2007-2013

Unione Europea
P.O.N. - "Competenze per lo Sviluppo" (FSE)
D.G. Occupazione, Affari Sociali e pari Opportunità

Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
D.G. per gli Affari Internazionali - Ufficio IV
Programmazione e gestione dei fondi strutturali europei e nazionali per lo sviluppo e la coesione sociale

AS agenziascuola

Numeri primi conosciuti e sconosciuti
"Straordinario quanto la matematica possa aiutarci" (S. Beckett)

A cura di Stefania Cotoneschi, Simonetta Ghelardini, Patrizia Piccinini

Introduzione

Nel primo biennio della scuola secondaria di I grado gli alunni incontrano differenti insiemi di numeri; con opportuni algoritmi e ragionamenti, cominciano a conoscere e riconoscere proprietà e caratteristiche dei vari numeri.
Questa attività può essere introdotta quando gli alunni conoscono il significato di numero primo, i criteri di divisibilità per 2, per 3, per 5, sanno usare una calcolatrice tascabile e consultare le tavole riportate nei loro testi. L'obiettivo è creare una certa familiarità con i numeri che non si possono sgretolare in prodotti di numeri più piccoli e che si chiamano numeri primi.

Riferimenti curricolari

Indicazioni curricolari

Le attività M@t.abel hanno precisi *obiettivi di apprendimento* che rientrano tra quelli inseriti nelle Indicazioni Curricolari attualmente in vigore (D.M. 16 novembre 2012, n. 254) e nelle Prove INVALSI. All'inizio di ciascuna attività sono riportati, perciò, i relativi riferimenti presenti nelle Indicazioni Curricolari 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 curricolari: riferimenti

MATEMATICA

Traguardi per lo sviluppo delle competenze al termine della scuola secondaria di primo grado
L'alunno:

- si muove con sicurezza nel calcolo anche con i numeri razionali, ne padroneggia le diverse rappresentazioni e stima la grandezza di un numero e il risultato di operazioni;
- riconosce e risolve problemi in contesti diversi valutando le informazioni e la loro coerenza;
- spiega il procedimento seguito, anche in forma scritta, mantenendo il controllo sia sul processo risolutivo, sia sui risultati;
- confronta procedimenti diversi e produce formalizzazioni che gli consentono di passare da un problema specifico a una classe di problemi;
- produce argomentazioni in base alle conoscenze teoriche acquisite (ad esempio sa utilizzare i concetti di proprietà caratterizzante e di definizione);
- ha rafforzato un atteggiamento positivo rispetto alla matematica attraverso esperienze significative e ha capito come gli strumenti matematici appresi siano utili in molte situazioni per operare nella realtà.

Obiettivi di apprendimento al termine della classe terza della scuola secondaria di primo grado
Numeri

- Eseguire addizioni, sottrazioni, moltiplicazioni, divisioni, ordinamenti e confronti tra i numeri conosciuti (numeri naturali, numeri interi, frazioni e numeri decimali), quando possibile a mente oppure utilizzando gli usuali algoritmi scritti, le calcolatrici e i fogli di calcolo e valutando quale strumento può essere più opportuno.
- Individuare multipli e divisori di un numero naturale e multipli e divisori comuni a più numeri.
- In casi semplici scomporre numeri naturali in fattori primi e conoscere l'utilità di tale scomposizione per diversi fini.

Prove INVALSI

a.s. 2009/2010 - Domanda D13
Scuola secondaria di I grado – Classe II

D13. Filippo si prepara per una gara di triathlon. Si allena nel nuoto ogni 3 giorni, nella corsa a piedi ogni 6 giorni e nella corsa in bicicletta ogni 8 giorni. Se oggi si è allenato in tutti e tre gli sport, tra quanti giorni gli accadrà di nuovo di allenarsi nei tre sport nella stessa giornata?

☐ A. 8

☐ B. 12

☐ C. 17

☐ D. 24

Soluzione INVALSI: D

Commento
L'alunno deve saper riconoscere in questo problema la presenza dei multipli di un numero: gli allenamenti di uno sport si ripetono nei multipli di un dato numero di giorni.

a.s. 2009/2010 - Domanda D20
Scuola secondaria di I grado – Classe I

D20. L'insegnante chiede: "Un numero primo maggiore di 2 è sempre dispari?". Quattro studenti rispondono così:

Chi ha ragione?

- ☐ A. Paolo
- ☐ B. Giorgio
- ☐ C. Cristina
- ☐ D. Monica

Soluzione INVALSI: B

Commento
L'alunno deve conoscere la definizione di numero primo, come numero che non ha divisori maggiori di 1 e minori di se stesso. Deve inoltre sapere che essere pari significa proprio che ha 2 come divisore e quindi ciò esclude le risposte A. e C. La risposta D. va contro la definizione di numero primo per numeri maggiori di 2.

a.s. 2010/2011 - Domanda D25
Scuola secondaria di I grado – Classe I

D25. Roberto pensa a un numero intero e lo triplica.

a. Quale di questi numeri NON può essere certamente il risultato dell'operazione?

☐ A. 150

☐ B. 126

☐ C. 75

☐ D. 55

b. Giustifica la tua risposta.

.....

