

Numeri primi e poligoni stellati

A cura di Nicoletta Nolli, Silvano Rossetto, Angela Sclavi, Sergio Zoccante

Riferimenti curriculari	2
Indicazioni curriculari	2
Prove INVALSI	3
Descrizione dell'attività	6
Attività 1	6
Attività 2	11
Attività 3	13
Attività 4	15
Indicazioni metodologiche	19
Eventuali difficoltà e suggerimenti	21
Spunti per un approfondimento disciplinare	25
Elementi per prove di verifica	25
Spunti per altre attività con gli studenti	29
Documentazione e materiali	34
Proposta di attività per il corsista	34

Introduzione

Questa attività si colloca all'inizio della classe prima, quando si approfondiscono le informazioni sugli insiemi numerici. Qui si pone in particolare rilievo l'importanza dei concetti "essere primo" ed "essere divisibile".

Si suppone che si siano già richiamate le definizioni di numero primo, di numero composto e di numeri primi fra loro.

L'intenzione è anche quella di porre l'accento sul legame fecondo fra matematica ed arte, illustrando alcune applicazioni in campo artistico della geometria (i mosaici) e intravedendo un nesso fra l'arte e l'aritmetica dei numeri primi.

Riferimenti curriculari

Indicazioni curriculari

Le attività M@t.abel hanno precisi obiettivi di apprendimento che rientrano tra quelli inseriti nelle Indicazioni nazionali attualmente in vigore (D.M. n. 211 del 07/10/2010, Direttiva n. 57 del 15/07/2010, Direttiva n. 65 del 09/07/2010) e nelle Prove INVALSI. All'inizio di ciascuna attività sono riportati, perciò, i relativi riferimenti presenti nelle Indicazioni nazionali e alcuni quesiti delle Prove Invalsi che ripropongono la situazione stimolo dell'attività considerata. Una domanda Invalsi può aiutare a valutare se gli allievi hanno sviluppato, attraverso lo svolgimento dell'attività, la capacità di utilizzare la matematica per rispondere a domande in una situazione specifica. Le domande sono tratte tra quelle presenti nei vari livelli scolastici, in quanto le attività M@t.abel sono pensate in un'ottica di verticalità.

Indicazioni Nazionali per i Licei

Linee generali e competenze

Concetti e metodi che saranno obiettivo dello studio: costruzione e analisi di semplici modelli matematici di classi di fenomeni, anche utilizzando strumenti informatici per la descrizione e il calcolo.

Obiettivi specifici di apprendimento

Aritmetica e algebra

Il primo biennio sarà dedicato al passaggio dal calcolo aritmetico a quello algebrico. Lo studente svilupperà le sue capacità nel calcolo (mentale, con carta e penna, mediante strumenti) con numeri interi.

In questo contesto saranno studiate le proprietà delle operazioni. Lo studio dell'algoritmo euclideo per la determinazione del MCD permetterà di approfondire la conoscenza della struttura dei numeri interi.

Geometria

La realizzazione di costruzioni geometriche elementari sarà effettuata sia mediante strumenti tradizionali sia mediante programmi informatici di geometria.

Istituti Tecnici e professionali

Aritmetica e algebra

Conoscenze

- I numeri: naturali, interi.
- Le operazioni con i numeri interi e loro proprietà.

Abilità

- Utilizzare le procedure del calcolo aritmetico (a mente, per iscritto, a macchina) per calcolare espressioni aritmetiche e risolvere problemi.
- Operare con i numeri interi.

Geometria

Abilità

Eseguire costruzioni geometriche elementari utilizzando la riga e il compasso e/o strumenti informatici.

Prove INVALSI

a.s. 2013/2014 - Domanda D6

Scuola secondaria di II grado – Classe II

- D6. Marco afferma che, per ogni numero naturale n maggiore di 0, $n^2 + n + 1$ è un numero primo. Marco ha ragione?

Scegli una delle due risposte e completa la frase.

☐ Marco ha ragione, perché

.....

☐ Marco non ha ragione, perché

.....

Soluzione INVALSI

Marco non ha ragione perché...

Accettabili tutte le risposte che forniscano un contro esempio. Per esempio: per $n = 4$ si ha 21, che non è primo.

Sono anche accettabili risposte in cui lo studente afferma di aver sostituito a n alcuni numeri senza mostrarli esplicitamente, concludendo che non sempre si ottiene un numero primo.

Esempio:

Ho provato a sostituire a n diversi numeri e ho visto che non sempre si otteneva un numero primo.

Non accettabile:

- Una risposta generica che non contiene un contro esempio.

Esempio:

- la somma non può venire sempre un numero primo
- non tutti i numeri naturali danno come risultato un numero primo

Commento

Ci si aspetta che l'alunno risponda dopo aver fatto qualche tentativo: per $n = 1, 3, 5$ il risultato è un numero primo, mentre per $n = 4, 7, 10 \dots$ (con $n = 3p+1$) viene un multiplo di 3.

Se l'alunno si limita a qualche caso del primo tipo, potrebbe essere indotto ad una risposta affermativa (Marco ha ragione ...) basandosi solo su questi, mentre se trova un esempio del secondo tipo dovrebbe rispondere correttamente con il controesempio.

a.s. 2012/2013 - Domanda D16

Scuola secondaria di II grado – Classe II

D16. Indica se ciascuna delle seguenti proposizioni è vera (V) o falsa (F).

		V	F
a.	Se un numero è pari allora è multiplo di 4	<input type="checkbox"/>	<input type="checkbox"/>
b.	Se un numero è multiplo di 9 allora è multiplo di 3	<input type="checkbox"/>	<input type="checkbox"/>
c.	Un numero è multiplo di 6 solo se è pari	<input type="checkbox"/>	<input type="checkbox"/>
d.	Un numero è multiplo di 5 se e solo se è multiplo di 10	<input type="checkbox"/>	<input type="checkbox"/>

Soluzione INVALSI

D16_a: F

D16_b: V

D16_c: V

D16_d: F

La risposta si considera corretta con 3 risposte corrette fornite su 4 item

Commento

La domanda riguarda l'acquisizione dell'implicazione logica, anche se coinvolge il concetto di multiplo di un numero.

a.s. 2010/2011 - Domanda D4

Scuola secondaria di II grado – Classe II

**D4. Considera l'affermazione: "Per ogni numero naturale n , $2^n + 1$ è un numero primo".
Mostra con un esempio che l'affermazione è falsa.**

.....

.....

.....

Soluzione INVALSI

Per mostrare che l'affermazione basta un solo esempio contrario (che viene detto *controesempio*).

Se scegliamo $n=3$, si ottiene $2^3+1=9$, che non è un numero primo.

Per rispondere correttamente si può anche presentare un esempio diverso da questo.

Ad esempio, si può anche scegliere $n=5$ (si ottiene $2^5+1=33$, che non è primo) oppure $n=6$ (si ottiene $2^6+1=65$ che non è primo), ecc.

Basta fornire un solo contro esempio.

Commento

Dal quaderno "Servizio Nazionale di Valutazione a.s. 2010/11 - Guida sintetica alla lettura della prova di Matematica – Classe seconda – Scuola secondaria di II grado"

Il numero di risposte mancanti è rilevante: quasi il 40% non fornisce alcuna risposta a questa domanda. Fra gli studenti che rispondono 2 su 3 circa danno una risposta corretta.

L'elevato numero di risposte mancanti difficilmente dipende dalla ritrosia, già rilevata anche in altre prove, degli studenti nel fornire giustificazioni, spiegazioni, descrizioni di processi risolutivi. In questo caso, infatti, veniva richiesto solo di esibire un esempio che certificasse la falsità dell'affermazione. È quindi probabile che molti degli studenti che non hanno risposto e quelli che hanno sbagliato abbiano incontrato difficoltà con la logica del controesempio.

Per molti studenti l'affermazione è vera in alcuni casi e falsa in altri, perché perdono di vista il quantificatore universale e il suo ruolo strategico nella determinazione della valutazione di verità della proposizione, prestando solo attenzione alla proposizione aperta $2n + 1$ è primo. Per i diversi valori di n che uno studente può facilmente provare ($n = 0$; $n = 1$; $n = 2$; $n = 4$), $2n + 1$ è un numero primo. Ciò è sufficiente per

concludere che l'affermazione non è falsa, almeno non sempre. Il quesito rischia quindi di non avere senso per molti studenti.

La logica del controesempio può essere compresa, accettata e applicata solo ponendo attenzione sul significato dei quantificatori per la valutazione del valore di verità di una proposizione.

Descrizione dell'attività

Attività 1

Poligoni stellati

Questa attività nasce da un lavoro di Maria Angela Chimetto (si veda la bibliografia)

Fase 1

La prima attività scaturisce dall'osservazione dell'immagine delle decorazioni presenti nel palazzo dell'Alhambra di Granada, in Spagna. Nella figura proposta sono presenti numerosi poligoni regolari di 12 lati, all'interno di ciascuno dei quali si intravedono alcuni poligoni stellati.

L'interesse è quello di individuare, dato un poligono regolare di n lati, quanti sono i poligoni stellati che si possono ottenere a partire da esso.

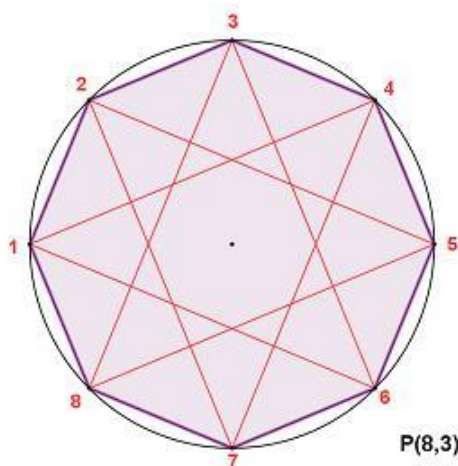


È importante introdurre alcuni concetti prima di procedere con l'attività.

