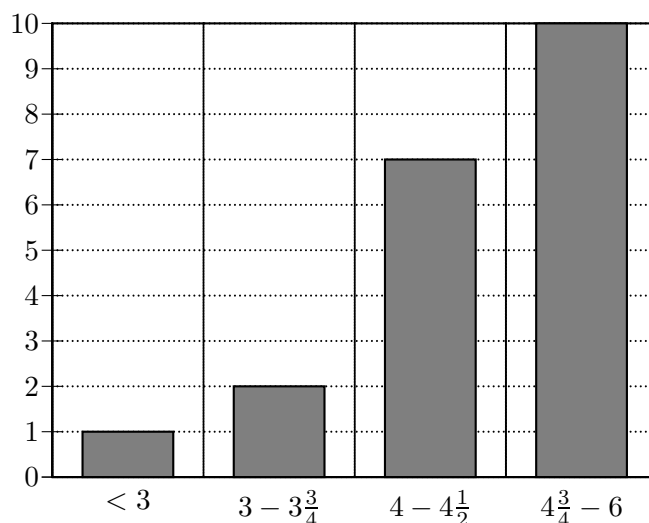
Competenze di teoria dei numeri

Obiettivo	% Tasso di riuscita
Fattorizzazione	85
La fattorizzazione : NP	68
Conversione da base 10 a base b	74
Conversione da base b a base 10	68
Potenze in \mathbb{Z}_n e algoritmo di Legendre	70
MCD e algoritmo di Euclide	65
Algoritmo di Euclide esteso	84
Inverso in \mathbb{Z}_n	65
Funzione $\varphi(n)$ di Euler	95
Media teoria dei numeri	75

Risultato (nota) dei singoli allievi



Risultato d'assieme della classe per fascia di note



Analizzando i risultati riportati nelle tabelle precedenti, possiamo notare che il risultato complessivo come gruppo classe è dato da un tasso di riuscita superiore al 70%, sia per quel che riguarda l'aspetto crittografia RSA, sia per quello inerente la teoria dei numeri. Ecco alcuni commenti più specifici.

- A proposito di quella che era ritenuta la difficoltà maggiore, ossia il calcolo dell'inverso in \mathbb{Z}_n , è possibile notare come la competenza di calcolo, cioè l'applicazione dell'algoritmo di Euclide esteso, ha ottenuto un elevato tasso di successo, mentre il calcolo dell'inverso presenta un risultato più che accettabile ma meno marcato. La differenza è imputabile essenzialmente al fatto che alcuni allievi hanno "perso" punti a causa di errori di calcolo, ciò che ha portato a un abbassamento del tasso di riuscita del risultato finale, ossia l'inverso in \mathbb{Z}_n .
- Gli ostacoli associati al calcolo delle potenze in \mathbb{Z}_n sono stati degnamente superati grazie alla buona assimilazione dell'algoritmo di Legendre. Anche qui si sono purtroppo riscontrati alcuni errori di calcolo.
- Va notato come il risultato inerente il massimo comun divisore (MCD) e l'algoritmo di Euclide non sia rappresentativo, infatti quattro allievi non hanno affrontato la verifica della coprimalità tra il valore e scelto e $\varphi(n)$ (da notare che tre di essi hanno comunque svolto correttamente l'algoritmo di Euclide esteso, che ingloba l'algoritmo di Euclide).

Analizzando il grafico che illustra il risultato d'assieme della classe, possiamo notare come si ottiene il grafico di apprendimento [6]. Questo tipo di risultato attesta un buon apprendimento del gruppo classe: il numero di allievi per fascia cresce con l'aumentare della nota assegnata, esso attesta quindi che la maggior parte degli allievi ha raggiunto gli obiettivi preposti.

Poiché valutare significa anche valutarsi, dall'analisi della prova sommativa, possiamo affermare che, visto il risultato dei singoli obiettivi disciplinari unitamente al risultato d'assieme della classe, l'attività didattica proposta è stata portata a termine con successo.

5.2 Valutazione da parte degli allievi

Al termine del percorso didattico è stato sottoposto agli allievi un questionario di valutazione, con lo scopo di “misurare” come loro hanno vissuto questo capitolo sia dal punto di vista disciplinare (difficoltà, struttura, ...) sia dal punto di vista dell'interesse verso quanto studiato (vedi allegato B.3). I risultati possono essere letti nell'allegato B.4; ecco alcune considerazioni generali sui sette punti presenti nel questionario.

- La fase di scoperta è stata ritenuta utile e di lunghezza adeguata dalla grande maggioranza degli allievi. Per la metà della classe questa attività ha permesso di intravedere a sufficienza ostacoli legati all'implementazione della crittografia RSA, mentre per un terzo degli allievi queste difficoltà sono apparse in modo chiaro.
- La strategia adottata per introdurre \mathbb{Z}_n (tabelle, classificazione in righe) è stata ritenuta utile per due allievi su tre.
- Gli approfondimenti di teoria dei numeri gestiti tramite algoritmi sono stati valutati di difficoltà iniziale media-alta, mentre, dopo opportuna esercitazione, queste difficoltà sono scemate e la maggioranza degli allievi ha ritenuto di padroneggiarli senza difficoltà. Quasi tutti hanno capito le necessità crittografiche inerenti agli approfondimenti di teoria dei numeri svolti (il 55% in modo chiaro, mentre solo il 10% non ha colto la connessione crittografia-teoria dei numeri).
- L'integrazione di Excel è stata ritenuta utile e anche interessante da due allievi su tre e per la grande maggioranza la difficoltà delle attività proposte è stata media o bassa.
- Così come presentato, l'insegnamento della crittografia RSA e della teoria dei numeri a essa connessa può essere considerato, per quel che concerne la sua difficoltà, un capitolo che ben si inserisce nel programma di prima liceo.
- L'esperienza di essere confrontati con un soggetto di matematica applicata come la crittografia RSA è ritenuta positiva per la grande maggioranza degli allievi, solo uno di loro la ritiene negativa.
- Il materiale didattico preparato e consegnato dal docente è ritenuto buono da 9 allievi su 10.

