Università di Pisa

Corso di Perfezionamento in "Strategie didattiche per promuovere un atteggiamento positivo verso la matematica e la fisica"

Relazione di Tirocinio

E. Balducci, A. Blotti, F. Daddi

1 aprile 2007

Indice

1 Introduzione

La Settimana Matematica 2007 che si è svolta al Dipartimento di Matematica (5-8 febbraio 2007) ci ha visto coinvolti, come studenti del corso di perfezionamento, nel laboratorio 5: *Problemi e congetture in aritmetica: da Goldbach a Wiles coordinato dal* Prof. G. Puglisi

In questa relazione abbiamo riportato il lavoro svolto e le riflessioni, legate ai temi del corso di perfezionamento, che questa esperienza ha fatto nascere.

Il gruppo di studenti presenti al Laboratorio era costituito da 6 maschi e 11 femmine. La partecipazione alle lezioni è stata vivace e gli studenti si sono subito appassionati al mondo misterioso che avvolge questo argomento. Siamo tutti ben consapevoli che il mondo dei numeri ruota attorno ad alcune verità di facile comprensione anche per uno studente delle scuole superiori, e infatti i ragazzi hanno seguito con attenzione ed in modo proficuo le dimostrazioni a loro presentate.

Il clima che si è creato in aula è stato familiare soprattutto grazie alla umanità del Prof. Puglisi che si è coinvolto personalmente con quasi tutti gli studenti, scambiando qualche battuta anche nelle pause. La chiarezza e la precisione argomentativa del professore è stata molto apprezzata dai ragazzi che hanno potuto prendere gli appunti in maniera ordinata - tranne qualche eccezione. Abbiamo chiesto di poter fare le fotocopie dei loro appunti ma nessuno, liberamente, ci ha consegnato il materiale; forse una maggiore insistenza da parte nostra avrebbe potuto mostrare, in questo lavoro, la buona qualità dei loro appunti. Alcuni ragazzi si sono fermati durante le pause e alla fine della lezione a fare domande sullo studio universitario. Un buon numero di ragazzi del gruppo ha dimostrato buone capacità nell'approcciare i problemi proposti e nel seguire, con osservazioni e domande pertinenti, le lezioni del professore. Abbiamo anche notato che questo "sano" interesse verso la matematica è corrotto da una preoccupazione per il futuro e per l'eventuale difficoltà del percorso di studi. Sarebbe interessante capire se tali preoccupazioni, che non sembrano essere proprie di una età di grande aspirazioni come la loro, sono prodotte dalla scuola o dall'ambiente familiare.

Nella prima lezione sono stati introdotti concetti a loro familiari, come quella di multiplo e di divisore, introducendo la formalizzazione necessaria per non appesantire le dimostrazioni e per trovare un linguaggio simbolico condiviso da tutti. In effetti i prerequisiti per addentrarsi in questo mondo non sono di complessità elevata: occorre saper eseguire la divisione euclidea e conoscere (che si sia dimostrato oppure no) che la scomposizione in fattori primi è unica. Molti di loro non sapevano perché 1 non è considerato primo.

Ai ragazzi sono state presentate, oltre alla dimostrazione dell'infinità dei numeri primi, anche la dimostrazione dell'algoritmo euclideo per la determinazione del massimo comun divisore; quest'ultimo è un concetto che i ragazzi conoscono benissimo, ma che sanno calcolare, dalle scuole medie, con la scomposizione in fattori primi.

Nella seconda lezione sono stati presentati i vari modi per trovare i numeri primi e le congetture a loro legate (il teorema di Dirichlet) nonché i primi di Fermat e i primi di Mersenne e le congetture a loro legate (falsa nel caso di Fermat e irrisolte nel caso di Mersenne). Nella seconda parte della lezione i ragazzi sono stati chiamati a risolvere alcuni esercizi, per mettere in pratica le conoscenze acquisite. In questa parte sono state introdotte anche le equazioni diofantee per le quali si era precedentemente dimostrato il teorema di Bezout.