- Definiamo "poligono stellato" una poligonale intrecciata ottenuta partendo da un vertice di un poligono regolare, congiungendo fra loro vertici non consecutivi

con un'unica spezzata (senza alzare la penna dal foglio), e "saltando" ogni volta lo stesso numero di vertici; la spezzata deve risultare chiusa (cioè il primo vertice e l'ultimo devono coincidere) e contenere tutti i vertici del poligono di partenza.

- Definiamo $P(n, k)$ il "poligono derivato" dal poligono regolare di n lati, ottenuto con salti di k lati: quindi $P(8, 3)$ è il poligono derivato dall'ottagono regolare con salti di 3 lati, congiungendo cioè il 1° con il 4° vertice, il 4° con il 7°, ecc.



I vertici del poligono stellato sono nell'ordine: 1, 4, 7, 2, 5, 8, 3, 6

Ci proponiamo di riconoscere, fra tutti i poligoni derivati $P(n, k)$ che si ricavano da un poligono regolare di n lati, quanti sono i poligoni stellati.

Fase 2: Costruisci un poligono stellato

Questa fase si può svolgere vantaggiosamente in laboratorio di informatica, usando un software di geometria dinamica (Cabri 2D o Geogebra), dividendo la classe in gruppi di due studenti.

Dopo aver costruito un poligono regolare, diventa importante la numerazione dei vertici, in modo da individuare il poligono derivato a partire dalla sequenza dei suoi vertici.

Si può partire dalla costruzione dell'ottagono regolare: individuiamo prima i poligoni derivati che se ne deducono e poi, fra questi, gli stellati. Si osserva che dall'ottagono si possono ricavare 2 stellati, secondo il verso di percorrenza (orario o antiorario) seguito. Quindi l'ottagono ha 2 stellati che in realtà coincidono: $P(8,3) = P(8,5)$.

L'insegnante suggerisce quindi di partire dal poligono regolare di 11 lati: quanti stellati si ottengono in questo caso? Facilmente si individuano 4 diversi poligoni stellati: $P(11,2) = P(11,9)$, $P(11,3) = P(11,8)$, $P(11,4) = P(11,7)$, $P(11,5) = P(11,6)$; la coincidenza dei poligoni deriva, come prima, dal fatto che il verso di percorrenza può essere orario o antiorario.

A questo punto l'insegnante chiede: **aumentando il numero di vertici, possiamo aspettarci che aumenti il numero di poligoni stellati?**

Si può arrivare alla risposta esaminando il numero di stellati che si ricavano dal dodecagono regolare, proprio il poligono presente nel mosaico osservato all'inizio; il risultato è sorprendente: il dodecagono ha solo 2 stellati fra loro coincidenti.

Fase 3: Vertici e tabelle

L'insegnante chiede di descrivere in una tabella tutti i poligoni derivati da un poligono regolare dato; ogni poligono derivato è individuato con la sequenza dei suoi vertici.

poligono di 8 lati	1	2	3	4	5	6	7	8
P(8,2)	1		2		3		4	
P(8,3)	1	4	7	2	5	8	3	6
P(8,4)	1				2			
P(8,5)	1	6	3	8	5	2	7	4
P(8,6)	1		4		3		2	

Per esempio, la riga P(8,2) corrisponde al caso in cui partiamo dal vertice 1 e facciamo ogni volta salti di 2 lati: troviamo nell'ordine i vertici 3, 5, 7 e poi torniamo nel vertice 1 (senza essere passati per i vertici pari).

Nella riga successiva, P(8,3), facendo salti da 3, troviamo nell'ordine i vertici 4, 7, 2, ecc.: in questo caso, passiamo per tutti i vertici dell'ottagono e quindi otteniamo un poligono stellato.

poligono di 11 lati	1	2	3	4	5	6	7	8	9	10	11
P(11,2)	1	7	2	8	3	9	4	10	5	11	6
P(11,3)	1	5	9	2	6	10	3	7	11	4	8
P(11,4)	1	4	7	10	2	5	8	11	3	6	9
P(11,5)	1	10	8	6	4	2	11	9	7	5	3
P(11,6)	1	3	5	7	9	11	2	4	6	8	10
P(11,7)	1	9	6	3	11	8	5	2	10	7	4
P(11,8)	1	8	4	11	7	3	10	6	2	9	5
P(11,9)	1	6	11	5	10	4	9	3	8	2	7
P(11,10)	1	11	10	9	8	7	6	5	4	3	2

poligono di 12 lati	1	2	3	4	5	6	7	8	9	10	11	12
P(12,2)	1		2		3		4		5		6	
P(12,3)	1			2			3			4		
P(12,4)	1				2				3			
P(12,5)	1	6	11	4	9	2	7	12	5	10	3	8
P(12,6)	1						2					
P(12,7)	1	8	3	10	5	12	7	2	9	4	11	6
P(12,8)	1	4			3	6			2	5		
P(12,9)	1			5			3			2		4
P(12,10)	1		6		5		4		3		2	7

Note per l'insegnante

1 - Nella tabella del poligono di 8 lati, si fa osservare, colorando lo sfondo, che il numero 8 compare solo nelle righe che contengono tutti i vertici; la tabella del poligono di 11 lati fa osservare, usando colori diversi per i diversi numeri, che l'11 compare in tutte le righe ed inoltre che i numeri uguali sono 'allineati'.

2 - Quando la riga contiene tutti i numeri non ordinati, il poligono è stellato; non vale però il viceversa: ci sono poligoni derivati che risultano stellati ma non contengono tutti i vertici. Ad esempio, nel poligono di 10 lati, D(10,4) ha come vertici 1,5,9,3,7. Si tratta della stella contenuta nel pentagono che, a sua volta, è un derivato del decagono. Anche in questo caso, non contenendo tutti i vertici, il 10 non compare.

Fase 4: Analisi delle tabelle e legame con i numeri primi

L'insegnante chiede se è possibile descrivere le tabelle precedenti in termini matematici, chiarendo le operazioni che permettono di costruirle.

È utile pensare ai 12 vertici del dodecagono come le ore di un orologio analogico: quando le lancette arrivano a 12, ricominciano da 1.

L'idea si può estendere ad altri poligoni regolari, ad esempio a quello di 11 lati.

Osservando le costruzioni e le tabelle ottenute, l'insegnante pone le seguenti domande:

- 1. A quali "salti" corrispondono le righe che non contengono tutti i vertici?**
Le righe incomplete corrispondono a poligoni derivati che non risultano stellati. La risposta è che, in questi casi, il numero di vertici saltati è un numero che non è primo con il numero dei vertici del poligono originario.
- 2. Perché il poligono di 11 lati ha più poligoni derivati di quello di 12?**
Perché 11 è primo con tutti i numeri interi che lo precedono, mentre il 12 è primo solo con 5, con 7 e con 11.

Naturalmente non si considerano i casi in cui i salti hanno lunghezza 1 oppure $n-1$, perché si ritroverebbe il poligono originario e non un poligono stellato.

3. In quale fra i casi esaminati sono più numerose le righe che comprendono tutti i vertici?

Naturalmente con il poligono di 11 lati.

Fase 5: Il dodecagono e l'aritmetica dell'orologio

È facile vedere che, se una spezzata ottenuta con salti di k lati dà luogo a un poligono stellato, allora congiungendo un vertice dopo l'altro vengono compiuti k "giri".

L'insegnante propone di immaginare il dodecagono regolare come un orologio in cui i numeri dei vertici corrispondono alle ore.

Se qualcuno ci chiede: "hai un orologio analogico che segna le sei; devi dire dove si trova la lancetta delle ore fra 5 ore e dopo un successivo intervallo di 5 ore", la risposta è semplicissima: $6 + 5 = 11$, $11 + 5 = 16$. Ma l'orologio non segna 16 ore: arrivato alle 12 ricomincia un nuovo giro; occorre quindi sottrarre: $16 - 12 = 4$ per ottenere la nuova ora. Se da qui si riparte a contare altri intervalli, ogni volta che si supera la 12-sima ora, dal numero ottenuto si deve sottrarre 12: in sostanza, i nostri conti trascurano i multipli di 12.

Questo principio è alla base di un'aritmetica chiamata "aritmetica dell'orologio".

Così, se ora sono le 8, alla domanda: "che ore segnerà l'orologio fra 14 ore?" la risposta viene data addizionando $8 + 14 = 22$ e poi considerando la divisione $22 : 12$; di questa divisione si deve valutare solo il resto:

$22 : 12 = 1$, con resto 10, dunque l'ora segnata è 10.

In linguaggio matematico, l'operazione che calcola il resto di una divisione è indicata con mod, e si dice che ho addizionato 14 ad 8 mod 12, o meglio, che ho calcolato

$$(8 + 14) \bmod 12$$

(mod è l'abbreviazione di modulo e si legge "modulo").

Si dice anche, ad esempio, che $22 \equiv 10 \pmod{12}$ (22 è "congruo" a 10 mod 12) per dire che 10 e 22 hanno lo stesso resto nella divisione per 12.

In definitiva:

La scrittura $a \equiv b \pmod{n}$ significa che a e b hanno lo stesso resto nella divisione per n (dopo avere aggiunto " a " ore, la lancetta dell'orologio con n ore mirerà alla stessa ora che se avessimo aggiunto " b " ore). Dire che a e b hanno lo stesso resto nella divisione per n significa che $a-b$ è divisibile per n .

Dire che $a \equiv r \pmod{n}$, con $0 \leq r < n$, equivale a dire che a è della forma $a = kn+r$ (un multiplo di n più r).

Possiamo anche considerare orologi con un numero diverso di ore, per esempio, un orologio con 7 ore (come i giorni della settimana).

Con questo orologio: $2 + 20 \equiv 1 \pmod{7}$: infatti, pensando ai giorni della settimana, 2 corrisponde a martedì, 20 giorni sono 2 settimane complete più 6 giorni; partendo da martedì e contando 6 giorni si arriva a lunedì.

Una proprietà alla base dell'aritmetica modulo n è che il resto di una somma è uguale alla somma dei resti. Per esempio:

da $25 \equiv 1 \pmod{12}$ e $15 \equiv 3 \pmod{12}$ segue
 $25 + 15 \equiv 1 + 3 \pmod{12}$, cioè $40 \equiv 4 \pmod{12}$.