.....

.....

.....

Soluzione INVALSI
a: D
b: la giustificazione deve far riferimento ai criteri di divisibilità o al fatto che 55 non è multiplo di 3.

Commento
L'alunno deve saper riconoscere i multipli di 3 e individuare il numero 55 come unico non divisibile per 3. Lo può fare sia applicando il criterio di divisibilità (somma delle cifre), sia calcolando il resto della divisione.

Descrizione dell'attività

Presentazione

Alcuni temi sono talvolta trasmessi soltanto con definizioni ed esercizi, senza che se ne veda la ricaduta in campo sociale e scientifico e senza che se ne apprezzi la bellezza intrinseca attraverso la scoperta di regolarità.
Uno di questi temi riguarda i numeri primi: si tratta di un tema che ha grande valenza storica e, allo stesso tempo, offre collegamenti con moderne discipline quali la crittografia, usata in particolare per transazioni sicure in rete. Il tema, pur essendo molto antico, presenta ancora problemi aperti, sui quali si lavora a livello di ricerca.
L'attualità del tema offre l'occasione di parlare del "mestiere" del matematico. Scrive Mario Livio nel paragrafo Numeri e meraviglia del libro "La sezione aurea", citando il poeta John Keats, che "la poesia dovrebbe [...] colpire il lettore come una parafrasi dei suoi più alti pensieri sembrando quasi reminescenza. Ma la matematica, diversamente dalla poesia, spesso riesce gradevole non tanto quando è conforme a ciò

che abbiamo intuito, ma quando smentisce tutte le attese. Inoltre, il piacere della matematica è spesso legato alla sorpresa prodotta dalla percezione di relazioni e unità del tutto insospettate". (M. Livio - *La sezione aurea* - Storia di un numero e di un mistero che dura da tremila anni - BUR - 2003 pag. 340)

Prima fase

All'inizio di questa attività richiamiamo la definizione di **numero primo**: un numero naturale maggiore di 1 è primo se ammette come divisori soltanto se stesso e 1. Proponiamo poi agli alunni, eventualmente divisi in gruppi, di discutere le strategie che consentono di riconoscere i numeri primi in un dato insieme di numeri, come: 27; 37; 63; 91; 114; 437; 619; 629; 2065; 7019.
Dalle discussioni dovrebbe emergere che:

- lo svolgimento **a mano** del compito è possibile, ma al crescere del numero aumentano rapidamente la complessità del calcolo e il tempo necessario per rispondere;
- se il numero (maggiore di 5) è pari o è divisibile per 3 oppure per 5, allora possiamo rapidamente escludere che si tratti di un numero primo applicando i **criteri di divisibilità**;
- la ricerca sulle **tavole** è fattibile solo fino ad un certo numero (di solito fino a 5000);
- l'uso della **calcolatrice** per eseguire divisioni successive è di aiuto, ma richiede un certo ragionamento; in primo luogo gli studenti si devono convincere che è inutile eseguire le divisioni per 2, per 5 e forse anche per 3, perché, applicando i criteri di divisibilità, siamo più veloci della calcolatrice.

È bene che l'insegnante richiami l'attenzione di tutta la classe sull'ultima strategia (uso della calcolatrice): se un numero non è divisibile per 2, è superfluo eseguire le divisioni per i pari maggiori di 2 (un numero dispari non è divisibile per un numero pari); se un numero non è divisibile per 5, è superfluo eseguire le divisioni per i successivi multipli di 5; ecc. Si arriva così alla conclusione che basta eseguire solo le divisioni per 7, 11, 13, ., cioè le divisioni in cui il divisore è un numero primo diverso da 2, da 3 e da 5.

Successivamente, l'insegnante chiede ai ragazzi a che punto ci possiamo fermare nel provare le divisioni successive. Vediamo alcuni esempi.

439:7= 62,71. non è divisibile per 7
439:11= 39,90. non è divisibile per 11
439:13= 33,76. non è divisibile per 13
439:17= 25,82. non è divisibile per 17
439:19= 23,10. non è divisibile per 19
439:23= 19,08. non è divisibile per 23
Mi posso fermare al divisore 23, perché, con le divisioni che ho fatto, ho escluso tutti i possibili divisori di 439. Infatti, se trovassi un divisore maggiore di 23, la divisione dovrebbe dare un quoziente intero minore di 19, che a sua volta, sarebbe divisore di 439; ma ho già escluso tutti i divisori interi minori di 19.
827:7= 118,14...
827:11=75,18...
827:13=63,61...
827:17=48,64...
827:19=43,52...

827:23=35,95...
827:29=28,51...
Per lo stesso motivo visto nel caso precedente, mi posso fermare al 29.

In questa ricerca con gli alunni possiamo accettare anche prove in più di quelle strettamente necessarie, ma è bene porre la domanda:
- C'è una regola che ci consenta di non sprecare tempo facendo divisioni inutili?
La risposta è che possiamo fermarci quando troviamo un quoziente minore del divisore.
Se l'attività è proposta in una classe in cui gli alunni conoscono già la radice quadrata, possiamo esprimerci così: se vogliamo scomporre un numero n in fattori primi, basta provare a dividere n per tutti i numeri primi minori di $\sqrt{n}$ (infatti se $n = p \cdot q$ allora $p \leq \sqrt{n}$ oppure $q \leq \sqrt{n}$).