In base a queste considerazioni, possiamo affermare che il feedback ricevuto dagli allievi è globalmente positivo, sia per quel che concerne la realizzazione del percorso didattico, sia per quanto riguarda la loro esperienza personale.

6 Conclusione

L'idea di una fase di scoperta nella quale si mettono in campo tutti gli elementi del protocollo di crittografia RSA è stata vincente e apprezzata dagli allievi; essa ha permesso di stabilire il filo conduttore delle attività più formalizzate messe in atto nella fase di sviluppo. In quest'ultima, come attestato anche dagli allievi, è stato possibile motivare la necessità di approfondire determinati aspetti della teoria dei numeri con il loro risvolto pratico nel campo della

crittografia. Ad esempio, le operazioni di ciframento e deciframento definite inizialmente per mezzo del calcolo del resto della divisione euclidea per n sono state poi rapportate alla relazione di congruenza modulo n . Le difficoltà degli allievi nel calcolare esplicitamente i resti delle divisioni euclidee per n delle potenze M^e e C^d , nel caso di grandi numeri, ha motivato l'approfondimento del calcolo delle potenze in \mathbb{Z}_n . Infine l'approfondimento del problema dell'inverso moltiplicativo in \mathbb{Z}_n è stato facilmente motivato con le necessità della generazione della chiave privata. Un discorso analogo vale per lo studio delle differenti basi numeriche.

Si è rivelata molto proficua la gestione degli insiemi \mathbb{Z}_n , con le loro particolarità aritmetiche, utilizzando le tavole di addizione e di moltiplicazione così come introdotte in [12], e gestite in tempo reale con la proiezione del foglio di calcolo Excel, unitamente alla strutturazione di \mathbb{Z} come proposto in [3]. Queste modalità sono state molto apprezzate dagli allievi e hanno permesso di "scoprire" diversi aspetti importanti, non tra i più semplici, per esempio le caratteristiche delle operazioni di addizione e moltiplicazione in \mathbb{Z}_n oppure la problematica dell'esistenza dell'elemento inverso moltiplicativo. A mio modo di vedere, questo modo di procedere ha permesso di eliminare molte delle difficoltà soggiacenti a questi insiemi numerici dalle caratteristiche particolari.

L'integrazione del software Excel quale mezzo informatico, per implementare gli algoritmi fondamentali alla crittografia RSA, è stato ritenuto utile e interessante da una buona maggioranza degli allievi, cosa che si è anche tradotta in un buon apprendimento dell'aspetto algoritmico. Questa attività ha pure motivato un paio di allievi, che già padroneggiavano la programmazione php, a creare piccoli programmi in grado di eseguire alcuni degli algoritmi presentati in classe (vedi la pagina di matematica del sito web [24]), ciò è senza dubbio una chiara testimonianza del grande interesse che la tematica ha suscitato in alcuni ragazzi.

Infine, l'attività sulla complessità della fattorizzazione in numeri primi, svolta con i software Maple ed Excel, è stata particolarmente istruttiva, perché ha permesso di mostrare il nocciolo della sicurezza del protocollo RSA su un piano accessibile agli studenti e che hanno potuto "toccare con mano". Inoltre questa attività ha mostrato alla classe che anche il calcolo per mezzo del computer ha dei limiti, aspetto istruttivo in relazione al problema della complessità computazionale.

In relazione alla domanda iniziale, "Può un'attività di matematica applicata fungere da catalizzatore per l'apprendimento di alcuni concetti elementari della teoria dei numeri?", credo di poter rispondere affermativamente, sia in base al risultato complessivo scaturito dalla valutazione dell'apprendimento, ottenuto dall'analisi della prova sommativa, sia sulla scorta delle considerazioni seguenti. Come detto sopra, l'aggancio quasi costante con le necessità matematiche della crittografia RSA ha potuto stimolare gli allievi, per lo meno per il fatto che hanno potuto e dovuto mettere in atto le loro competenze matematiche in un contesto concreto che esula dal classico corso di matematica. Inoltre il taglio scelto, che puntava sulla scoperta, parzialmente supportato dai software Maple ed Excel, trascurando gli aspetti più formali (comunque importanti ma probabilmente non a livello della prima liceo), ha permesso di coinvolgere anche gli allievi meno inclini alla matematica, che in

generale hanno ottenuto risultati discreti nella valutazione sommativa. Malgrado non si possa pretendere che gli allievi siano in grado di lavorare con il classico rigore matematico, sono convinto che l'attività proposta abbia permesso loro di "aprire gli orizzonti" sui fondamenti della matematica, ossia l'aritmetica. Infatti, la possibilità di essere confrontati con un insieme numerico dalle proprietà particolari come \mathbb{Z}_n , che differiscono dalle classiche proprietà degli insiemi \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} già conosciute all'arrivo al liceo, permette sicuramente di migliorare la qualità dell'apprendimento, perché l'allievo è obbligato a riflettere in un contesto nuovo e inusuale, ad esempio il significato profondo dell'esistenza dell'elemento inverso moltiplicativo che permette di affrontare, quale obiettivo di sviluppo, concetti non banali come quelli di divisori di zero e di campo. Questo consente di mostrare come gli assiomi di anello e campo, che non vanno appresi a memoria ma che l'élève devono saper utilizzare e riconoscere in casi particolari, sono alla base dell'aritmetica. In questo contesto gli anelli \mathbb{Z}_n e i campi \mathbb{Z}_p , anche per la loro caratteristica di insiemi finiti, offrono un contesto di studio dal carattere semplice ma nello stesso tempo profondo.