Naturalmente, se la somma dei resti supera n , è necessario considerare il resto di tale somma:

$30 \equiv 6 \pmod{12}$ $20 \equiv 8 \pmod{12}$
 $6 + 8 = 14 \equiv 2 \pmod{12}$, cioè $30 + 20 = 50 \equiv 2 \pmod{12}$.

Un discorso analogo vale per la moltiplicazione:

da $22 \equiv 2 \pmod{10}$ e $4 \equiv 4 \pmod{10}$
segue $22 \times 4 = 88 \equiv 2 \times 4 \pmod{10}$.

Attività 2

Criteri di divisibilità

Gli alunni conoscono già i criteri di divisibilità per 2, 5, 3 e 9.

Con questa attività si vuole portarli ad una giustificazione di questi criteri.

Due sono le idee guida sottostanti: l'aritmetica dell'orologio (si veda la Fase 5 della prima attività) e la notazione posizionale dei numeri.

Fase 1

Si comincia ponendo il problema: come possiamo verificare rapidamente se un numero m è divisibile per n ? Interessa in questo contesto che sia evidente a tutti che ciò significa: il resto della divisione $m:n$ è 0, ossia, con le notazioni viste nell'attività 1, $(m \equiv 0) \pmod{n}$.

Si porta poi il discorso sui criteri di divisibilità: questi sono metodi veloci per ottenere la risposta senza eseguire la divisione.

Si ricorda il criterio di divisibilità per 10 e si chiede alla classe di giustificarlo. Dalla discussione dovrà emergere che l'ultima cifra fornisce il resto: il numero m può essere riscritto come somma di decine e unità: $m = q \cdot 10 + r$.

Conclusione: un numero è divisibile per 10 se e solo se la sua cifra delle unità è divisibile per 10.

Fase 2

Si passa ora alla divisibilità per 2 e per 5. Si tratta di far emergere che questi sono fattori di 10 e quindi che se un numero è divisibile per 10, allora è anche divisibile per 2 e per 5.

Resta allora da discutere il caso in cui un numero m non è divisibile per 10.

La scrittura già trovata $m = q \cdot 10 + r$ consente di affermare che m è divisibile per 2 o per 5 se tale è r . L'aritmetica dell'orologio (a 10 ore) ci garantisce che il resto della somma è uguale alla somma dei resti.

Conclusione: un numero è divisibile per 2 o per 5 se e solo se la sua cifra delle unità è divisibile per 2 o per 5.

Fase 3

Si pone poi in discussione il criterio di divisibilità per 9.

Qui già la formulazione è più complessa.

1. Si propone di calcolare il resto dei numeri seguenti: 99, 999, 9999, ...
I numeri possono essere riscritti nella forma $9 \cdot 11$, $9 \cdot 111$, $9 \cdot 1111$, ...
per cui è facile concludere che si tratta di multipli di 9 (il resto è 0).
2. Poi si passa al calcolo del resto di 100, 1000, 10000, ...
La risposta è facile con la legge dell'orologio (a 9 ore): il resto della somma è uguale alla somma dei resti.
Ad esempio, $1000 = 999 + 1$, quindi modulo 9 si ha:
 $1000 \equiv 999 + 1 \equiv 0 + 1 = 1$
3. Si propone ora il calcolo del resto di 1000, 2000, 3000, ...
Anche ora la risposta è facile per lo stesso motivo, o ricordando che il resto del prodotto è uguale al prodotto dei resti dei fattori.
Ad esempio, $3000 = 3 \times 1000$ e quindi $(3000 \equiv 3) \bmod 9$.

Infine, si propone di calcolare il resto di 4715.

Dovrebbe emergere rapidamente che, riscritto il numero come

$$4715 = 4000 + 700 + 10 + 5$$

il resto sarà la somma dei resti, o, se necessario come in questo caso, il resto della somma dei resti.

Conclusione: un numero è divisibile per 9 se e solo se la somma delle cifre è divisibile per 9.

Fase 4

Si passa ora alla divisibilità per 3. In analogia alla fase 2, si tratta di far emergere che 3 è fattore di 9 e quindi che se un numero è divisibile per 9, allora è divisibile anche per 3.

Se poi il numero non è divisibile per 9, sarà divisibile per 3 se il resto della divisione per 9 è divisibile per 3.

Conclusione: un numero è divisibile per 3 se e solo se la somma delle cifre è divisibile per 3.

Fase 5

Si pone infine in discussione il criterio di divisibilità per 11.

Per questo si procede come per il 9: si considerano le potenze del 10 e se ne calcola il resto.

Modulo 11, risulta:

$$10 \equiv 10$$

$$100 \equiv 1$$

$$1000 \equiv 10$$

$$10000 \equiv 1 \dots$$

In pratica, se la potenza di 10 ha esponente dispari (potenze evidenziate in rosso), il resto è 10, altrimenti è 1.

Ragionando come nel caso del criterio del 9, possiamo ad esempio provare se 88715 è divisibile per 11. Eseguiamo le somme modulo 11:

$$88715 \equiv 80000 + 8000 + 700 + 10 + 5 \equiv 8 + 80 + 7 + 10 + 5 \equiv 110 \equiv 0$$

e quindi il numero è divisibile per 11.

Già con questi risultati si potrebbe concludere, ma un'osservazione che permetterà di semplificare i calcoli: quando il resto è 10, è comodo ricorrere ai numeri negativi. In altre parole, terremo presente che

$$(10 \equiv -1) \bmod 11 \text{ (infatti la differenza } 10 - (-1) \text{ è un multiplo di 11)}$$
$$1000 \equiv -1 \bmod 11, \dots$$

Riprendendo l'esempio precedente, mod 11 possiamo scrivere

$$88715 \equiv 80000 + 8000 + 700 + 10 + 5 \equiv 8 - 8 + 7 - 1 + 5 \equiv 11 \equiv 0.$$

Da questo possiamo dedurre il criterio:

Conclusione: un numero è divisibile per 11 se e solo se la somma delle cifre di posto dispari (a partire dalla cifra delle unità) meno la somma delle cifre di posto pari è divisibile per 11.

Attività 3

Fase 1

La prima fase è finalizzata ad una ripresa dei concetti di divisibilità e primalità. Si consiglia al riguardo l'unità **Numeri primi conosciuti e sconosciuti**

<https://repository.indire.it/repository/working/export/4122/> . Anche se dedicata agli alunni della scuola secondaria di primo grado, offre interessanti spunti di lavoro; in particolare si consiglia di riproporre le fasi 1 e 2 dell'attività.

Fase 2

Si vuole focalizzare l'attenzione sul metodo per controllare se un numero n è primo per ricavarne un algoritmo.

La domanda guida è:

per quali numeri si deve dividere n , per concludere che n è composto?

Le risposte "per tutti i numeri, a partire da 2 e fino a $n-1$ " o "a partire da 2 e fino alla metà di n " saranno le prime e più frequenti.

È facile convenire che se queste risposte non sono errate, certamente non sono efficienti. Basta proporre un numero quale 997 per capire che il numero di divisioni diventa proibitivo.

Una risposta diametralmente opposta può essere: "per tutti i numeri primi minori di n ".

Anche in questo caso, la risposta è corretta. Ma se conoscessimo già tutti i primi, la domanda posta non avrebbe senso. E d'altra parte, se abbiamo un numero veramente grande, ad esempio con 10 cifre, il numero di primi da memorizzare sarebbe eccessivo. Naturalmente, con numeri di tale grandezza, non è pensabile procedere con un calcolo manuale: bisognerà istruire opportunamente un calcolatore per ottenere il risultato.

Comunque, questa risposta è utilizzabile almeno parzialmente: ad esempio, dopo aver provato che un numero non è divisibile per 2, è inutile verificare se è divisibile per numeri multipli di 2. Questo consente di ridurre alla metà il numero delle prove.

Ma il punto chiave sta nell'osservare che i divisori di un numero sono a coppie: se x divide n , ciò significa che esiste un naturale y tale che $x \cdot y = n$, e quindi che anche y è un divisore. (Naturalmente, in classe al posto di n useremo numeri: ad esempio 144 e 92).

Ora o $x < y$, o $y < x$, o $x = y$. Il caso $x = y$ si presenta solo se n è un quadrato perfetto: allora x è la radice quadrata di n . È il caso di $144 = 12 \cdot 12$.

Negli altri casi il minore dei due divisori è minore della radice di n , e l'altro è maggiore. Per esempio, si ha $7 \cdot 17 = 119$: il fattore 7 è minore della radice di 119 (che è compresa fra 10 e 11), mentre 17 è maggiore.

Tornando al nostro problema, possiamo allora concludere che i tentativi di ricerca di un divisore di n devono procedere al più fino alla radice di n , e si possono saltare i pari (se il numero n non è pari).

Fase 3

Problemi aperti

È importante che gli studenti percepiscano la matematica come una scienza in cui molte cose sono sicure ed acquisite, ma che ha ancora molti problemi aperti. Solo così è possibile presentarla come un edificio che è ancora in costruzione, e non come una struttura cristallizzata.

Si faccia riferimento alla già citata unità **Numeri primi conosciuti e sconosciuti** <https://repository.indire.it/repository/working/export/4122/> , Fasi 3 e 4.

Attività 4

Scrivere 'messaggi segreti' è un'attività che abbiamo fatto tutti da bambini. La stessa attività ha impegnato l'uomo in ogni epoca, compresa la nostra, sia per ragioni militari o diplomatiche, sia per ragioni commerciali. In bibliografia sono riportati alcuni testi e siti, accessibili almeno in parte anche agli allievi, che trattano il tema in modo divulgativo.

Il primo passo consiste nel codificare il testo che si vuole rendere segreto: con questa operazione si associa un numero a ciascun carattere del messaggio. Spesso il codice è semplicemente il numero d'ordine delle lettere nell'alfabeto in cui è scritto il messaggio.