Seconda fase

Scriviamo nell'ordine i primi 100 numeri interi positivi in una tabella a 6 colonne e osserviamo la disposizione dei numeri primi.

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	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90
91	92	93	94	95	96
97	98	99	100		

Individuiamo i numeri primi, anche aiutandoci con le tavole.
Fra le osservazioni introduttive, è bene notare che:

- nella prima riga si trovano ben tre numeri primi;
- nelle righe seguenti i numeri primi si diradano: in ogni riga compaiono al massimo due primi; in alcune righe c'è un solo primo e in qualche caso, come nella riga tra 91 e 96, addirittura non c'è alcun numero primo.

Quindi si osserva un'altra regolarità, molto importante: i numeri primi si trovano tutti o nella prima riga, o nella prima colonna, o nella penultima colonna. Infatti, i numeri della seconda, della quarta e della sesta colonna sono pari e, quindi, ad eccezione di 2, non sono primi. D'altra parte, nella terza colonna, non ci sono numeri primi tranne 3, perché tutti i numeri sono multipli di 3.

Va anche detto esplicitamente che ogni apparente regolarità sulla distribuzione dei primi "salta" e non è mai "completa": non c'è una semplice regola per prevedere in quali caselle compare un numero primo.
Si può poi cambiare il numero di colonne: cambieranno di conseguenza le regolarità da osservare. Metodologicamente è importante che ogni alunno compili concretamente almeno una tabella; si possono assegnare diverse tabelle ai diversi componenti della classe e avviare una discussione in gruppo.

Terza fase

Problemi aperti

Osservando la tavola dei numeri primi posta alla fine di ogni testo di matematica, si colgono altre regolarità e proprietà. Contando quanti numeri primi ci sono tra i primi 100 numeri naturali, e poi nel secondo gruppo di 100 naturali, e così via, si nota che i numeri primi si diradano.
Se fissiamo intervalli di ampiezza 1000, avremo che fra 1 e 1000 ci sono 168 numeri primi, tra 1000 e 2000 ce ne sono 135, tra 2000 e 3000 ce ne sono 127, ., tra 9000 e 10000 ce ne sono 112.

Sempre servendoci della tavola dei numeri primi, osserviamo che ci sono spesso coppie di dispari primi consecutivi, come (3; 5), (11; 13), (29; 31). Questi numeri, del tipo p e p+2, si chiamano **primi gemelli**; il primo a battezzare gemelli i numeri primi che differiscono di 2, è stato Paul Stäckel (1862 - 1919), un matematico tedesco esperto in Teoria dei Numeri.
Le coppie di numeri primi gemelli entro il 100 sono:
3 e 5; 5 e 7; 11 e 13; 17 e 19 ; 29 e 31; 41 e 43; 59 e 61; 71 e 73.
C'è una relazione che vale per i numeri primi gemelli: tutti, tranne quelli della prima coppia 3 e 5, sono della forma $6n \pm 1$. Ad esempio, 5 e 7 sono $6x1 \pm 1$; 11 e 13 sono $6x2 \pm 1$; 17 e 19 sono $6x3 \pm 1$, e così via. Questa relazione può essere verificata o scoperta dagli alunni stessi.
La giustificazione è legata a quanto visto nella tabella della Fase 2: tutti i numeri primi maggiori di 3 sono uguali a un multiplo di 6 aumentato oppure diminuito di 1.

La più grande coppia di primi gemelli nota è $2003663613 \times 2195000 \pm 1$.
Si sa che i numeri primi gemelli diventano sempre più rari; a tutt'oggi, però, non sappiamo se esista un'ultima coppia di numeri primi gemelli, oppure se queste coppie siano infinite. Si pensa che ci siano infinite coppie di numeri primi gemelli, ma nessuno finora è riuscito a dimostrarlo: si tratta, quindi, di un "problema aperto".

I ragazzi possono essere invitati a cercare sulle tavole i primi gemelli in un intervallo stabilito, ad esempio tra 1801 e 2099.
Recentemente i numeri primi gemelli, che sono separati da un solo numero pari, vicini ma non abbastanza per toccarsi davvero, hanno ispirato un romanzo di grande successo, *La solitudine dei numeri primi* di Paolo Giordano.

Non è questo il solo problema aperto che riguarda i numeri primi.
Martin Gardner scrive "Nessun ramo della teoria dei numeri è più saturo di mistero e di eleganza dello studio dei numeri primi: quegli esasperati numeri interi ribelli che rifiutano di essere esattamente divisi da qualsiasi altro intero eccetto se stessi e 1.

Alcuni problemi concernenti i numeri primi sono così semplici che può capirli anche un bambino e tuttavia sono così profondi e lontani dalla soluzione che molti matematici ormai temono che possano non avere soluzione." (*Enigmi e giochi matematici*, vol V Sansoni, Firenze 1980)

Parlando dei primi gemelli, si possono porre altri problemi. Ne citiamo due.