Ringraziamenti

Il presente lavoro è il frutto di un'esperienza didattica svolta al Liceo di Locarno con la classe IG, che ringrazio quindi della disponibilità ad accogliere un tema che solitamente non viene affrontato nei programmi standard liceali. È anche grazie alla disponibilità del Prof. Michele Impedovo che questo lavoro è stato possibile: egli si è messo a disposizione con molto entusiasmo e ha seguito con interesse la mia sperimentazione; ho potuto usufruire dei suoi preziosi consigli e parte del suo materiale didattico, ma mi ha anche permesso di "fare di testa mia", cosa che ho particolarmente apprezzato. Infine ringrazio la collega Karima Pabst e il Prof. Patrik Ferrari (Università di Bonn) per la rilettura critica del presente documento, come pure Margherita Nosedà per i preziosi consigli.

Riferimenti bibliografici

- [1] G. Alberti, *Aritmetica e crittografia*, Università di Pisa (2001)
- [2] J.D. Barrow, *Perché il mondo è matematico*, Bollati-Boringhieri (1992)
- [3] J. Conway, R. Guy, *Il libro dei numeri*, Hoepli (2003)
- [4] CRM, *Fundamentum de mathématique: Algèbre*, Tricornè (1996)
- [5] M. Délès, *Jouer avec les congruences*, Bulletin de la SSPMP **104** (2007)
- [6] E. Dozio, *La valutazione*, Corso ASP (2003)
- [7] F. Eugeni, R. Mascella, D. Tondini, *La crittografia a chiave pubblica per giocare e imparare: il gioco del codice RSA*, Periodico di Matematiche **1** (2001)
- [8] C. Ferrari, *Fisica quantistica: un approccio moderno*, note personali (2008)
- [9] L. Filippini, *Appunti di matematica*, Liceo di Locarno (2007)
- [10] R. Friedberg, *An adventurer's guide to number theory*, Dover (1994)
- [11] G.H. Hardy, E.M. Wright, *An introduction to the theory of numbers - Sixth edition*, Oxford (2008)
- [12] M. Impedovo, *Aritmetica e crittografia: l'algoritmo RSA*, Progetto Alice **21** (2006)
- [13] M. Impedovo, *Calcolo 2: Strutture algebriche e calcolo letterale*, Corso ASP (2008)
- [14] S. Loepp, W.K. Wootters, *Protecting information*, Cambridge (2006)
- [15] N. Martignoni, *Cryptologie*, Chaiers de la CRM n°2 (2004)
- [16] R. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM **21** (1978)
- [17] L. Rovelli, comunicazione privata
- [18] V. Scarani, *Quantum physics a first encounter*, Oxford (2006)
- [19] S. Singh, *Codici e segreti*, Fabbri (2001)
- [20] A. Stucki, *Etait-ce un vendredi 13?*, Bulletin de la SSPMP **93** (2003)
- [21] P. Wassef, *Arithmétique: application aux codes correcteurs et à la cryptographie*, Vuibert (2008)
- [22] *Piano quadro degli studi liceali*, Ufficio dell'insegnamento medio superiore
- [23] *Piano di sede del gruppo di Matematica*, Liceo di Locarno
- [24] http://www.liceolocarno.ch/Liceo_di_Locarno/Internetutti/ferrari/mateI.html
- [25] <http://critto.liceofoscarini.it/>
- [26] <http://lnx.liceogaribaldi.it/moodle/login/index.php>
- [27] <http://primes.utm.edu/>
- [28] <http://www.rsa.com/>
- [29] <http://www.math.sunysb.edu/~scott/Book331/>
(Mathematical problem solving with computers)
- [30] <http://it.wikipedia.org/wiki/>

A Materiale didattico

A.1 Scheda per la fase di scoperta

Introduzione alla crittografia ed alcuni esempi introduttivi

Presentazione

In questa serie di attività affronteremo un tema di matematica applicata con lo scopo di mostrare come questa disciplina non sia fine a se stessa, come spesso si sente affermare, ma che presenta applicazioni nella vita di tutti i giorni. Gli scambi di informazione sono sempre stati di fondamentale importanza nelle società, sia civile sia militare. Ai giorni nostri, in una società in cui la tecnologia legata all'informazione avanza a una velocità sempre più frenetica, la possibilità di scambiare informazione in modo sicuro è diventata una necessità di primaria importanza. Già nell'antichità, Giulio Cesare aveva concepito una tecnica in grado di scambiare informazione in modo (abbastanza) sicuro; poi durante la prima e la seconda guerra mondiale altri sforzi in questa direzione furono intrapresi. Nell'era dell'informatica, e in particolare di Internet, la questione dello scambio sicuro di informazione riguarda non più soltanto l'ambito militare ma anche quello civile e concerne tutti: pensiamo ad esempio alle carte bancarie oppure all'acquisto on-line.

Con questa serie di attività, vedremo diversi aspetti della matematica in azione, con lo scopo ultimo di approfondire e capire il sistema maggiormente utilizzato per rendere sicuro lo scambio di informazioni; avremo quindi la possibilità di approfondire diversi aspetti dell'aritmetica in un contesto applicato come la *crittografia*, ossia la scienza che si occupa della sicurezza dell'informazione.

Per tutte queste attività è fondamentale avere la calcolatrice!

Introduzione alla crittografia

I possibili metodi crittografici si suddividono in due grandi classi.

- La *crittografia a chiave privata*: Alice e Bob vogliono scambiare informazioni in modo segreto: Alice nasconde il messaggio originale grazie a una chiave k conosciuta solo da lei e da Bob, che grazie alla *stessa* chiave k decifra il messaggio; per questo motivo questo sistema è anche chiamato *crittografia a chiave simmetrica*.
- La *crittografia a chiave pubblica*: Alice e Bob vogliono scambiare informazione in modo segreto: Alice nasconde il messaggio originale grazie a una chiave e fornita da Bob e di dominio pubblico; quest'ultimo, grazie a un'altra chiave d , conosciuta solo da lui, decifra il messaggio; per questo motivo questo sistema è anche chiamato *crittografia a chiave asimmetrica*.