Ai giorni nostri l'esempio più diffuso di codice associato ad un insieme di caratteri è il codice ASCII (American Standard Code for Interchange Information) nato nel 1920 per le telescriventi e ora in uso con i computer. Nel codice ASCII l'insieme dei caratteri comprende le usuali lettere dell'alfabeto, maiuscole e minuscole, le dieci cifre, altri caratteri grafici, alcuni caratteri 'speciali' come il 'CR' (carriage return - ritorno carrello, che corrisponde a caporiga) e il 'ESC' (escape - uscita senza esecuzione) che ne tradiscono l'origine, per un totale di 256 simboli.

Quando il testo è tradotto in numeri, si possono applicare trasformazioni numeriche (codifica o cifratura) che lo rendano segreto e che ne consentano la lettura (decodifica o decifratura) solo a chi possiede la chiave. A volte l'aspetto numerico non traspare immediatamente, ma bastano poche considerazioni per svelarlo.

In questa attività si descrivono gli aspetti più semplici, adatti ad allievi del biennio, di alcuni processi di cifratura, anche con qualche riferimento storico. Talvolta i termini codificare, cifrare e criptare vengono usati come sinonimi.

Fase 1: Cifrari a sostituzione: cifratura monoalfabetica e polialfabetica

Il metodo più semplice di criptare un messaggio consiste nel sostituire i caratteri del messaggio con altri traslando la posizione del carattere nell'alfabeto di un numero fisso (la chiave).

Nelle due righe sottostanti sono riportati l'alfabeto italiano e una sua traslazione di 9 posizioni. Nella seconda riga le lettere ripartono dall'inizio quando sono esaurite.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Ecco un esempio di cifratura:

Testo in chiaro

L	A		P	R	O	F		D	I		M	A	T	E		N	O	N		C'	È
---	---	--	---	---	---	---	--	---	---	--	---	---	---	---	--	---	---	---	--	----	---

Testo criptato

U	L		B	D	A	Q		O	T		V	L	F	P		Z	A	Z		N	P
---	---	--	---	---	---	---	--	---	---	--	---	---	---	---	--	---	---	---	--	---	---

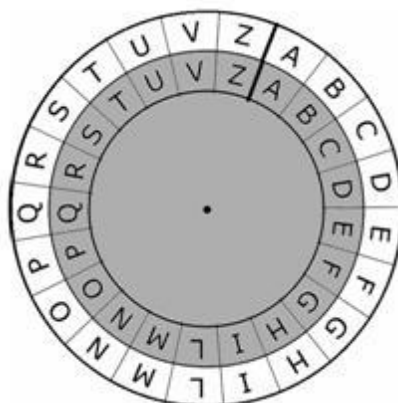
In questo semplice esempio il codice, cioè la traduzione delle lettere in numeri, segue l'ordine alfabetico: $A \rightarrow 1$, $B \rightarrow 2$, ..., $Z \rightarrow 21$. Per criptare il messaggio codificato si somma la chiave (nel nostro caso 9) al codice di ciascun carattere; se il risultato supera 21, si sottrae 21 (in termini intuitivi: si ricomincia da capo).

In formula: $n \rightarrow (n + 9) \bmod 21$

Ricordiamo che la scrittura "mod 21" significa proprio che, qualora la somma superi 21, si sottrae 21. Per decriptare il messaggio criptato si può procedere in due modi equivalenti:

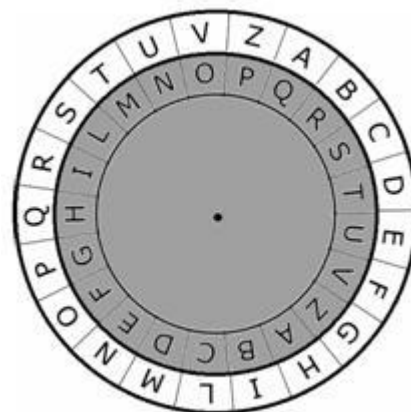
- si applica ai codici l'operazione inversa, cioè si traslano 'indietro' di 9 posizioni:
 $m \rightarrow (m - 9) \bmod 21$
("mod 21" significa anche che, quando il risultato è negativo, si aggiunge 21)
- oppure si applica la stessa operazione usando come chiave il complementare di 9 rispetto a 21, ossia 13 = 21-9:
 $m \rightarrow (m + 12) \bmod 21$

Per quanto semplice, e quindi facilmente svelabile, questo codice era usato da Giulio Cesare che faceva uso di due dischi simili a quelli della figura seguente:



Sopra ad un primo disco (nella figura, più chiaro), viene posto un secondo disco concentrico più piccolo (disco più scuro). Una borchia tiene insieme i due dischi che possono ruotare in modo indipendente. I due dischi, ruotati secondo la chiave, permettono la codifica e la decodifica del messaggio.

Ecco una codifica al modo di Giulio Cesare con una chiave di 7. Il disco grigio viene ruotato di 7 lettere in senso orario: in questo modo la lettera A viene traslata nella lettera H.



Il messaggio: ARRIVO DOMANI viene cifrato cercando le lettere nel disco interno e riportando le corrispondenti in quello esterno.

A	R	R	I	V	O		D	O	M	A	N	I
H	B	B	R	F	V		M	V	T	H	U	R

Per la decodifica si procede al contrario: si cercano le lettere del messaggio cifrato nel disco esterno e si riportano le corrispondenti in quello interno.

Di questo codice esistono molte varianti: un esempio consiste nel concordare un particolare ordine delle lettere dell'alfabeto (una permutazione), diverso dall'ordine alfabetico, sul quale poi si applica la traslazione delle lettere determinata dalla chiave. Questo tipo di codici si chiama **monoalfabetico**.

Una evoluzione dei codici monoalfabetici (a traslazione fissa) sono i codici **polialfabetici** che sono stati introdotti per aumentarne la sicurezza.

Nel codice polialfabetico la traslazione (la chiave) delle lettere non è fissa, ma viene determinata da un'altra frase che costituisce la chiave di codifica/decodifica. Il mittente ed il destinatario concordano una frase segreta che costituisce la chiave del codice. La frase viene posta sotto il messaggio, eventualmente ripetuta se il messaggio è più lungo. Ad esempio, concordiamo come chiave la parola FIORE.

Si conviene anche di togliere dal messaggio in chiaro gli spazi, senza con ciò comprometterne la leggibilità.

Dopo aver scritto sotto il messaggio in chiaro la chiave (ripetuta), ciascuna lettera del messaggio viene traslata usando come chiave la lettera posta sotto. La traslazione si realizza nel modo seguente: si fa coincidere la lettera chiave (disco interno) con la lettera Z e si legge nel disco interno la lettera che corrisponde alla lettera data sul disco più grande.

A	R	R	I	V	O	D	O	M	A	N	I
F	I	O	R	E	F	I	O	R	E	F	I
G	D	H	D	D	U	O	E	F	E	T	T

Si osservi che, da una parte, una stessa lettera viene codificata con lettere diverse, ma anche che, viceversa, una stessa lettera nel messaggio codificato proviene da lettere diverse; tutto questo rende piuttosto difficile interpretare il messaggio per chi non conosca la chiave.

Chi invece conosce la chiave decodifica il messaggio con la stessa tecnica dei due dischi, leggendo la lettera del messaggio codificato nel disco esterno per risalire alla corrispondente nel disco interno.

Fase 2: Cifrari a trasposizione: cifratura a permutazione

Un secondo metodo di cifratura consiste nel permutare i caratteri del messaggio. Questo metodo ha una certa efficacia con messaggi sufficientemente lunghi: un messaggio di 48 caratteri può infatti essere permutato in $48!$ modi possibili (anagrammi); $48!$ è maggiore di 10^{61} .

La prima tecnica di cifratura documentata risale al V secolo a.C. e viene riferita alla guerra tra Sparta e la Persia. Lisandro, generale spartano, riceve una striscia di cuoio che avvolge attorno ad un'asta cilindrica (chiamata scitale) nella quale legge il messaggio decodificato.

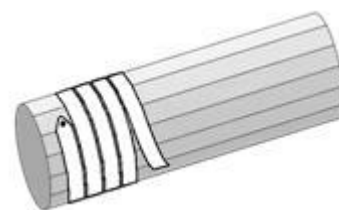
Vediamo come si procede per criptare il messaggio di 48 caratteri (compresi gli spazi):

ARRIVO_GIOVEDI_PROSSIMO_DUE_ORE_DOPO_IL_TRAMONTO

e trascriverlo criptato in una striscia per trasmetterlo.

Si avvolge una striscia in un cilindro (la scitale) con la superficie laterale suddivisa in fasce parallele. Nella figura la superficie del cilindro è divisa in 12 parti.

Il messaggio viene trascritto in orizzontale, sopra le varie fasce: il messaggio dell'esempio è di 48 caratteri e quindi si suddivide in 12 blocchi (righe) di 4 caratteri ciascuno.

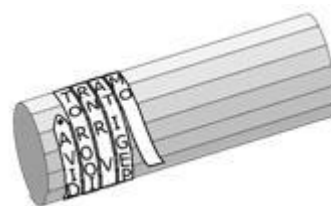


Quando si svolge la striscia vi si leggerà il messaggio criptato:

AVIDRIDOD · TOROOIOMUROIRNR · V · SOEEPLATIGEPS · · · O · MO

Il messaggio potrà essere decriptato semplicemente riavvolgendo la striscia nella scitale e leggendone la ricomposizione in orizzontale.

La trasposizione dei caratteri realizzata con questo metodo può essere descritta con una tabella a $x \times b$, dove $a \cdot b$ è la lunghezza del messaggio da trasmettere. Se necessario, quando la lunghezza del messaggio non è un multiplo della chiave, si può allungare il messaggio scrivendo alla fine caratteri a caso in modo da riempire la tabella.



Se consideriamo come chiave di cifratura la lunghezza della tabella, la larghezza può essere calcolata dividendo la lunghezza del messaggio per la chiave: se il risultato non è intero, lo si arrotonda all'intero per eccesso.