- La terna di numeri (3, 5, 7) è formata da tre numeri primi del tipo (p, p+2, p+4). Ci sono altre terne nella stessa situazione?
La risposta è negativa, perché, se si considera una qualunque terna del tipo (n, n+2, n+4), uno dei tre numeri è divisibile per 3.

- Ci sono coppie di numeri primi che differiscono di 4, come 3 e 7 (li potremmo chiamare numeri primi cugini). Facciamo cercare ai ragazzi, con l'aiuto delle tavole, le coppie di primi del tipo (p, p+4) entro il 100.
Si tratta delle coppie: (3; 7), (7; 11), (13; 17), (19; 23), (37; 41), (43; 47), (67; 71), (79; 83).
Per analogia potremmo cercare coppie del tipo: p e p+6; p e p+8 e così via.

Un famoso problema aperto va sotto il nome di **Congettura di Goldbach**, perché il matematico tedesco nel 1742 scriveva ad Eulero chiedendo aiuto per dimostrare che ogni numero pari maggiore di 2 può essere scritto come somma di due numeri primi.
Per esempio: 4=2+2, 6=3+3, 8=3+5, 10=5+5, 12=5+7.
Questa congettura non è stata dimostrata, ma non è stato trovato nemmeno un **controesempio** (cioè non è stato trovato un numero pari maggiore di 2 che non si possa esprimere come somma di due primi).
In *Il Mago dei numeri* di H.M. Enzensberger leggiamo:

- prendi un numero pari, non importa quale, basta che sia superiore a 2, e ti farò vedere che è la somma di due numeri prìncipi.
- 48, esclamò Roberto.
- 31 + 17, disse il vecchio, senza pensarci molto.
- 34, gridò Roberto
- 29 + 5, replicò il vecchio, senza nemmeno levarsi la pipa di bocca.

E funziona sempre? Chiese Roberto stupito. Perché? Piacerebbe saperlo anche a me, disse il vecchio corrugando la fronte e osservando i riccioli di fumo che soffiava in aria. Quasi tutti i maghi dei numeri che conosco hanno cercato di scoprirlo. Funziona sempre, senza eccezioni, ma nessuno sa perché. Nessuno è riuscito a dimostrare che è così.

Per uno studente è interessante verificare che ogni numero pari, ad esempio tra 4 e 100, è somma di due numeri primi. Inoltre possiamo chiedere: c'è qualche numero pari che si ottiene in più modi come somma di due primi? (Per esempio, 16 = 11 + 5 oppure 16 = 13 + 3).
Anche i **numeri primi di Fermat** pongono un problema aperto. Pierre Fermat, matematico del 1600, aveva formulato l'ipotesi (o congettura) che tutti i numeri della forma $2^{(2^n)}+1$ siano primi.

Per esempio:

$F_0 = 2^{(2^0)} + 1 = 3$

$F1 = 2^{(2^1)} + 1 = 5$

$F2 = 2^{(2^2)} + 1 = 17$

$F_3 = 2^{(2^3)} + 1 = 257$

$F_4 = 2^{(2^4)} + 1 = 65537$

...

Tuttavia, nel 1732 Eulero trovò che $2^{(2^5)} + 1$ non è primo perché è il prodotto dei numeri 641 per 6 700 417. La congettura di Fermat, dunque, è sbagliata; ma a tutt'oggi non si sa se i numeri primi di Fermat siano infiniti e, anzi, non si sa se esistano altri numeri primi della forma $2^{(2^n)} + 1$, oltre a quelli citati.
Possiamo chiedere ai ragazzi di verificare con una calcolatrice il risultato di Eulero. È una buona occasione per sottolineare che, se si verifica una certa proprietà in molti casi, questo non basta per stabilire in generale una legge matematica.

Se parliamo di questi numeri in classe, va posta molta attenzione all'uso delle parentesi: per esempio $2^{(2^3)}$, è diverso da $F_3 = (2^2)^3$.

Quarta fase

Numeri primi "grandi"

Il più grande numero primo oggi noto è stato scoperto nell'agosto del 2008: si tratta di 2 elevato alla 43 112 609-ma potenza meno 1, cioè $2^{43112609} - 1$. Questo numero è formato da quasi 13 milioni di cifre: per visualizzarlo nell'usuale notazione decimale, con un editor di testo standard, con 50 righe per pagina e 75 cifre per riga, sarebbero necessarie 3461 pagine.
La scoperta è stata fatta utilizzando i **numeri primi di Mersenne**, ossia i numeri del tipo $2^n - 1$ dove n è primo.