Sono state introdotte anche in modo semplice le congruenze con la loro simbologia e sono stati proposti alcuni esercizi di costruzione di tabelle di addizione modulo n. Si sono osservate differenze tra n primo e n non primo; alcuni ragazzi non avevano mai visto questi argomenti e per la prima volta hanno visto il primo esempio di divisori dello zero.

Nella terza lezione si è parlato della congettura di Fermat e della dimostrazione di Wiles e di altre congetture ancora irrisolte come quella dei primi gemelli della forma p, $p+2$, di cui ancora non esiste la dimostrazione riguardo la loro infinità (si suppone che la congettura sia vera dal momento che, ultimamente, si sono trovate coppie di tal genere con milioni di cifre). Si è parlato anche delle terne pitagoriche (unico caso in cui la congettura di Fermat trova soluzioni non banali) e della loro forma. Infine sono stati fatti alcuni cenni sugli algoritmi di primalità, deterministici e non.

2 Le lezioni

Riportiamo, in questa sezione, gli appunti delle lezioni del Prof. Puglisi.

Abbiamo cercato di sintetizzare il più possibile lì dove la lezione ha seguito una linea tradizionale e nello stesso tempo abbiamo cercato di sottolineare i punti in cui la lezione è stata più "teatrale", usando le stesse parole del professore.

2.1 Prima Lezione

L'insieme dei numeri naturali. Notazione: parentesi graffe, simbolo di appartenenza, i puntini per indicare che continuano all'inifinito. La questione dello zero (lo zero così naturale non è: i romani non lo usavano).

$$\mathbb{N} = \{1, 2, 3, 4, \cdots\}$$

L'insieme dei numeri relativi. Qui lo zero c'è di sicuro. I numeri a coppie: segno + e segno -. Come scriverli: doppi puntini a sinistra e a destra? (si pretende troppo dal lettore):

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \cdots\}$$

Le operazioni nell'insieme dei numeri naturali: l'addizione (+) e le sue proprietà; l'operazione inversa all'addizione: la sottrazione (-).

Definizione 1 *:* $n - m = k$ *significa che* $m + k = n$

La sottrazione si può sempre fare in $\mathbb{Z}$ ma non in $\mathbb{N}$.

L'operazione di moltiplicazione $(\cdot)$ e l'operazione inversa $(:)$.

Definizione 2 *:* $n : m = k$ *significa che* $m \cdot k = n$

La divisione non è sempre possibile in $\mathbb{Z}$.
Fin qui è l'aritmetica elementare.
Introduciamo adesso il concetto di divisibilità tra interi (che ha a che fare con la divisione).

Definizione 3 *:* $m \mid n$ *(si legge* m *divide* n*) vuol dire che la divisione* $n : m$ *si può fare.*

Esempio. : $2 \mid 3$? No, infatti per definizione di divisione dovrebbe $\exists k \in \mathbb{N}$ t.c.$2k = 3$. Poiché ciò non è possibile scriveremo che $2 \nmid 3$. ■
Riscriviamo la definizione di sopra in maniera formalmene corretta:

Definizione 4 *:* $m \mid n$ *se* $\exists k \in \mathbb{N}$ *t.c.*$m \cdot k = n$

Esempio. : $5 \mid 26$? No. Però posso fare la divisione con resto (che si può sempre fare). Devo quindi trovare il più grande numero k che moltiplicato per 5 (non fa, chiaramente, 26) si "parcheggia" il più vicino possibile a 26. Questo numero k è 5: infatti $26 = 5 \cdot 5 + 1$. Il numero 1 è quello che serve per arrivare a 26. ■
[Esempio un pò sfortunato: era meglio avere un quoziente diverso dal divisore!]
Osserviamo che il resto è sempre minore del divisore.
La stesse considerazioni valgono sui polinomi.
Le proprietà ovvero cose che è bene conoscere.