Si osservi che la lunghezza della tabella corrisponde al numero di fasce del cilindro: naturalmente questa informazione è implicita nella scitale che deve essere concordata tra mittente e destinatario.

Il messaggio dell'esempio viene cifrato scrivendolo in ordine di riga e leggendo poi criptato lungo le colonne.

La decifratura si ottiene scrivendo il messaggio cifrato in colonna e leggendo poi lungo le righe. Naturalmente, per decrittare il messaggio, occorre conoscere la chiave di cifratura (il numero delle righe della tabella che corrisponde al numero delle strisce orizzontali della scitale).

Chi vuole può vedere sia una trasposizione sulla carta tramite tabelle e un programma sulla cifratura con la scitale, sia un ulteriore metodo di cifratura negli [Spunti per altre attività con gli studenti](#).

A	R	R	I
V	O	.	G
I	O	V	E
D	I	.	P
R	O	S	S
I	M	O	.
D	U	E	.
O	R	E	.
D	O	P	O
.	I	L	.

Indicazioni metodologiche

Attività 1

L'attività è proposta in modo da offrire spunti di riflessione sul legame fra l'arte e la matematica, in particolare l'aritmetica dei numeri primi e la geometria piana.

L'osservazione del mosaico e la possibilità di visualizzare le costruzioni in laboratorio con un software di geometria dinamica consentono di pervenire in modo abbastanza diretto alle conclusioni previste. L'attività è suddivisa in 5 fasi che accompagnano lo studente in un itinerario che parte dall'osservazione di una forma d'arte e si conclude con un cenno alla teoria delle congruenze.

È indispensabile, per una corretta interpretazione dei risultati, la compilazione delle tabelle associate ai poligoni derivati; l'osservazione delle tabelle porta naturalmente alla congettura riguardante il legame fra il numero dei lati del poligono di partenza e i salti che si fanno nel caso si ottenga un poligono stellato. La fase 5, riepilogativa del procedimento seguito nelle fasi precedenti, analizza in modo più puntuale il caso del dodecagono, proponendo lo studio dell'aritmetica dell'orologio, per arrivare in modo semplificato al concetto di congruenza aritmetica.

Attività 2

L'attività porta alla giustificazione dei criteri di divisibilità, e, volendo, permette di costruirne di nuovi.

I criteri si basano in modo esplicito o implicito sulle **congruenze** e sulla **notazione posizionale** dei numeri. Per giustificarli non è tuttavia necessario affrontare in modo

sistematico le congruenze e le classi resto, però bisogna avere riflettuto almeno sul fatto che "il resto della somma è la somma dei resti" (e sul fatto che, quando la somma dei resti supera il divisore, "il resto della somma è il resto della somma dei resti").

Sugli stessi principi si basa anche la famosa (ma sempre meno usata) "prova del 9". Per quanto riguarda la scrittura posizionale, a nostro parere è opportuno inserirla nella programmazione di scuola. Una riflessione approfondita sulla scrittura posizionale dei naturali, anche riferita a basi diverse, fornisce un buon punto di partenza per un approccio corretto ai polinomi: in fondo, la notazione posizionale è la forma polinomiale dei numeri. Chi vuole approfondire troverà strette analogie tra i criteri di divisibilità su esposti e il teorema del resto (o di Ruffini), che è un criterio di divisibilità tra polinomi.

L'attività è stata scomposta in fasi che portano in modo naturale alla conclusione voluta.

La metodologia consigliata è una lezione interattiva, con frequenti discussioni volte a chiarire i vari passaggi.

Attività 3

Si deve richiamare la definizione di numero primo. Al riguardo, si ricorda che la definizione concordemente accettata considera primo un numero naturale **maggiore** di 1 che sia divisibile **solo** per 1 e se stesso.

Sulla divisibilità e sulla primalità si trovano argomenti interessanti in Elementi di aritmetica e di algebra elementare, e negli altri testi citati negli [Spunti per un approfondimento disciplinare](#).

Nella fase 2, in questo contesto, si consiglia una lezione con domande stimolo.

Si insiste molto su questo algoritmo, perché la difficoltà di fattorizzare velocemente numeri naturali grandi (di 2 o 3 centinaia di cifre) è alla base della crittografia a chiave pubblica, molto usata per la trasmissione sicura di dati su Internet. Il metodo di crittografia più noto è detto RSA, dalle iniziali dei nomi dei suoi inventori: Rivest, Shamir e Adleman. Questo è un esempio del fatto che nella tecnologia informatica attuale c'è molta più matematica di quanto si possa immaginare.

Osservazione

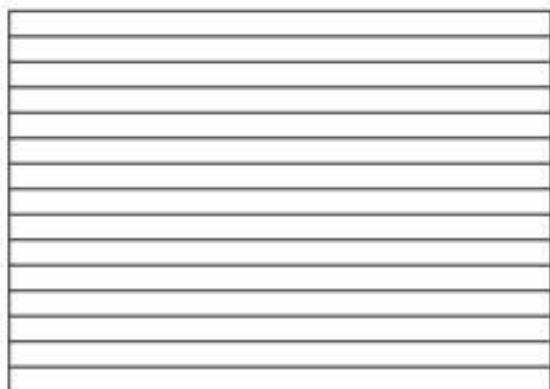
Una difficoltà che si trova le prime volte che si scrive un algoritmo, è di capire quali siano le istruzioni che un "esecutore" sa eseguire: nel caso specifico, l'esecutore saprà determinare se " x divide n "? È evidente che prima di cominciare la stesura dell'algoritmo bisogna convenire quali siano le "capacità" dell'esecutore. E questo non solo se l'algoritmo è scritto per un esecutore elettronico, ma anche per un esecutore umano, come capita se stiamo scrivendo le istruzioni per un compagno di un'altra classe, magari più giovane.

Attività 4

I codici segreti costituiscono un argomento di grande fascino per i nostri allievi e anche di attualità nelle implicazioni con le comunicazioni via computer.

L'attività proposta inizia con le più semplici tecniche di crittografia usate nella storia e mostra alcuni aspetti dell'aritmetica modulare.

Agli insegnanti suggeriamo di costruire una scitale con cui far codificare e decodificare messaggi agli allievi. Si prende un cartoncino della consistenza del dorso di un blocco notes. Si ricava un rettangolo di dimensioni 20 cm x 10 cm. Si segnano 10 strisce da 1 cm di larghezza e si marcano le linee con la punta di una penna biro. Si piega il cartoncino lungo le linee e lo si chiude, fissandolo con del nastro adesivo secondo la chiave del messaggio da cifrare (che sarà un numero minore o uguale ad 10).



Il cartoncino è stato chiuso in modo da formare una scitale a 7 colonne.

Può essere usato, ad esempio, per codificare un messaggio di 35 caratteri. In tal caso la striscia di carta si avvolgerà attorno alla scitale formando 5 giri.

L'aritmetica costituisce un naturale contesto per la descrizione di algoritmi che motivano l'uso del computer come strumento per l'esplorazione matematica e non solo come facilitatore o controllore per il calcolo.

I suggerimenti di [Spunti per altre attività per gli studenti](#) mostrano qualche esempio di pagine html con funzioni scritte in linguaggio javascript.

Attività 2: "la scitale al computer" propone un esempio di calcolo con le lettere che ha lo scopo di costruire la formula di trasposizione dei caratteri dal messaggio in chiaro al messaggio cifrato (e viceversa).

Attività 3: "cifatura e numeri primi" contiene certamente parti troppo complesse per allievi del biennio, in particolare nei mesi iniziali del primo anno. Riteniamo tuttavia che l'argomento possa essere proposto agli alunni più motivati per un approfondimento nel corso del secondo o terzo anno e che comunque offra qualche utile spunto ai docenti.

Eventuali difficoltà e suggerimenti

Questa unità può rappresentare un esempio di come si possano attivare gruppi di lavoro a livelli differenti su tematiche parallele, intorno ad un nucleo centrale condiviso.

Gli argomenti di cui si occupa, pur riguardando tutti problemi connessi, spaziano dalla geometria ai criteri di divisibilità, dall'aritmetica modulare alla rappresentazione

algebrica. Possono dunque servire a coinvolgere ogni alunno in un'attività che l'insegnante giudichi più congeniale per i suoi interessi e le sue potenzialità.

Di seguito si cercano di evidenziare le difficoltà più probabili che gli alunni potranno incontrare nelle diverse attività, avanzando alcuni suggerimenti in proposito. Si invita tuttavia l'insegnante a valutare molto bene quali delle attività vadano proposte a tutti gli alunni e quali siano da riservare a gruppi più ristretti.

Attività 1: I poligoni stellati e la tabella

Se l'insegnante ritiene che questa attività rappresenti una significativa occasione di apprendimento anche per i propri alunni più deboli, egli dovrà prevedere di lasciare loro il tempo di provare (a mano o con software di geometria dinamica), magari a coppie, eventualmente sotto la guida di un compagno più esperto. Si segnala tuttavia come possa essere controproducente mettere in cantiere un'attività se non si pervenga poi a un qualche punto fermo: per questo motivo, è bene che l'insegnante preveda fin dall'inizio dove desidera che tutti gli studenti arrivino, in modo da attivare operativamente i percorsi per ognuno.

Sicuramente la proposta a partire da una situazione reale (i mosaici dell'Alhambra o più in generale analoghe decorazioni) serve a motivare e comprendere di cosa si parla. Una difficoltà può derivare dalla comprensione esatta della differenza fra "poligono derivato" e "poligono stellato". Se la definizione risulta oscura per alcuni alunni, bisogna che essi siano lasciati liberi di provare a costruire i propri poligoni, rilevando in quali casi la costruzione "funzioni" e i quali no. Si scoprirà allora, partendo da esempi, che il quadrato all'interno dell'ottagono regolare o il triangolo equilatero all'interno dell'esagono regolare sono derivati ma non stellati. È consigliabile, affinché venga chiarito il meccanismo con cui si costruiscono gli stellati, far iniziare gli studenti dal caso dell'ottagono regolare, come suggerito nella fase 2; è anche importante far emergere spontaneamente le discussioni sul verso di percorrenza (orario od antiorario) in cui si eseguono i salti.