Possiamo rappresentarci i due metodi con la seguente analogia. Metaforicamente la crittografia a chiave privata corrisponde alla situazione in cui Alice e Bob (e solo loro) possiedono la *stessa* chiave per chiudere una cassaforte nella quale viene inserito il messaggio; mentre la crittografia a chiave pubblica metaforicamente corrisponde alla situazione in cui Bob (che sarà il destinatario) invia ad Alice una cassaforte con due aperture e una chiave monouso (la chiave pubblica); dopo aver inserito il messaggio, Alice la chiude e invia il tutto a Bob, che, avendo la chiave della seconda apertura (la chiave privata), può accedere al messaggio.

Entrambi i metodi hanno vantaggi e svantaggi.

- *Crittografia a chiave privata*: il vantaggio è l'assoluta segretezza della comunicazione; lo svantaggio (non irrilevante!) è la necessità che Alice e Bob si incontrino per scambiarsi in modo assolutamente sicuro la chiave k , a tal proposito è importante osservare che, affinché la comunicazione sia assolutamente sicura, è necessario che la chiave k sia utilizzata una sola volta.
- *Crittografia a chiave pubblica*: il vantaggio è che Alice e Bob non necessitano di incontrarsi; è sufficiente che il destinatario comunichi (anche non in modo sicuro) la **chiave pubblica** e con la quale il mittente cifra il messaggio (mentre la **chiave privata** è unicamente conosciuta dal destinatario); lo svantaggio sta nel fatto che conoscendo la chiave pubblica e è fondamentale essere certi che nessuno sia in grado di recuperare la chiave privata d ; questo dipende dal dettaglio del sistema di crittografia.

Tra i metodi di crittografia a chiave pubblica vi è la crittografia RSA, che si fonda sulla teoria dei numeri e la cui sicurezza, come vedremo, è garantita dalla difficoltà di fattorizzare in numeri primi numeri con molte cifre.

Un esempio storico

Una delle prime tecniche di crittografia è il *cifrario di Cesare*, che consiste nello scrivere il messaggio originale e poi nel sostituire tutte le lettere con la terza lettera seguente. Ad esempio la A è sostituita con la D , la B con la E e via di seguito, e una volta raggiunta l'ultima lettera si ricomincia da capo, esattamente come se le lettere fossero disposte in modo circolare: per esempio la Z è sostituita con la C . Il destinatario per decifrare il messaggio non fa altro che operare la sostituzione al contrario.

- Ad ogni lettera dell'alfabeto (composto dalle 26 lettere)

$ABCDEFGHIJKLMNOPQRSTUVWXYZ$

si associa un numero da 0 a 25 nel modo seguente:

$A \leftrightarrow 0 \quad B \leftrightarrow 1 \quad C \leftrightarrow 2 \quad \dots \quad Y \leftrightarrow 24 \quad Z \leftrightarrow 25$

al messaggio viene poi assegnata una lista di numeri e viceversa.

- Per *cifrare* il messaggio è sufficiente aggiungere a ogni numero 3 (che gioca il ruolo di *chiave*, che può essere cambiata) considerando i numeri da 0 a 25 disposti in modo circolare; la lista di numeri così ottenuta costituisce il messaggio da inviare.

- Per *decifrare* il messaggio è sufficiente sottrarre a ogni numero della lista 3 o aggiungere 23(= 26 - 3) sempre con i numeri disposti in modo circolare.

Questo protocollo è un esempio concreto di *crittografia a chiave privata*; infatti il numero 3 gioca il ruolo della chiave ed è la stessa per il mittente e il destinatario, i quali devono essere gli unici ad esserne a conoscenza.

Osserviamo che, se ai tempi di Cesare poteva funzionare, questo sistema è poco sicuro, perché conoscendo il messaggio cifrato, ma non la chiave, è sufficiente provare le 26 possibilità per decifrare il messaggio.

Esercizio Da svolgere in gruppi (3/4 persone).

1. Provate a scambiare alcuni messaggi semplici.
2. Costruite poi la tavola di addizione per l'insieme dei numeri da 0 a 25 disposti circolarmente.
3. Trovate che relazione esiste tra l'equivalenza $24 + 3 \equiv 1$ e il resto della divisione euclidea $27 : 26$ o tra l'equivalenza $2 + 3 \equiv 5$ e il resto della divisione euclidea $5 : 26$?
4. Conoscete altri esempi di numeri circolari?

Un'introduzione al protocollo RSA con Maple

Come prima attività possiamo simulare il protocollo RSA grazie a una serie di operazioni eseguite dal software Maple; lo scopo non è quello di capire in dettaglio come si eseguono le operazioni, bensì di conoscere quali sono le operazioni necessarie sia alla *trasmissione dell'informazione* sia alla *generazione delle chiavi* pubblica e privata.

Esercizio

1. Riassumi le operazioni fondamentali della crittografia RSA.
2. Qual è la differenza tra crittografia a chiave privata e crittografia a chiave pubblica?
3. Perché la crittografia RSA è a chiave pubblica?

Cominciamo a eseguire il protocollo RSA

Lo scopo di questo esempio semplice è di impratichirsi del protocollo RSA senza però avere la necessità di conoscere tutti i concetti di aritmetica alla sua base; si tratta quindi di eseguire determinate operazioni semplici. L'attività è da svolgere in gruppi di 3/4 persone e quando si incontrano difficoltà di calcolo (numeri troppo grandi) ci si rivolge al docente.

Sia dato un messaggio $\mathcal{M} = \mathcal{M}_1\mathcal{M}_2 \dots \mathcal{M}_\ell$ costituito di una sequenza di lettere dove per ogni $1 \leq i \leq \ell$

$$\mathcal{M}_i \in \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\} .$$

Più avanti avremo bisogno di introdurre lo spazio tra caratteri, a esso assoceremo il numero 0, la corrispondenza carattere \leftrightarrow numero vista sopra è quindi spostata a destra di un'unità, ossia

$$A \leftrightarrow 1 \quad B \leftrightarrow 2 \quad C \leftrightarrow 3 \quad \dots \quad Y \leftrightarrow 25 \quad Z \leftrightarrow 26 .$$

Dopo aver associato al messaggio una lista di numeri, lo scopo è di cifrare alcuni messaggi *lettera per lettera* grazie alla chiave pubblica, costituita dalla coppia di numeri (n, e) , e inviarli a due compagni del gruppo, i quali dovranno decifrarli grazie alla chiave privata, anch'essa data da una coppia di numeri (n, d) . Ecco le chiavi fornite.