Ai ragazzi più bravi e motivati possiamo proporre un'attività per scoprire alcuni numeri primi di Mersenne. Costruiamo la seguente tabella: nella colonna di sinistra si scrivono i numeri naturali cominciando da 2, nelle colonne successive si trova con la calcolatrice il valore di $2^n - 1$. Infine, si controlla con le tavole se il numero ottenuto è primo. Si osserverà che:

- se n non è primo, si ottiene un numero non primo;
- se n è primo, "molto spesso" si ottiene un numero primo;
- il minimo controesempio si ha per n=11: infatti, 11 è un numero primo, ma $2^{11} - 1$ è uguale a 2047, che non è primo, anche se non è facile da scomporre (23x89).

n>1	$2^n - 1$	Risultato	È primo?
2	$2^2 - 1$	3	SI
3	$2^3 - 1$	7	SI
4	$2^4 - 1$	15	NO
5	$2^5 - 1$	31	SI
6	$2^6 - 1$	65	NO
7	$2^7 - 1$	127	SI
8	$2^8 - 1$	255	NO
9	$2^9 - 1$	511	NO
10	$2^{10} - 1$	1023	NO
11	$2^{11} - 1$	2047	NO
12	$2^{12} - 1$	4095	NO
13	$2^{13} - 1$	8191	SI

Ancora una volta non possiamo "fidarci" di una regolarità che vale per un certo numero di casi: con n=11 abbiamo trovato un controesempio, e quindi sappiamo che in generale, se n è primo, non è detto che anche $2^n - 1$ sia primo. Tuttavia, la relazione di Mersenne ha aiutato a trovare nuovi numeri primi "grandi" (per numero primo grande si intende un numero primo con almeno 100 cifre).

La scoperta di grandi numeri primi di Mersenne è stata possibile grazie al lavoro congiunto di decine di migliaia di computer. Ma qual è il valore della scoperta? A che cosa servono i numeri primi grandi?
Forse per superare un record, ma più plausibilmente per la **crittografia** moderna.
Crittografia è parola di origine greca che significa **scrittura segreta**; troviamo questa tecnica già nella Bibbia, in cui si parla di un codice segreto per scrivere il nome di Babele (il codice Atbash). Per secoli la crittografia è stata usata quasi esclusivamente a scopi militari e diplomatici.
Oggi un uso assai frequente della crittografia è nelle transazioni online: per evitare truffe è necessario utilizzare messaggi non facili da decodificare. Chi usa il bancomat, internet, il cellulare, ricorre, senza saperlo a tecniche crittografiche. L'idea è che il passaggio dal messaggio alla codifica deve essere molto più facile del passaggio inverso (si veda l'approfondimento disciplinare). In termini matematici, si sfrutta il fatto che è facile calcolare il prodotto di due numeri primi (esempio: 503 x 137 = 68911), mentre la ricostruzione dei fattori a partire dal prodotto è molto più laboriosa e richiede molto più tempo. Nella pratica, si usano prodotti di numeri primi più grandi, in modo da renderne estremamente lunga, anche per un potente computer, la scomposizione. A titolo di curiosità, aggiungiamo che ci sono premi in denaro per chi scopre nuovi numeri primi.

Indicazioni metodologiche

L'insegnante avrà cura di verificare l'acquisizione dei prerequisiti necessari per svolgere serenamente l'attività (conoscenza dei concetti di multiplo, di divisore, dei criteri di divisibilità, del significato di numero primo).
Proporrà esercizi e quesiti in modo problematico, per sviluppare le capacità di riflessione, di ragionamento, di intuizione, di problem solving; sarà opportuno sollecitare i ragazzi anche ad affinare le capacità di calcolo, scritto e mentale.

L'insegnante favorirà il lavoro a coppie e di gruppo, mettendo a disposizione materiale vario (tavole numeriche, calcolatrice, sitografia, testi scolastici,.) e solleciterà la discussione, la scoperta di regolarità, la formulazione di congetture.
In ogni caso evidenzierà l'importanza di un contesto interno alla matematica per riconoscere e risolvere problemi numerici che facilitino il passaggio alla formalizzazione e alla generalizzazione.

Spunti per un approfondimento disciplinare

Infinità dei numeri primi

Euclide nel 300 a.C. ha dimostrato in modo elegante che 'Esistono numeri primi in numero maggiore di quanti numeri primi si voglia proporre'.
Nella traduzione di Fraiese-Maccioni degli Elementi si trova la seguente considerazione: «Euclide non introduce direttamente l'infinità dei numeri primi. Si tratta soltanto dell'infinità intesa in senso potenziale: qualunque insieme di numeri primi ci piaccia fissare esiste sempre almeno un altro numero primo non compreso nell'insieme: cioè i numeri primi sono sempre di più di qualunque quantità prefissata di numeri primi».
La dimostrazione per assurdo è la seguente. Si suppone che l'insieme dei numeri primi sia finito:
$P = \{p_1, p_2, \ldots, p_t\}$
e costruisce un nuovo numero naturale N calcolando il loro prodotto e sommando 1:
$N = p_1 \cdot p_2 \cdot \ldots \cdot p_t + 1$
Per tale numero si presentano due possibilità:

- N è un numero primo maggiore di p_t e quindi quest'ultimo non è il più grande di tutti i numeri primi;
- N non è un numero primo, ma allora ammette un divisore primo che non compare tra i $p_i \in P$, in quando il resto della divisione di N per ciascun p_i è uguale a 1.