La simbologia stessa acquisterà significato a partire dalla necessità di comunicare le proprie scoperte: la scrittura $P(8,3) = P(8,5)$ (o altra analoga, che poi l'insegnante si occuperà di far convergere con questa, universalmente accettata) deve emergere naturalmente dalla necessità di esprimere il fatto che "a partire dall'ottagono regolare si possono saltare via via 3 lati oppure 5 e si ottiene la stessa figura".

Analogamente, è importante che gli studenti possano avanzare da soli eventuali congetture sul numero e sulla regolarità dei poligoni stellati costruibili a partire da uno stesso poligono. La tabella prevista nella Fase 3 diventa un utile strumento per formulare congetture, cercare controesempi (come quello citato al termine della Fase 2) o rispondere alle domande della Fase 4. Perché essa però svolga effettivamente la sua funzione, essa deve essere ben compresa. Si raccomanda perciò che ogni alunno ne compili direttamente almeno qualche riga, ricorrendo alla propria operatività: solo quando sarà chiaro a tutti come si compila la tabella, ci si potrà avvalere delle informazioni fornite dai compagni più veloci o motivati, sfruttando le informazioni da essi fornite per completare la tabella con quanti più dati possibile.

A questo punto, l'insegnante potrà chiedere di rispondere a domande del tipo:

- A quali "salti" corrispondono le righe che non contengono tutti i vertici?
- Perché il poligono di 11 lati ha più poligoni derivati di quello di 12?
- In quale tra i casi esaminati ottieni un maggior numero di righe che comprendano tutti i vertici?

È necessario che l'insegnante richieda la soluzione della proposta di lavoro relativa al poligono di 11 lati e quella relativa al poligono di 12 lati, per far poi confrontare le due tabelle. Per rispondere, in particolare alla terza domanda, possono aiutare richieste "intermedie" dell'insegnante, come: "quale caratteristica aritmetica ha il numero 11 rispetto al 12", oppure "se consideri il poligono di 12 lati e i salti corrispondono a un divisore di 12, ottieni un poligono stellato?", o ancora "cerca una relazione fra 12 e il numero di lati saltati quando si ottiene un poligono stellato".

A tali domande gli studenti cercheranno di rispondere a coppie, sulla base delle tabelle in loro possesso: è importante che ogni coppia (e dunque ogni studente) abbia il tempo di riflettere e cercare esempi, esternando e socializzando i propri dubbi e le proprie scoperte, prima di arrivare alla formalizzazione delle risposte. A questo punto, può seguire una fase di discussione che agevoli la risposta a tutte le domande, con la messa in evidenza delle caratteristiche di primalità.

Attività 1: l'aritmetica modulare (o dell'orologio)

La Fase 5, che introduce al discorso delle congruenze numeriche, presenta a sua volta alcuni punti delicati, che per alcuni studenti richiederanno un lavoro pratico non banale e non breve. Essa può forse essere ulteriormente semplificata partendo dall'esempio dei giorni della settimana, con domande poste dall'insegnante, quali: "se oggi è lunedì 3 maggio, il 15 maggio che giorno è? E il 25 maggio? Come fai a rispondere senza la disponibilità di un calendario?".

L'insegnante che voglia trattare questo tema (anche indipendentemente dalla parte precedente dell'attività) può trovare alcuni spunti sul sito "Eduscienze" <https://eduscienze.com/> dove viene presentata un'attività su questo tema, pensata per un laboratorio di Scuola media con il supporto di sussidi concreti, che aiutino a realizzare il necessario transfer fra l'operazione manuale (mediata dall'oggetto) e la concettualizzazione richiesta.

Naturalmente, l'insegnante dovrà adattare la proposta al nostro livello scolastico, dove ci si aspetta di sfociare in una formalizzazione più alta e nella costruzione del concetto di congruenza. Tuttavia, ancora una volta, è bene che la formalizzazione segua la sperimentazione concreta, come conclusione del lavoro e come necessità di "accelerare" o "semplificare" la scrittura. I quesiti che l'insegnante porrà a questo riguardo avranno lo scopo non solo di verificare l'acquisizione del concetto, ma anche di costringere lo studente a motivare i passaggi, raffinando il proprio livello di rappresentazione verbale e simbolica.

Attività 2

Quest'attività è certamente importante per tutti gli studenti: si tratta infatti anzitutto di riprendere un argomento già studiato al livello scolastico precedente (e di solito

memorizzato abbastanza facilmente) e importante per applicazioni di routine, quali la scomposizione in fattori, il calcolo con le frazioni, ecc. L'attività dunque rappresenta quanto meno un'occasione per riprendere in mano le conoscenze relative e la loro messa in pratica; inoltre, può essere preziosa per mettere anche gli studenti più restii davanti al fatto che ogni affermazione in matematica ha un motivo dimostrabile.

Se tutti gli studenti avranno acquistato sufficiente abilità nel trattare l'aritmetica modulare, l'insegnante potrà seguire la traccia indicata, eventualmente ricorrendo a interventi in gruppi di lavoro.

In caso contrario si consiglia di concentrarsi su quelle dimostrazioni (divisibilità per 2, per 3, per 5, per 9) che si provano facilmente usando la notazione posizionale: questo costringerà infatti a ragionare su tale notazione, consolidando al contempo le conoscenze e abilità ad essa relative.

Attività 3

Mentre si raccomanda di riprendere le attività relative ai numeri primi, a partire dal "crivello di Eratostene" e come proposte nell'unità "Numeri primi conosciuti e sconosciuti" <https://repository.indire.it/repository/working/export/4122/> fino a riflettere su quanti tentativi sia opportuno fare per verificare la primalità di un numero, sarà l'insegnante a valutare l'opportunità di insistere per tutti gli alunni sulla realizzazione o meno dell'algoritmo relativo.

In caso affermativo però si deve considerare la necessità di chiarire, almeno operativamente, che cosa sia un algoritmo. Allo scopo si consiglia di presentare alcune operazioni della vita quotidiana che richiedono sequenze di operazioni "elementari" e di scelte, che sono le "istruzioni" fondamentali per ogni algoritmo. Esempi ormai classici: l'algoritmo per fare un caffè, o per prelevare un panino dal distributore automatico, o per chiamare qualcuno al telefono, ... Un altro esempio significativo (e che può tornare utile all'insegnante in altro contesto, offrendo un interessante collegamento) riguarda i vari algoritmi con cui si costruiscono le figure base con un software di geometria dinamica.

Una difficoltà che si incontra nella scrittura di un algoritmo è naturalmente quella di capire quali siano le istruzioni base che un "esecutore" sa eseguire. È molto utile, come esercizio, dopo avere affidato ad alcuni alunni la redazione dell'algoritmo, sperimentarlo operativamente a coppie, chiedendo a un ragazzo di eseguirlo step by step sotto il controllo dell'altro (oppure collettivamente in classe).

Attività 4

Questa attività possiede indubbiamente un fascino particolare (e si presta, come sottolineato, a collegamenti con altre discipline). Anche il suo aspetto ludico la rende sicuramente attraente per tutti gli studenti. Inoltre non dovrebbero presentare difficoltà le codifiche delle Fasi 1 e 2, poiché l'esecuzione concreta della codifica tramite i dischi (Fase 1) o la scitale (Fase 2) consente di esplicitare i concetti sottostanti. Può essere anche opportuno sfruttare la scrittura in tabella come esposto nell'attività: questo consente di capire meglio il funzionamento dell'algoritmo di codifica e di decodifica, mentre il ricorso al disco (Fase 1) permette di riprendere

alcuni temi dell'aritmetica modulare. L'attività si presta inoltre ad una ricerca su internet sulle problematiche della cifratura o su argomenti connessi; tale ricerca potrebbe procedere parallelamente all'attività proposta come "altre attività per gli studenti" e dichiaratamente rivolta a ragazzi con competenze di livello superiore. Si potrà così realizzare un ulteriore esempio di attività su una stessa tematica affrontata da tutti, ognuno al proprio livello di apprendimento.

Spunti per un approfondimento disciplinare

Chi voglia approfondire questi temi, può utilmente vedere:

Vinicio Villani, *Cominciamo da zero*, Pitagora Editrice, Bologna (2003).

Roberto Dvornicich, *Elementi di aritmetica e di algebra elementare*. In "L'Algebra fra tradizione e rinnovamento", MPI, Pacchetto formativo multimediale per docenti di Scuola superiore (scarica il file **Elementi di Aritmetica** [https://repository.indire.it/repository/working/export/5230/files/Elementi di Aritmetica.doc](https://repository.indire.it/repository/working/export/5230/files/Elementi_di_Aritmetica.doc)).

Giulio C. Barozzi, *Aritmetica: un approccio computazionale*, 2007, Springer Verlag (collana Convergenze)

Marcus De Sauty, *L'enigma dei numeri primi*, BUR, 2005.

Andrea Sgarro, *Crittografia*, Muzzio, 1986.

Simon Singh, *Codici & segreti*, BUR, 1999.

Chimetto M. A., 2002, *Congruenze numeriche e poligoni stellati*, Matematica e calcolatore, Tecnodid Editrice, pagg. 87-92.

Chimetto M. A. *Algebra e Cabri: poligoni stellati e aritmetica delle congruenze in Proceedings of the third Cabri Geometry International Conference*, a cura di Giuseppe Accascina, Giovanni Margiotta Ed. Nuova Cultura pagg. 427-433.

Elementi per prove di verifica

1. L'insegnante di matematica decide di interrogare gli studenti nell'ordine stabilito nel modo seguente. Sceglie un numero, quindi interroga via via gli alunni che nel registro hanno numero d'ordine uguale ai multipli del numero scelto; quando il multiplo supera il numero di alunni della classe, prende il resto della divisione per quel numero. Per interrogare tutti gli alunni, come deve essere il numero scelto dall'insegnante?