Chiave numero	Chiave pubblica	Chiave privata
1	$(n = 35, e = 7)$	$(n = 35, d = 7)$
2	$(n = 33, e = 7)$	$(n = 33, d = 3)$
3	$(n = 34, e = 3)$	$(n = 34, d = 11)$
4	$(n = 39, e = 5)$	$(n = 39, d = 5)$
5	$(n = 51, e = 11)$	$(n = 51, d = 3)$
6	$(n = 38, e = 5)$	$(n = 38, d = 11)$
7	$(n = 33, e = 9)$	$(n = 33, d = 9)$
8	$(n = 33, e = 9)$	$(n = 3, d = 9)$
9	$(n = 35, e = 5)$	$(n = 35, d = 5)$

Per codificare e decodificare, esegui le seguenti operazioni; M_i indica il numero associato alla lettera \mathcal{M}_i del messaggio:

- *codifica*: calcola $(M_i)^e$ e determina il resto della divisione euclidea

$$(M_i)^e : n$$

sia C_i questo numero;

- *decodifica*: calcola $(C_i)^d$ e determina il resto della divisione euclidea

$$(C_i)^d : n$$

il risultato è il numero M_i .

Per concludere analizziamo brevemente le chiavi utilizzate.

Esercizio Per ogni chiave qui sopra:

1. scomponi in fattori primi il numero n , troverai una fattorizzazione del tipo $n = pq$;
2. calcola il valore di $f = (p - 1)(q - 1)$;
3. calcola $\text{MCD}(e, f)$;
4. considerando i numeri circolari da 0 a $f - 1$, determina a che cosa equivale il prodotto ed .

Riassumi le caratteristiche della chiave.

Esercizio Da svolgere in gruppi (3/4 persone).

1. Considera la chiave pubblica ($n = 10, e = 3$), determina la chiave privata (n, d).
2. Considera la chiave pubblica ($n = 15, e = 5$), determina la chiave privata (n, d).
3. Prova a costruire la tavola di moltiplicazione per i numeri circolari da 0 a $f - 1$ nel caso $n = 10$ e $n = 15$.
4. Considera il messaggio di quattro lettere *MATE*. Codifica il messaggio nel modo seguente: a ogni lettera associa il numero m_i come sopra, ma invia ai destinatari (due per gruppo) il numero c_i tale che $m_i c_i \equiv 1$ nell'insieme dei numeri circolari da 0 a 26. Ai destinatari il compito di decodificare il messaggio.
(*Attenzione*: questo non è il protocollo di crittografia RSA).

A.2 Scheda di esercizi

Esercizi di teoria dei numeri e crittografia

Esercizio 1 Costruire le tavole di addizione e di moltiplicazione di: \mathbb{Z}_2 , \mathbb{Z}_3 , \mathbb{Z}_6 , \mathbb{Z}_7 e \mathbb{Z}_9 .

Esercizio 2 Determinare il massimo comun divisore delle seguenti coppie di numeri, utilizzando l'*algoritmo di Euclide*, e dire se i numeri sono coprimi.

1. (15; 6) [3]
2. (345; 75) [15]
3. (987; 610) [1;coprimi]
4. (1233; 9999) [9]
5. (2345; 350) [35]
6. (37; 6576) [1;coprimi]

Esercizio 3 Determinare le seguenti potenze negli anelli \mathbb{Z}_n dati, utilizzando l'*algoritmo di Legendre*.

1. 2^8 in \mathbb{Z}_5 [1]
2. 3^{21} in \mathbb{Z}_{10} [3]
3. 89^{66} in \mathbb{Z}_{91} [64]
4. 58^{37} in \mathbb{Z}_{77} [9]
5. 9^{34} in \mathbb{Z}_{35} [16]
6. 14^7 in \mathbb{Z}_{33} [20]

Esercizio 4 Determinare, se possibile, gli inversi dei seguenti elementi degli anelli \mathbb{Z}_n dati, utilizzando l'*algoritmo di Euclide esteso*.

1. 2 in \mathbb{Z}_5 [3]
2. 18 in \mathbb{Z}_{35} [2]
3. 6 in \mathbb{Z}_{112} [non esiste]
4. 7 in \mathbb{Z}_{67} [48]
5. 4 in \mathbb{Z}_{17} [13]
6. 5 in \mathbb{Z}_{34} [7]

Esercizio 5 Determinare la funzione $\varphi(n)$ di Euler per i seguenti numeri.

1. $\varphi(4)$ [2]
2. $\varphi(5)$ [4]
3. $\varphi(9)$ [6]
4. $\varphi(10)$ [4]
5. $\varphi(17)$ [16]
6. $\varphi(27)$ [18]

Esercizio 6 Determinare (quando esiste) l'inverso dei numeri dell'esercizio 3 con il piccolo teorema di Fermat e il teorema di Euler.