Geometria e numeri primi

Sorprendente è il collegamento tra geometria e numeri primi.
La costruzione con riga e compasso dei poligoni regolari di n lati rappresentò una sfida per i matematici dall'antichità fino al XIX secolo. Tale costruzione è equivalente alla suddivisione della circonferenza in n archi uguali (problema della ciclotomia): congiungendo i punti in cui la circonferenza viene suddivisa, si ottiene il poligono regolare, cioè equilatero ed equiangolo, che si vuole costruire.
Gauss nel 1796 dimostrò che la costruzione con riga e compasso di un poligono regolare di n lati è possibile se e solo se n è una potenza di 2, o il prodotto di una potenza di 2 e di uno o più numeri primi di Fermat (cioè del tipo $2^{(2^n)}+1$), a due a due diversi fra loro.
La circonferenza, dunque, può essere suddivisa in 17 parti uguali, ma non in 7, dato che 7 non è un primo di Fermat: la costruzione dell'ettagono regolare risulta quindi impossibile con l'uso degli strumenti elementari. Gli unici primi di Fermat conosciuti sono 3, 5, 17, 257, 65537. Una tabella sulla costruzione dei poligoni regolari spiega meglio la situazione.

n	conoscenze ellenistiche	risultati di Gauss		n	conoscenze ellenistiche	risultati di Gauss
3	SI	SI		12	SI	SI
4	SI	SI		13	?	NO
5	SI	SI		14	?	NO
6	SI	SI		15	SI	SI
7	?	NO		16	SI	SI
8	SI	SI		17	?	SI
9	?	NO		18	?	NO
10	SI	SI		19	?	NO
11	?	NO		20	SI	SI

Notiamo che la dimostrazione di Gauss è stata una delle prime "dimostrazioni di impossibilità" di una certa costruzione.
Gauss risolve tutti i casi dubbi, per la maggior parte con una dimostrazione di impossibilità, ma nel caso n=17 dando una nuova costruzione. Pare che la costruzione del poligono regolare di 17 lati sia stata per Gauss a 18 anni un successo. Gauss fu così entusiasta della sua scoperta che chiese che sulla sua tomba fosse inciso un poligono regolare di 17 lati. Lo scultore si rifiutò, sostenendo che la costruzione era troppo difficile e che il poligono risultante non si sarebbe distinto da una circonferenza.

Numeri primi e crittografia

Un discorso più esteso merita la relazione tra numeri primi e crittografia. Dagli anni '50 i conti necessari per controllare se numeri grandi sono primi vengono effettuati dalle macchine calcolatrici; c'è stata anche un'utilità pratica, perché i programmi per riconoscere numeri primi (test di primalità) sono stati usati per testare nuovo hardware.
A partire dagli anni '80, numeri primi grandi sono usati per cifrare messaggi segreti con il metodo di **crittografia a chiave pubblica** detto RSA (dai nomi dei suoi ideatori Rivest, Shamir e Adleman). L'aspetto nuovo è che la chiave per cifrare non è la stessa di quella per decifrare; per questo motivo si parla anche di **cifrari asimmetrici**.
Questi sistemi sono resi sicuri dal fatto che si basano su funzioni relativamente facili da calcolare ma molto difficili da invertire: il prodotto di due numeri primi è facile da calcolare, ma la fattorizzazione del prodotto è assai più complessa. Anche al giorno d'oggi, la fattorizzazione di un numero di 150 cifre resta in generale un problema difficile.
Per cercare di capire il funzionamento del metodo RSA, immaginiamo che A debba spedire un messaggio segreto a B. Occorrono i seguenti passaggi:
1. B sceglie due numeri primi molto grandi (per esempio da 300 cifre) e li moltiplica con il suo computer (impiegando meno di un secondo).
2. B invia il numero che ha ottenuto ad A. Qualcuno può intercettare questo numero.
3. A usa quel numero per cifrare il messaggio.
4. A manda il messaggio cifrato a B; il messaggio può essere intercettato, ma decifrarlo è molto difficile.
5. B riceve il messaggio, che è in grado di decifrare utilizzando i due fattori primi che solo lui conosce.
A e B hanno impiegato pochi secondi a cifrare e decifrare, ma chiunque avesse intercettato le loro comunicazioni impiegherebbe secoli per scoprire i due fattori primi, con cui si riesce a decifrare il messaggio.
Per approfondire questo argomento si può fare riferimento al testo Crittologia di Berardi, Beutelspacher oppure a Codici e segreti di Simon Singh.

Curiosità

Sui numeri primi sono state trovate molte curiosità: Mario Livio, nel libro La sezione aurea, scrive "La maggior parte delle persone è d'accordo che certi primi siano più gradevoli di altri". Alcuni matematici come il francese Françoise Le Lionnais e l'americano Chris Caldwell aggiornano l'elenco di numeri < notevoli > e < titanici >. Ecco qualche gemma tratta dal ricco filone dei numeri primi:

- il numero 1 234 567 891, che comprende tutte le cifre escluso 0, è primo;
- il numero formato da 317 cifre uguali a 1 è primo
- c'è un numero primo, di 6400 cifre, che è formato da 6399 nove e un solo otto.

Elementi per prove di verifica

1) Completa le seguenti frasi:
a. Il più piccolo numero primo pari è ..
b. Il più piccolo numero primo dispari è ..
c. Il più grande numero primo di due cifre è ..
d. Il più piccolo numero primo di due cifre è ..

2) È corretto dire che "un numero naturale maggiore di 1 si chiama primo se ammette come divisori se stesso e 1"?

3) Due numeri primi consecutivi sono primi fra loro? C'è un solo caso in cui due numeri consecutivi sono entrambi primi: quali sono questi numeri?