Risposta

Se il numero degli studenti è primo, l'insegnante interroga tutti, qualunque numero scelga per il salto. In generale, per interrogare tutti gli alunni è necessario e sufficiente che il numero degli studenti e il numero scelto per il salto siano primi fra loro.

2. Considera l'orologio della figura seguente.



Stabilisci che ora segnerà:

- dopo 2 ore e mezza;
- dopo 1620 minuti;
- 425 minuti prima;
- supposto che l'ora indicata in figura sia di mattina, 250 ore prima era mattina o pomeriggio?

3. Oggi è lunedì; la lancetta delle ore del mio orologio indica le 8. Che giorno sarà fra 50 ore? E fra 60 ore?

(Attenzione: si può rispondere con sicurezza a una sola delle due domande.)

4. a) Se oggi è sabato, che giorno della settimana sarà tra 30 giorni? Che giorno della settimana era 30 giorni fa?

b) Il 22 febbraio del 2005 era un mercoledì. In quell'anno la scuola finiva il 10 giugno; che giorno della settimana era?

5. Scrivi un numero di tre cifre e poi scrivi di seguito le stesse cifre nello stesso ordine. Verifica che il numero così costruito è divisibile per 7, per 11 e per 13. Si può affermare che ogni numero così costruito è multiplo di 7, 11 e 13?

Risposta

La risposta è affermativa: il numero costruito si ottiene moltiplicando il numero di partenza per $1000 + 1 = 1001$, che è multiplo di 7, 11, 13. Per esempio, partendo da 512, si ha:

$$512512 = 512 \times 1000 + 512 = 512 \times (1000 + 1) = 512 \times 1001 = 512 \times 7 \times 11 \times 13.$$

6. Il 1789, anno della rivoluzione francese, è un numero primo? Descrivi un algoritmo che ti consenta di stabilirlo.

7. Ad un accampamento romano arriva il seguente messaggio, cifrato con un codice di Cesare, da parte di una legione impegnata in un combattimento:
ZLYCVUVYPUMVYGP

Al comandante dell'accampamento arriva anche la notizia che la chiave del messaggio è un divisore di 203.

Cosa farà il comandante dell'accampamento?

(Si considera un alfabeto di 26 caratteri).

Risposta

Il comandante invierà dei rinforzi alla legione. Infatti $203 = 7 \times 29$; la chiave cercata è 7.

Applicando il codice di Cesare con uno spostamento di 7 cifre, si ottiene il messaggio SERVONORINFORZI.

8. Si vuole cifrare il messaggio seguente:

LASCITALEEUNCIFRARIOATRASPPOSIZIONE

usando una scitale che può contenere 4 lettere per ogni giro.

Si osservi che nel messaggio sono stati eliminati gli spazi e l'accento: la comprensione del messaggio non è compromessa.

- Dire quanti giri completi farà la striscia attorno alla scitale, per consentire la trasposizione del messaggio.
- Cifrare il messaggio usando una tabella di 4 righe.

Il numero dei giri della striscia attorno alla scitale è il più piccolo numero intero non inferiore alla lunghezza del messaggio diviso 4 (caratteri per giro): $34/4 = 8,5$ e quindi ci saranno 9 giri.

La cifratura può essere descritta facilmente con una tabella 4×9 (completata con due caratteri scelti a caso).

Trascriviamo il messaggio sulla tabella in orizzontale.

L	A	S	C	I	T	A	L	E
E	U	N	C	I	F	R	A	R
I	O	A	T	R	A	S	P	O
S	I	Z	I	O	N	E	P	H

La lettura del messaggio in verticale produce il messaggio cifrato:

LEISAUOISNAZCCTIIIROTFANARSELAPPEROH

Allo stesso risultato si giungere con la tecnica del salto di caratteri. Numeriamo la posizione dei caratteri cominciando da 0:

L	A	S	C	I	T	A	L	E	E	U	N	C	I	F	R	A	R	I	O	A	T	R	A	S	P	O	S	I	Z	I	O	N	E
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Per comporre il messaggio in codice occorre leggere i caratteri "in colonna", e quindi prenderne uno ogni 9. In numero 9 è l'intero più piccolo maggiore o uguale di $34/4$, dove 34 è il numero di caratteri del messaggio e 4 è il numero di caratteri attorno alla scitale.

Spunti per altre attività con gli studenti


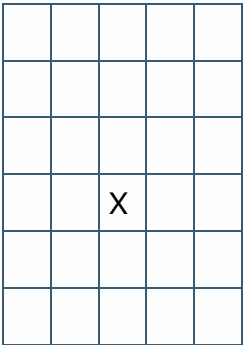

Attività 1

Quanti divisori ha un numero?

(Suggerimento. Ricorda: un numero d è divisore di n se i fattori primi di d sono fattori anche di n , e di grado minore o uguale. Consideriamo per esempio $n = 180 = 2^2 \times 3^2 \times 5^1$. Un divisore sarà del tipo $2^a \times 3^b \times 5^c$, dove: a è 0, 1 oppure 2; b è 0, 1 oppure 2; c è 0 oppure 1. In tutto, abbiamo $3 \times 3 \times 2 = 18$ possibilità di scelta degli esponenti e quindi 18 divisori.)

Attività 2: La scitale al computer

Ci proponiamo ora di ottenere un algoritmo che generi via via i caratteri del messaggio criptato con il metodo della scitale; si tratta di costruire una formula che calcola ad ogni passo il carattere corrispondente nel messaggio in chiaro. Immaginiamo il messaggio in chiaro trascritto nella tabella come nell'esempio dell'attività 4.

		<p>Messaggio in chiaro: il carattere X occupa nel messaggio la posizione p_1. Possiamo convenire che la posizione dei caratteri inizia da 0 (e non da 1) sia nei messaggi che nelle righe e colonne della tabella seguente</p>
<p>La tabella ha a righe e b colonne, gli indici di riga e di colonna iniziano da 0. Nella tabella il carattere X occupa la posizione (i,j): i-sima riga e j-sima colonna.</p>		<p>Il messaggio in chiaro viene trascritto in orizzontale, cioè lungo le righe: il messaggio in codice è letto lungo le colonne. Immaginiamo la scitale disposta orizzontalmente e quindi la colonna della tabella è la striscia di cuoio che la avvolge. Leggendo per riga (messaggio in chiaro) la posizione del carattere X nella tabella è data da: $p_1 = i \cdot b + j \quad (1)$ mentre leggendo per colonna (messaggio criptato) avremo: $p_2 = j \cdot a + i \quad (2)$ Ricavando i in (2) e sostituendo in (1): $p_1 = (p_2 - j \cdot a) \cdot b + j$ Inoltre, si osserva che: $j = \text{Parte intera} (p_2/a)$</p>
		<p>Dato che (cominciando a contare da 0) X è preceduto in tabella da j colonne.</p>

La cifratura è descritta dalla procedura seguente:

1. Sono dati la chiave di cifratura e il messaggio in chiaro.
2. Si calcolano le dimensioni della tabella $a \times b$:
 n_1 = numero dei caratteri del messaggio in chiaro;
 a = chiave (numero di righe della tabella, corrispondente al numero di parti in cui è divisa la superficie della scitale);
 b = controchiave: il minimo intero non minore di n_1/a (numero di colonne della tabella, corrispondente al numero di fasce attorno alla scitale).
3. Si completa il messaggio in chiaro con caratteri a caso in modo da ottenere un messaggio di $n_2 = a \times b$ caratteri.
4. Si pone $p_2 = 0$ (inizio del messaggio da criptare) e s (contenitore del messaggio criptato) stringa di caratteri vuota,

finché $p_2 < n_2$, si calcola:
 j = parte intera di (p_2/a)
 $p_1 = (p_2 - j \cdot a) \cdot b + j$
si aggiunge in coda a s il carattere del messaggio in chiaro che trova nella posizione p_1
si aumenta p_2 di 1 (carattere successivo nel messaggio criptato)
si ripete il ciclo.
5. Si scrive s (messaggio cifrato).

La decifratura utilizza la stessa procedura: basta solo scambiare nel passo 4. la chiave (a) con la controchiave (b).

Il file "scitale.htm"

<https://repository.indire.it/repository/working/export/5230/files/scitale.htm>

descrive in linguaggio javascript questa procedura.

Attività 3: Cifratura e numeri primi

I codici a sostituzione o a permutazione, comprese le ultime evoluzioni che prevedevano l'uso di complesse macchine elettromeccaniche come la famosa ENIGMA, utilizzata dall'esercito tedesco nella seconda guerra mondiale e interpretata con il decisivo contributo di Alan Turing, avevano come punto debole l'uso diretto dell'alfabeto anche nelle chiavi.

Un metodo che maschera i caratteri, e che quindi rende non applicabili le precedenti strategie di decodifica, passa attraverso una codifica del testo, cioè una sostituzione dei caratteri con codici numerici, una loro ricomposizione e successiva elaborazione.

Un primo esempio: supponiamo di avere un alfabeto di 100 caratteri codificati da 00 a 99; e supponiamo anche che le prime lettere dell'alfabeto corrispondano ai codici 01, 02, 03, ecc. La codifica di un messaggio produrrà una sequenza di cifre decimali lunga il doppio del messaggio in chiaro. Per esempio, la parola "lince" si codifica con 10 09 12 03 05.

Si può stabilire che il numero complessivo delle cifre di un messaggio sia multiplo di un fattore prefissato, ad esempio 3: gli eventuali caratteri mancanti sono scelti a caso e inseriti in coda al messaggio.

Scomponiamo ora il messaggio in blocchi di tre cifre che verranno elaborate separatamente come numeri da 000 a 999. Il primo effetto è che in questo modo viene perso ogni riferimento ai caratteri del messaggio testuale. Ad esempio, per il messaggio precedente, la ricomposizione è: 100 912 030 511.

Possiamo ora elaborare i codici come se fossero corrispondenti ad un alfabeto di 1000 caratteri e non più di 100.

D'ora in poi pensiamo ai nostri messaggi (in chiaro e criptati) semplicemente come sequenza di cifre: il passaggio dal messaggio in chiaro (in cifre) al testo è la semplice operazione inversa della codifica.