Proprietà 1 *:* $m \mid n$ *e* $m \mid l \Longrightarrow m \mid n + l$ *(e* $m \mid n - l$ *in* $\mathbb{Z}$*)*

[Il professore fa un commento sulla pigrizia storica sulle lettere: si prendono tutte nell'intorno di n che sta per numero].

Proprietà 2 *(transitiva):* $m \mid n$ *e* $n \mid l \Longrightarrow m \mid l$

Adesso occupiamoci della struttura algebrica $(N, \cdot)$: questa scrittura vuol dire che ci occupiamo dei numeri naturali dal punto di vista dell'operazione di moltiplicazione.
$(N, +)$ vorrebbe dire studiare i naturali dal punto di vista dell'addizione. In questa struttura il numero 1 fa da mattone, perché da esso si possono costruire tutti i numeri naturali (mono-mattonico).
Se consideriamo la struttura $(N, \cdot)$ le cose sono diverse. Ci sono i mattoni? Cioé esistono numeri "mattoni" che consentono di generare tutti i numeri naturali usando la moltiplicazione? Sapete che la risposta è sì: stiamo parlando dei numeri primi o irriducibili. Indichiamo l'insieme dei numeri primi con la lettera P. Nell'insieme dei numeri primi non c'è l'1; il numero 1 è neutro per la moltiplicazione nel senso che moltiplicare per 1 un qualsiasi numero non ha alcun effetto: il prodotto coincide con il numero.
Osserviamo che ogni intero ha due divisori di diritto: il numero 1 e se stesso:

Osservazione 1 *:* $1 \mid n$ *e* $n \mid n$.

Quanti sono i numeri primi? La risposta a questa domanda si deve ad Euclide:

Teorema 1 *(di Euclide): I numeri primi sono infiniti.*

Dimostrazione. La dimostrazione è per assurdo.
Supponiamo che sia p_N il numero primo più grande.
Costruiamo il numero n così fatto:

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_N$$

dove $p_1 = 2, p_2 = 3, p_3 = 5$ e così via. Chiaramente n è un "interone" cioè un numero molto grande. Consideriamo il successivo di n cioé $k = n+1$. Poniamoci le seguenti domande:

$p_1 \mid k$? E' chiaro che la risposta è no; infatti se facciamo la divisione di k per p_1 ci verrà un resto pari a 1 :

$$k = n + 1 = \underbrace{p_1}_{divisore} \cdot \underbrace{(p_2 \cdot p_3 \cdot \cdots \cdot p_N)}_{quoziente} + \underbrace{1}_{resto}$$

Apriamo una piccola finestra:
dalle proprietà di sopra segue che se $a \mid m$ e $a \mid m+1$ allora $a \mid m+1-m$ e quindi $a \mid 1$ ovvero $a = 1$. Questo significa che l'unico intero che divide due numeri successivi è il numero 1.
Deduciamo quindi che:

$$p_1 \nmid k, \quad p_2 \nmid k, \quad \cdots \quad p_N \nmid k$$

allora k non è divisibile per nessuno dei numeri primi, ma questo è assurdo perché k essendo un intero ha diritto di essere divisibile[1]. Da questo assurdo si deduce che deve esistere un altro numero primo maggiore di p_N che divide k.

Facciamo alcune prove:

$2 \cdot 3 + 1 = 7$ è primo
$2 \cdot 3 \cdot 5 + 1 = 31$ è primo
$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ è primo.

Continuando in questa maniera si ottengono sempre numeri primi? La risposta è no, quindi esistono numeri della forma $p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_N + 1$ che non sono primi. I numeri primi di questa forma vengono detti primoriali.

L'importanza dei numeri primi risiede nel teorema fondamentale dell'aritmetica:

[1] Si sta facendo riferimento al teorema fondamentale dell'aritmetica.

Teorema 2 *(fondamentale dell'aritmetica): Ogni intero positivo maggiore di 1 si scrive come prodotto di numeri primi in modo essenzialmente unico.*

Non lo dimostriamo.

Uno dei problemi più affascinanti è quello delle formule per i numeri primi.