4) Quale può essere la cifra delle unità di un numero primo maggiore di 5? (Ci sono solo 4 possibilità).

5) Trova tutti i numeri dispari minori di 100 che hanno la cifra delle decine doppia della cifra delle unità. Sono numeri primi? Motiva la tua risposta.

6) In alcuni casi la somma di due numeri primi è un numero primo: sai fare qualche esempio?

7) Il prodotto di due numeri primi non può mai essere un numero primo. Perché?

8) Completa la seguente tabella con i numeri primi minori di 100 che si ottengono sommando 1 ad un multiplo di 4. Osserva che questi numeri primi si possono rappresentare come somma di due numeri al quadrato.

Numeri primi	4n +1	Somma di quadrati
5	4x1 + 1	$2^2 + 1^2$
13	4x3 + 1	$3^2 + 2^2$
17	...	...
29		
...		

9) Una formula per trovare numeri primi?
a. Considera i numeri della forma $n^2 + n + 41$. Sostituisci ad n i valori 0, 1, 2, 3, 4, 5 e, aiutandoti con le tavole, scopri se il numero trovato è primo.
b. Dopo aver considerato diversi casi, siamo sicuri che la formula $n^2 + n + 41$ fornisce soltanto numeri primi?
c. Considera il valore n = 41. Trovi $41^2 + 41 + 41$. Come puoi far vedere che non è primo?

Scarica il documento con gli esercizi

Spunti per altre attività con gli studenti

L'arte di scrivere messaggi segreti e cifrati è molto antica; esempi si trovano nelle Storie di Erodoto, opera dedicata in gran parte alle guerre che i Greci combatterono contro i Persiani nel V secolo a.C. Si racconta di messaggi occultati su tavolette di cera con più strati ed anche di messaggi sulla cute rasata e nascosti da capelli ricresciuti. Questi ed altri metodi di occultamento erano comunque soggetti ad intercettazione; fu così che si comincio a pensare a metodi di crittografia.
La crittografia non mira a nascondere il messaggio, ma cerca di renderne incomprensibile il significato: il testo viene alterato con un metodo concordato tra mittente e ricevente. Invertendo il procedimento usato per criptare un messaggio, si ricostruisce il messaggio originale. Si possono proporre agli alunni alcuni metodi di crittografia leggendo brani del libro di Singh "Codici e segreti" (ad esempio da pag. 13 a pag. 29), da cui sono tratti gli esempi che seguono.

1) La scitale - risale a Sparta, nel V sec. A. C. Si tratta di un'asticella di legno attorno alla quale veniva arrotolata una striscia di pelle o di pergamena. Il mittente scriveva il messaggio e poi srotolava la striscia che veniva usata come cintura o altro. Il ricevente doveva avere una scitale dello stesso diametro.

Questo procedimento si realizza bene con striscioline di carta avvolte su una matita: si scrive sulla carta avvolta e poi si invia solo la striscia, sulla quale le lettere appaiono casuali; per leggere il messaggio bisogna riavvolgere la strisciolina su una matita uguale.

2) Trasposizione a inferriata

Consiste nella trascrizione di un testo in due righe orizzontali, una superiore e una inferiore, passando da una riga all'altra ad ogni successivo carattere alfabetico. Finita la trascrizione, la seconda riga sarà accodata alla prima per dare origine al testo cifrato. Come esempio, cifriamo la frase seguente.

Un segreto è il tuo prigioniero se lo lasci andare sarai suo prigioniero

U	S	G	E	O	I	T	O	R	G	O	I	R	S	L	L	S	I	N	A	E	A	A	I	S	O	R	G	O	I	R
N	E	R	T	E	L	U	P	I	I	N	E	O	E	O	A	C	A	D	R	S	R	I	L	U	P	I	I	N	E	O

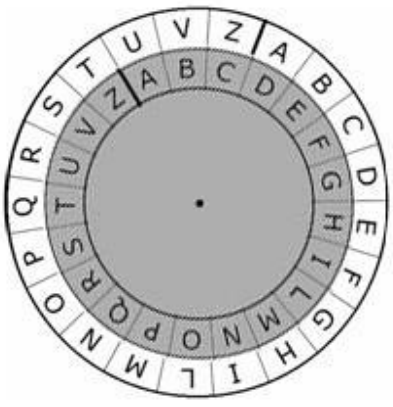
Testo cifrato:
USGEOITORGOIRSLLSINAEAAISORGOOIRNERTELUPIINEOEOACADRSRILUPIINEO

3) Sostituzione

Già Giulio Cesare inviava gli ordini scritti associando a ogni lettera quella che veniva dopo tre posizioni nell'alfabeto: la A diventava D, la B si trasformava in E, la C in F e cosi via.
Alfabeto chiaro ABCDEFGHILMNOPQRSTUVZ
Alfabeto cifrante DEFGHILMNOPQRSTUVZABC

testo chiaro	**veni vidi vici**
testo cifrato	**bhqn bngn bnfn**

Si può proporre ai ragazzi la costruzione di uno strumento per cifrare messaggi con questo algoritmo. Lo strumento è costituito da due cerchi concentrici di 21 posti (se si usa un alfabeto con 21 lettere). Il cerchio all'esterno è l'alfabeto chiaro e quello all'interno il cifrante; è bene mettere frecce o segni per evitare confusioni.