Esercizio 7

1. Sono dati i seguenti numeri in base b , determinare il numero decimale corrispondente.

- | | |
|--------------------------|------------------|
| (a) $(1011001)_2$ | $[(89)_{10}]$ |
| (b) $(3\ 9\ 1\ 15)_{26}$ | $[(58853)_{10}]$ |
| (c) $(171)_8$ | $[(121)_{10}]$ |
| (d) $(441)_5$ | $[(121)_{10}]$ |
| (e) $(567)_{10}$ | $[(567)_{10}]$ |
| (f) $(3\ 9\ 1\ 15)_{27}$ | $[(65652)_{10}]$ |

2. Determinare le cifre dei seguenti numeri decimali nella base data.

- | | |
|-------------------------------|------------------------|
| (a) $(89)_{10}$ in base 2 | $[(1011001)_2]$ |
| (b) $(89)_{10}$ in base 3 | $[(10022)_3]$ |
| (c) $(35)_{10}$ in base 17 | $[(2\ 1)_{17}]$ |
| (d) $(24)_{10}$ in base 24 | $[(1\ 0)_{24}]$ |
| (e) $(58853)_{10}$ in base 26 | $[(3\ 9\ 1\ 15)_{26}]$ |
| (f) $(65652)_{10}$ in base 27 | $[(3\ 9\ 1\ 15)_{27}]$ |

3. Verificare che

$$(75)_{10} = (300)_5 = (203)_6 .$$

Attenzione: Se la base $b > 10$ le cifre $0 \leq \beta_i \leq b - 1$ possono essere composte da due numeri (decimali), esse sono quindi indicate separate da degli spazi.

Esercizio 8 Determinare la lunghezza dei seguenti numeri utilizzando il logaritmo.

$$8 \quad 367 \quad 5654357 \quad 3.5 \cdot 10^3 \quad 6.4 \cdot 10^{32}$$

Esercizio 9 Utilizzare il criterio di primalità basato sul piccolo teorema di Fermat per dimostrare che 8, 15 e 22 *non* sono numeri primi.

Lo scopo degli esercizi seguenti è di applicare le competenze acquisite negli esercizi precedenti al protocollo di *crittografia RSA*.

Esercizio 10 Per i seguenti valori dei numeri primi p e q determinare una possibile coppia di chiavi pubblica e privata.

1. $p = 5, q = 11$
2. $p = 7, q = 3$
3. $p = 13, q = 5$
4. $p = 19, q = 5$
5. $p = 23, q = 3$
6. $p = 17, q = 29$

Esercizio 11 Eseguire la conversione *testo* \leftrightarrow *numero decimale* per i seguenti messaggi/numeri utilizzando l'alfabeto seguente

$$\{ , a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z \}$$

in corrispondenza con i 27 numeri $\{0, 1, 2, 3, \dots, 24, 26\}$.

1. $M = 6568$ [i g]
2. **enigma** [79367311]
3. $M = 13636$ [rsa]
4. **segreto** [7436812407]
5. $M = 52802025$ [cripto]

Esercizio 12 Cifrare e decifrare i seguenti numeri con le chiavi date.

1. $M = 6$ con $(e = 13, n = 55)$ e $(d = 37, n = 55)$ [$C = 51$]
2. $M = 2$ con $(e = 17, n = 33)$ e $(d = 13, n = 33)$ [$C = 29$]
3. $M = 17$ con $(e = 11, n = 86)$ e $(d = 23, n = 86)$ [$C = 67$]
4. $M = 55$ con $(e = 29, n = 143)$ e $(d = 29, n = 143)$ [$C = 22$]
5. $M = 11$ con $(e = 73, n = 249)$ e $(d = 9, n = 249)$ [$C = 206$]
6. $M = 26$ con $(e = 25, n = 395)$ e $(d = 25, n = 395)$ [$C = 151$]

Esercizio 13 Con *Excel* costruire gli algoritmi seguenti.

1. Algoritmo di Euclide per l'MCD;
2. algoritmo di Euclide esteso per l'inverso in \mathbb{Z}_n ;
3. algoritmo semplice per le potenze in \mathbb{Z}_n ;
4. algoritmo di scomposizione di un numero decimale in base 27.

Esercizio 14 Sono date le chiavi pubblica e privata

$$(e = 12575, n = 21949) \quad (d = 12715, n = 21949) .$$

Eseguire, con l'aiuto degli algoritmi dell'esercizio 13, il protocollo RSA con i seguenti messaggi.

1. **rsa** [$M = 13636, C = 9660$]
2. **mate** [**ma+te**: $M_1 = 352, C_1 = 17702; M_2 = 545, C_2 = 21218$]

Esercizio 15 Una spia scopre i seguenti messaggi cifrati C e le chiavi pubbliche (e, n) utilizzati per cifrarli.

1. $C = 373557$ con $(e = 275113, n = 414173)$ [**mate**]
2. $C = 132273$ con $(e = 85311, n = 191329)$
3. $C = 934$ con $(e = 58271, n = 86699)$
4. $C = 20958$ con $(e = 64309, n = 82063)$

Che informazione è necessario avere per decifrare i messaggi cifrati? Cosa è necessario "fare" per ottenere questa informazione?

Rompere poi il codice RSA e scoprire i messaggi originali. Utilizzare gli algoritmi dell'esercizio 13 e *Maple* per fattorizzare n (comando: `ifactor(numero);`).

Esercizio 16 Generare delle chiavi e scambiare messaggi con i compagni utilizzando il protocollo RSA e gli algoritmi *Excel*.

A.3 Scheda per l'attività sulla fattorizzazione

La sicurezza di RSA

Lo scopo di questa attività, supportata dai software Maple ed Excel, è di analizzare il problema della sicurezza del protocollo di crittografia RSA.

Preparazione Procedere con i comandi Maple indicati per ottenere quanto menzionato.

- Per generare dei numeri aleatori
`z:=lunghezza numero;`
`n1:=rand(10^floor(z/2)..10^floor(z/2+1))();`
`n2:=rand(10^floor(z/2)..10^floor(z/2+1))();`
- Per determinare due numeri primi vicini ai numeri generati e moltiplicarli
`p:=nextprime(n1);`
`q:=nextprime(n2);`
`n:=p*q;`
- Per determinare la lunghezza di n
`floor(evalf(log[10](n)+1));`
- Per determinare il tempo di calcolo di un'operazione data
`t:=time();`
`operazione;`
`time() - t;`

La fattorizzazione in numeri primi Con il comando

```
ifactor(n);
```

Maple è in grado di fattorizzare in numeri primi un numero n dato.