Un punto debole dei sistemi di cifratura consiste nel fatto che mittente e destinatario devono concordare metodo e chiave, che naturalmente sono mantenuti segreti.

In certi contesti è auspicabile che la cifratura possa essere fatta da chiunque con un metodo standard e una chiave pubblica - che quindi non è segreta. L'idea della chiave pubblica è che chiunque possa scrivere un messaggio segreto (per esempio tutti i clienti possono mandare un messaggio a una banca), ma che solo il destinatario sia in grado di interpretarlo.

Il messaggio codificato risulta addirittura illeggibile anche per chi lo ha composto se, per caso, perde l'originale. Il destinatario invece possiede la controchiave, che naturalmente conserva gelosamente segreta. In tal modo non corre il pericolo che 'cada in mani nemiche'. La controchiave è l'unica in grado di riportare in chiaro il messaggio codificato.

Si possono presentare varie situazioni, anche divertenti, in cui si desidera far sapere qualcosa ad un altro in modo che solo il destinatario sia in grado di ricostruire il messaggio. Per esempio: un ragazzo vuole inviare ad una ragazza in modo che il postino (che sa aprire le buste) non riesca a leggerle; oppure tutti i soldati possono telefonare al loro generale indicando la presenza di una spia, ma, anche se la telefonata viene intercettata, nessuno deve essere in grado di capirne il contenuto. In quest'ultimo caso, il generale deve fornire a tutti i soldati la chiave pubblica, ma solo lui conosce la controchiave che gli permetterà di interpretare i messaggi che riceve.

Prendiamo l'alfabeto di 100 caratteri codificato con cifre decimali ricomposte a blocchi di tre. Un metodo di cifratura può essere basato su un numero a tre cifre che costituisce la mia chiave pubblica e che distribuisco liberamente.

Il codice criptato è ottenuto in due passi:

- moltiplicando il codice in chiaro per la chiave;
- prendendo il resto del prodotto nella divisione per 1000 (si dice, in questo caso, che si esegue il prodotto in modulo 1000: il risultato è sempre minore di 1000).

In formula: sia c il codice del messaggio da criptare, d il codice del messaggio criptato e sia k la chiave. Allora

$$d = (c \times k) \bmod 1000$$

Per esempio, potrei distribuire come mia chiave pubblica il numero $k = 231$.

Chiunque può ora mandarmi un messaggio criptato. Ad esempio, il messaggio rappresentato in codice da $c = 725$ verrà così criptato:

$$d = (725 \times 231) \bmod 1000 = 167475 \bmod 1000 = 475.$$

In corrispondenza alla mia chiave pubblica 231, io possiedo la controchiave (privata) 671 che non devo distribuire. La controchiave è l'unico numero che riporta, con lo stesso procedimento, il codice criptato al valore originale:

$$c = (475 \times 671) \bmod 1000 = 318725 \bmod 1000 = 725.$$

Nelle condizioni poste quindi, alla chiave 231 (pubblica) corrisponde la controchiave (privata) 671, nota solo a chi deve decriptare il messaggio.

Qual è la ragione aritmetica che fa funzionare questo sistema di cifratura?

Dobbiamo dimostrare che $(231 \times c \times 671) \bmod 1000 = c$, per ogni numero (codice) da 000 a 999.

Nell'aritmetica modulare (cioè eseguendo le operazioni modulo un numero fissato, come nel caso dell'orologio) continuano a valere le usuali proprietà della moltiplicazione (associativa, commutativa ed elemento neutro). Possiamo allora commutare e associare i fattori nella forma:

$$[(231 \times 671) \times c] \bmod 1000 = c$$

$$\text{In effetti abbiamo } (231 \times 671) \bmod 1000 = 155001 \bmod 1000 = 1.$$

A questo punto, si pone un'altra domanda: dato il numero dei possibili codici (nell'esempio è 1000, il modulo nel quale operiamo) e una chiave, qual è la controchiave corrispondente?

Osserviamo le due tabelle seguenti della moltiplicazione, la prima modulo 7, la seconda modulo 10.

Modulo 7

X	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Modulo 10

X	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	0	2	4	6	8
3	3	6	9	2	5	8	1	4	7
4	4	8	2	6	0	4	8	2	6
5	5	0	5	0	5	0	5	0	5
6	6	2	8	4	0	6	2	8	4
7	7	4	1	8	5	2	9	6	3
8	8	6	4	2	0	8	6	4	2
9	9	8	7	6	5	4	3	2	1

Nella tabella in modulo 7, in ogni riga (e corrispondentemente in ogni colonna per la proprietà commutativa) compaiono tutti i numeri del modulo. In particolare in tutte le righe compare il numero 1. Ad esempio, nella riga del 3 il numero 1 si trova nella colonna del 5. Infatti $3 \times 5 = 15 = 2 \times 7 + 1$, ossia $(3 \times 5) \bmod 7 = 1$.

Se prendiamo come chiave 3, in questo sistema semplificato, la controchiave è 5. In questo sistema tutti i numeri del modulo (ovviamente escluso 0) possono essere scelti come chiave.

Nella tabella in modulo 10, invece, il numero 1 compare solo nelle righe del 3 e del 7, in corrispondenza reciprocamente delle colonne 7 e 3. Compare anche nella riga del numero 1 (che non va bene, perché significa lasciare inalterato un messaggio), e del 9; in quest'ultimo caso il numero 1 compare in corrispondenza alla colonna con lo stesso numero 9: ovviamente questa circostanza non va bene per il nostro sistema, perché vorrebbe dire che la chiave e la controchiave sono uguali facendo così cadere la sicurezza. Possiamo anche osservare che in tutte le altre righe compare invece almeno una volta lo 0.

La presenza del numero 1 nella riga del 7 (nel modulo 10) si esprime con la seguente equazione: $7x = 10y + 1$ o anche $7x - 10y = 1$

L'unica soluzione per x , ammettendo come soluzioni solo valori da 1 a 9, è 3; in corrispondenza per y la soluzione è 2: infatti $7 \cdot 3 - 10 \cdot 2 = 1$.

In generale l'equazione che lega chiave k e controchiave x per un dato modulo m si esprime nel modo seguente: $kx - my = 1$

Dall'equazione risulta evidente che può esserci soluzione solo quando il $\text{MCD}(k,m)=1$, cioè quando k e m sono primi tra loro; in caso contrario nel primo membro si può raccogliere il MCD, che non compare però nel secondo membro (uguale a 1).

Dato il modulo e data la chiave, è facile trovare la soluzione dell'equazione (se esiste) esaminando la tabella. Esiste un algoritmo che permette di calcolare la controchiave senza usare la tabella? e, soprattutto, un tale algoritmo si può applicare con il computer a numeri molto grandi (40 o più cifre decimali) in un tempo ragionevole?

Purtroppo l'algoritmo c'è e quindi questo metodo di cifratura a chiave pubblica non è del tutto sicuro: dalla chiave e dal modulo, che devono essere noti a tutti, è possibile, anche per modulo e chiave molto grandi, calcolare la controchiave.

Il file "reciproco.htm"

<https://repository.indire.it/repository/working/export/5230/files/reciproco.htm>

descrive uno dei possibili algoritmi per il calcolo del reciproco, se esiste, di un numero in un dato modulo. L'algoritmo è ripreso dal testo "ARITMETICA un approccio computazionale" di Giulio Cesare Barozzi.

Il linguaggio javascript, usato per descrivere l'algoritmo, rappresenta i numeri con 13 cifre esatte e questo è un limite per la sua applicabilità. L'uso di strumenti di calcolo simbolico, che consentono numeri con precisione non predefinita, permette di invertire numeri con molte più cifre in tempi non troppo lunghi.

Ecco alcune applicazioni dell'algoritmo:

Modulo	Numero	Reciproco
17	5	7
18	5	11
18	12	Non c'è
$163 \times 23 = 3749$	2000	2345
$163 \times 23 = 3749$	2300	Non c'è
1234567890	98765431	493827151

$$7 \times 5 = 35 = 2 \cdot 17 + 1$$

12 non ha reciproco perché non è primo con il modulo 18; il discorso è analogo nei due esempi seguenti: 2000 è primo con 3749 mentre 2300 non lo è (entrambi i numeri sono divisibili per 23).

Documentazione e materiali

[critto_uno.xls](#) un foglio di calcolo per la cifratura con codice di Cesare.

"scitale.htm"

<https://repository.indire.it/repository/working/export/5230/files/scitale.htm>

pagina html con codifica interattiva basata sul metodo della scitale.

"potenza.htm"

<https://repository.indire.it/repository/working/export/5230/files/potenza.htm>

pagina

html con algoritmo per il calcolo di potenze in modulo.

"reciproco.htm"

<https://repository.indire.it/repository/working/export/5230/files/reciproco.htm>

pagina

html con algoritmo per il calcolo del reciproco in modulo.

Proposta di attività per il corsista

Da condividere e discutere in rete.

Leggere l'attività, le indicazioni metodologiche e gli approfondimenti:

individuare i principali nodi didattici cui la situazione fa riferimento; esporli sinteticamente per scritto.

Aggiungere qualche problema in altri contesti, relativo alle stesse abilità e conoscenze.

Sperimentare l'unità proposta:

- fare una ricognizione del contesto scolastico specifico in cui si svolgerà l'attività;
- esplicitare gli adattamenti necessari;

- formulare il progetto didattico relativo;
- preparare una prova di verifica adatta a valutare le conoscenze e abilità relative alla situazione didattica posta (anche con riferimento alle prove OCSE-PISA e INVALSI).

Scrivere un diario di bordo (narrazione e documentazione del processo di sperimentazione vissuta in classe: l'insegnante dovrà elaborare un diario con l'esposizione dell'esperimento svolto, di come gli studenti hanno reagito alla proposta didattica, delle difficoltà incontrate in particolare nel processo di costruzione di significato e di procedura di soluzione e di come sono state superate le difficoltà.

Esplicitare i compiti dati agli studenti e le modalità con cui gli studenti stessi sono stati responsabilizzati all'apprendimento.