Il lavoro si svolge a piccoli gruppi: ogni gruppetto deve scrivere una frase composta da almeno 10 parole e la deve cifrare. Il messaggio cifrato passa ad un altro gruppo.
Ogni gruppo cerca di decrittare il messaggio ricevuto, scrivendo il procedimento seguito.

Avvenuto lo scambio e la decifrazione, a classe intera si discute delle strategie usate dai vari gruppi e delle difficoltà incontrate. Una variante che crea qualche difficoltà in più è quella di scrivere la frase cifrata senza lasciare nessuno spazio fra le parole, senza punteggiatura e senza accenti.

4) Accoppiamento casuale

Un'altra tecnica crittografica consiste nell'accoppiare in modo casuale le lettere dell'alfabeto e nel sostituire ciascuna lettera con quella a lei accoppiata. In questo caso lo strumento prima descritto è sempre costituito da due dischi, ma con lettere nel disco cifrante messe a caso.
Si fa preparare da un gruppo un messaggio cifrato di almeno 25 parole e il gruppo lancia la sfida alla classe (anche l'insegnante prova a decrittare). Il problema è diventato molto più difficile da risolvere.

La ricerca della soluzione è facilitata se si tiene conto della frequenza delle diverse lettere in italiano. Sul libro "Codici e segreti" c'è una tabella a pag. 20 che riportiamo:

Tavola 1 Frequenze delle diverse lettere in italiano.

Lettera	Percentuale	Lettera	Percentuale
a	11,74	n	6,88
b	0,92	o	9,83
c	4,50	p	3,05
d	3,73	q	0,51
e	11,79	r	6,37
f	0,95	s	4,98
g	1,64	t	5,62
h	1,54	u	3,01
i	11,28	v	2,10
l	6,51	z	0,49
m	2,51		

Se il percorso della classe lo consente, si può aprire una parentesi legata al tema "dati e previsioni", e trovare la frequenza delle lettere in modo sperimentale. Si distribuiscono ai diversi alunni brani tratti da testi diversi (di 4-5 righe ciascuno), si chiede di costruire una tabella con tre colonne: nella prima colonna mettiamo le lettere dell'alfabeto, nella seconda colonna la **frequenza assoluta*** (quante volte la lettera compare nel testo), nella terza colonna la frequenza percentuale (ricavata tenendo conto del numero totale di lettere del testo). Dopo che ogni gruppo ha trovato la frequenza di ogni lettera, è bene confrontare le frequenze tra di loro. Si possono poi calcolare le frequenze percentuali delle lettere dell'intera classe sommando le frequenze assolute e le lunghezze delle frasi analizzate da tutti i gruppi. È bene anche confrontare i dati con quelli che si trovano nella tabella precedente.

Con queste nuove informazioni sarà più facile decrittare il messaggio. È importante chiedere agli alunni perché la frequenza delle lettere ci ha aiutato, e cosa succede se cambiamo lingua (la frequenza delle lettere sarà la stessa?).
(Da un percorso sperimentato a Scuola-Città Pestalozzi da F. Spinelli)

***** vedi l'attività **Frequenza assoluta o frequenza relativa?**
https://repository.indire.it/repository/working/export/249/

Bibliografia

AAVV, Matematica 2001. *Materiali per un nuovo curricolo di matematica con suggerimenti per attività e prove di verifica. Scuola primaria. Scuola secondaria di I grado* (scarica il documento)
https://umi.dm.unibo.it/wp-content/uploads/2020/04/Matematica2001.pdf).

AAVV, Matematica 2003. *Materiali per un nuovo curricolo di matematica con suggerimenti per attività e prove di verifica. Scuola secondaria di II grado* (scarica il documento)
https://umi.dm.unibo.it/wp-content/uploads/2020/04/Matematica2003.pdf).

AAVV, Matematica 2002. *Materiali per un nuovo curricolo di matematica con suggerimenti per attività e prove di verifica* (scuola elementare e scuola media).

PISA 2003 Valutazione dei quindicenni a cura dell'OCSE, Roma, Armando Armando, 2004

Gli Elementi di Euclide (a cura di A. Frajese e L. Maccioni), Torino, UTET, 1970

Euclide, Tutte le opere (a cura di Fabio Acerbi), Bompiani 2007

M. Livio - La sezione aurea - Storia di un numero e di un mistero che dura da tremila anni - BUR - 2003 pag.348

Simon Singh -"Codici e segreti svelati ai ragazzi", Fabbri Editori, 2002Lucia Berardi, Albrecht Beutelspacher - "Crittologia, come proteggere le informazioni riservate", Franco Angeli, 1996

H.M. Enzensberger, "Il Mago dei numeri", Einaudi 2005

Sitografia

UMI-CIIM: Matematica, didattica per la scuola, sitografia
https://umi.dm.unibo.it/materiali-umi-ciim/

Invalsi https://www.invalsi.it/invalsi/ric.php?page=ocsepisa06

Proposta di attività per il corsista

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.