1. Genera dei numeri decimali n (con una lunghezza da 12 a 40, per esempio per passi di 4);
2. calcola la lunghezza ℓ e il tempo di fattorizzazione di n ;
3. riporta i valori ottenuti in una tabella Excel;
4. costruisci il grafico della funzione $T(\ell)$;
5. fai tracciare la linea di tendenza con equazione e coefficiente R^2 .

Il calcolo della funzione $\varphi(n)$ di Euler Con il comando

```
with(numtheory):  
phi(n);
```

Maple è in grado di calcolare la funzione $\varphi(n)$ di Euler.

1. Genera dei numeri decimali n (con una lunghezza da 12 a 40, per esempio per passi di 4);
2. calcola la lunghezza ℓ e il tempo di calcolo di $\varphi(n)$;
3. riporta i valori ottenuti in una tabella Excel;
4. costruisci il grafico della funzione $T(\ell)$;
5. fai tracciare la linea di tendenza con equazione e coefficiente R^2 .

Conclusione

1. Che relazione c'è tra i due problemi?
2. Calcola i valori di $T(\ell)$ per $\ell = 300$ (come nei protocollo reali di RSA).
3. Qual è la base della sicurezza della crittografia RSA?

A.4 Presentazione beamer riassuntiva

Riportiamo qui di seguito la presentazione beamer riassuntiva nella quale è possibile riconoscere il percorso didattico svolto.

Vedi [24].

B Materiale per la valutazione

B.1 Valutazione sommativa

Esercizio 1 Nella crittografia RSA la *Certification Authority* (CA) si occupa della gestione delle chiavi. Un generatore di numeri primi casuali della CA ha fornito i seguenti valori 17, 89, 31.

- 1.1 Mostrando in modo chiaro le quattro fasi della generazione delle chiavi costruisci una possibile coppia di chiavi pubblica e privata.
- 1.2 Con la chiave generata nel punto precedente puoi inviare il messaggio *estate* (senza spezzarlo)? In caso di risposta negativa, determina un limite inferiore per il valore di n .

Esercizio 2 Utilizzando la crittografia RSA, vuoi inviare i tuoi saluti (messaggio *ciao*) al presidente Obama. Come devi cifrare il messaggio? Cosa spedisce al presidente degli USA?

Elenco chiavi pubbliche della *Certification Authority*:

Presidente	n	e
Merz	221	137
Obama	91	23
Sarkozy	253	141

Esercizio 3

- 3.1 L'agente segreto 007 scopre il seguente messaggio cifrato $C = 14$ e conosce la chiave pubblica utilizzata per cifrarlo ($e = 5, n = 95$).
 - 3.1.1 Qual è il passo fondamentale per decifrare C ? Esegui.
 - 3.1.2 Determina il messaggio originale.
- 3.2 Una spia trova il messaggio cifrato $C = 16265$ e conosce la chiave pubblica utilizzata per cifrarlo ($e = 9055, n = 24253$). Se essa converte C direttamente in testo che cosa ottiene? Commenta! (Si sa che il testo originale è scritto in italiano).

Esercizio 4

- 4.1 Matematicamente qual è la relazione tra e e d che costituiscono le chiavi? Perché, conosciuto $\varphi(n)$, non è possibile scegliere un qualsiasi $e < \varphi(n)$?
- 4.2 Perché il numero decimale M associato al messaggio non deve superare n ?
Indicazione: Se $M > n$ cosa puoi dire di $C \equiv M^e \pmod n$ e poi di $C^d \pmod n$? Prova con dei numeri piccoli, ad esempio ($e = 3, n = 10$) e $d = 3$.
- 4.3 Qual è la base della sicurezza della crittografia RSA? Motiva la tua risposta!

B.2 Analisi della valutazione sommativa

Riportiamo qui di seguito l'analisi di dettaglio della valutazione sommativa.

Nella tabella seguente sono analizzati i quattro esercizi con i relativi obiettivi specifici, ai quali è associata una lettera esercizio per esercizio.

Esercizio	Obiettivo specifico	Media/Totale	%
1.a	Scelta di n	0.90/1	90
1.b	Calcolo di $\varphi(n)$	0.95/1	95
1.c	Scelta di e	0.95/1	95
1.d	Verifica MCD	0.65/1	65
1.e	Calcolo di d	1.20/2	60
1.f	Algoritmo di Euclide esteso	1.70/2	85
1.g	Conversioni (testo $\rightarrow M$, $b \rightarrow 10$)	0.70/1	70
1.h	Lunghezza minima di n	0.83/1	83
2.a	Possibilità di sezionare il testo	0.70/1	70
2.b	Conversioni (testo $\rightarrow M$, $b \rightarrow 10$)	1.55/2	78
2.c	Ciframento	1.40/2	70
2.d	Potenze in \mathbb{Z}_n e algoritmo di Legendre	1.55/2	78
3.a	Fattorizzazione	0.85/1	85
3.b	Calcolo di d	0.70/1	70
3.c	Algoritmo di Euclide esteso	1.65/2	83
3.d	Deciframento	1.30/2	65
3.e	Potenze in \mathbb{Z}_n e algoritmo di Legendre	1.25/2	63
3.f	Conversioni ($M \rightarrow$ testo , $10 \rightarrow b$)	0.55/1	55
3.g	Conversioni ($M \rightarrow$ testo , $10 \rightarrow b$)	1.60/2	80
3.h	Sicurezza di RSA	0.90/1	90
4.a	Esistenza dell'inverso in \mathbb{Z}_n	1.95/3	65
4.b	Lunghezza minima di n	1.20/2	60
4.c	Sicurezza di RSA + fattorizzazione : NP	1.35/2	68

Le percentuali riportate nella sezione 5.1 sono state ottenute tenendo conto dei diversi obiettivi specifici (vedi tabella precedente) come indicato nella tabella seguente.

Obiettivo RSA	%	punti valutati
Generazione chiave privata	86	1.a + 1.b + 1.c + 1.d
Generazione chiave privata	65	1.e + 3.b
Lunghezza minima chiave	71	1.h + 4.b
Possibilità di sezionare il testo	70	2.a
Conversione testo \rightarrow numero	74	1.g + 2.b
Conversione numero \rightarrow testo	68	3.f + 3.g
Ciframento	70	2.c
Deciframento	65	3.d
Sicurezza di RSA	79	3.h + 4.c
Media RSA	72	
Obiettivo teoria dei numeri	%	punti valutati
Fattorizzazione	85	3.a
La fattorizzazione : NP	68	4.c
Conversione da base 10 a base b	74	1.g + 2.b
Conversione da base b a base 10	68	3.f + 3.g
Potenze in \mathbb{Z}_n e algoritmo di Legendre	70	2.d + 3.e
MCD e algoritmo di Euclide	65	1.d
Algoritmo di Euclide esteso	84	1.f + 3.c
Inverso in \mathbb{Z}_n	65	1.e + 3.b + 4.a
Funzione $\varphi(n)$ di Euler	95	1.b
Media teoria dei numeri	75	

Infine nella tabella seguente riportiamo le note, ordinate in modo crescente, ottenute nella valutazione sommativa dai singoli allievi.

Allievo	Nota
A1	1.00
A2	3.00
A3	3.75
A4	4.00
A5	4.00
A6	4.00
A7	4.25
A8	4.50
A9	4.50
A10	4.50
A11	5.25
A12	5.25
A13	5.25
A14	5.50
A15	5.75
A16	5.75
A17	6.00
A18	6.00
A19	6.00
A20	6.00

Nota: l'allievo A1 ha abbandonato il Liceo all'inizio del mese di aprile.

B.3 Questionario di valutazione

Lo scopo di questo questionario è di raccogliere informazioni utili al docente in merito al percorso svolto sul tema crittografia e teoria dei numeri.

1. Come prima attività abbiamo svolto un'introduzione generale ma superficiale della crittografia.
 - (a) Trovi che questa introduzione, al fine di motivare lo studio di alcuni aspetti della teoria dei numeri (\mathbb{Z}_n , basi numeriche, numeri primi), sia stata
 - Utile
 - Indifferente
 - Inutile
 - (b) Trovi che questa introduzione sia stata
 - Troppo corta
 - Adeguata
 - Troppo lunga
 - (c) Trovi che questa introduzione abbia permesso di intravedere alcuni ostacoli (potenze in \mathbb{Z}_n per cifrare/decifrare, trovare la chiave privata, ...)
 - Sì
 - Abbastanza
 - No
2. L'introduzione di \mathbb{Z}_n è stata gestita con alcuni "trucchetti". In particolare trovi che l'utilizzo dei fogli Excel con le tabelle di \mathbb{Z}_n per il tuo apprendimento sia stato
 - Utile
 - Indifferente
 - Inutile
3. L'approfondimento del calcolo del MCD, dell'inverso in \mathbb{Z}_n e del calcolo delle potenze in \mathbb{Z}_n hanno rappresentato una parte importante della teoria matematica esposta dopo l'introduzione generale.
 - (a) Trovi che questi approfondimenti erano sufficientemente motivati dalle necessità concrete della crittografia RSA
 - Sì
 - Abbastanza
 - No
 - (b) La gestione di questi aspetti tramite l'utilizzo di algoritmi (aspetto nuovo per te) è stato di una difficoltà
 - iniziale* *finale*
 - Bassa Bassa
 - Media Media
 - Alta Alta

4. Nella fase finale gli algoritmi imparati in precedenza sono stati poi gestiti con Excel.
- (a) Trovi che l'integrazione dell'aspetto informatico sia
 - Utile ed interessante
 - Utile ma non interessante
 - Indifferente
 - Inutile
 - (b) Trovi che la "programmazione" degli algoritmi sia di difficoltà
 - Bassa
 - Media
 - Alta
 - (c) Trovi che tu abbia potuto reinvestire le competenze informatiche apprese nel corso di introduzione all'informatica seguito durante il primo semestre?
 - Sì
 - Abbastanza
 - No
5. In complesso hai trovato questo capitolo di una difficoltà
- Minore degli altri capitoli
 - Sullo stesso livello degli altri capitoli
 - Maggiore degli altri capitoli
6. Indipendentemente dai risultati ottenuti, come valuti l'esperienza di essere confrontato con un soggetto di matematica applicata come la crittografia RSA?
- Negativa
 - Indifferente
 - Positiva
7. Come valuti il materiale didattico ricevuto (scheda introduttiva, scheda di esercizi, presentazioni beamer)?
- Scarso
 - Medio
 - Buono
8. Questo capitolo non ha la pretesa di essere perfetto, quindi a te la possibilità di fare osservazioni costruttive.

B.4 Risultati del questionario di valutazione

Riportiamo qui di seguito l'analisi dei risultati del questionario di valutazione.

Domanda	Risposta	totale	%
1a	Utile	15	75
	Indifferente	4	20
	Inutile	1	5
1b	Troppo corta	0	0
	Adeguata	19	95
	Troppo lunga	1	5
1c	Sì	6	32
	Abbastanza	11	58
	No	2	10
2	Utile	13	65
	Indifferente	6	30
	Inutile	1	5
3a	Sì	11	55
	Abbastanza	7	35
	No	2	10
3b (iniziale)	Bassa	0	0
	Media	10	50
	Alta	10	50
3b (finale)	Bassa	14	70
	Media	5	25
	Alta	2	10
4a	Utile ed interessante	13	65
	Utile ma non interessante	2	10
	Indifferente	5	25
	Inutile	0	0
4b	Bassa	9	45
	Media	10	50
	Alta	1	5
4c	Sì	0	0
	Abbastanza	13	65
	No	7	35
5	Minore agli altri capitoli	10	50
	Sullo stesso livello degli altri capitoli	8	40
	Maggiore agli altri capitoli	2	10
6	Negativa	1	5
	Indifferente	2	10
	Positiva	17	85
7	Scarso	0	0
	Medio	2	10
	Buono	18	90