Problema: esiste una "formula" per l'n-simo numero primo p_n? O in formule, esiste $p_n = f(n)$?

Da due secoli si ritiene che la risposta a questa domanda sia no.

Un'altra domanda interessante è la seguente:

Problema: esiste una formula ricorsiva? esiste, cioé, una formula che usando i numeri $p_1, p_2, \cdots p_{n-1}$ consenta di trovare p_n?

Qualcosa si può fare però non si trovano tutti i numeri primi: se ne saltano alcuni. Per esempio si sa che:

$$\exists \alpha_0 \in \mathbb{R} \text{ tale che } [2^{\alpha_0}] = \alpha_1 \qquad [2^{\alpha_1}] = \alpha_2 \qquad \cdots \text{ sono tutti primi}$$

(le parentesi quadre indicano qui la parte intera del numero reale. Il problema, in questo caso, è che non si sa quanto vale α_0!

Abbassiamo il tiro. Ci chiediamo: fissato un numero primo qualunque, esiste un modo per scriverne un altro più grande? Chiaramente il modo deve essere unico.

Se ciò si potesse fare potremmo trovare un numero primo a 100 cifre!

2.2 Seconda lezione

Oggi ci occupiamo di numeri primi in forma esponenziale, cioé di numeri del tipo

$$p = a^n + b. \tag{1}$$

E' chiaro che $p = a^n$ non è primo e quindi ho dovuto sommare il numero b.

Iniziamo con l'osservare che se a è dispari allora a^n è dispari (essendo il prodotto di dispari); allora se $b = 1$ segue che $a^n + 1$ è pari. Per avere qualche speranza di generare primi deve essere a pari. Allora partiamo dal caso più semplice: $a = 2$ e $b = 1$.

Esistono primi della forma

$$p = 2^n + 1?$$

La risposta è sì e non bisogna andare neanche tanto lontano. Il numero 5 è in questa forma: $5 = 2^2 + 1$. Proviamo con $n = 3$. si vede subito che $2^3 + 1 = 9$ non è primo. Con $n = 4$ le cose invece funzionano perchè $2^4 + 1 = 17$ è primo.

Osservazione 2 *: Perché la formula abbia qualche speranza di generare un numero primo, n deve essere una potenza di 2, cioé deve essere $n = 2^k$, $k \in \mathbb{N}$.*

Dimostriamo. Non sono sicuro che venga fuori un numero primo però so dire che se non fosse $n = 2^k$ allora sicuramente non ottengo un numero primo. Il teorema può suonare così:

Teorema 3 : *Se $n \neq 2^k$ allora $p = 2^n + 1$ non è primo.*

Dimostrazione. Se n non è una potenza di 2 allora n è il prodotto di una potenza di 2 per un numero dispari:

$$n = 2^k \cdot d$$

dove d è un numero dispari. Riscriviamo il nostro numero p :

$$p = 2^n + 1 = 2^{2^k \cdot d} + 1 = (x)^d + 1$$

dove abbiamo chiamato $x = 2^{2^k}$; chiaramente x è pari. Il numero p scritto in questa maniera ci ricorda la scomposizione dei polinomi. Sappiamo, infatti, che il polinomio $x^d + 1$ è divisibile per $(x+1)$ se d è dispari. Allora possiamo scrivere:

$$p = x^d + 1 = (x+1) \cdot (b)$$

dove b è un numero. Cosa deduciamo?

$$(x+1) \mid \underbrace{(x^d+1)}_{p} \implies (x+1) \mid \underbrace{2^n+1}_{p} \implies \left(2^{2^k}+1\right) \mid (2^n+1)$$

quindi $2^n + 1$ non può essere primo essendo $2^{2^k} + 1$ un suo divisore maggiore di 1. E' chiaro che tutto è stato una conseguenza del fatto che d è dispari. .

Interessiamoci allora del caso in cui $n = 2^k$. Si tratta della famosa congettura di Fermat:

Congettura 1 *(di Fermat):* $\forall k, F_k = 2^{2^k} + 1$ *è primo.*

Ecco le prove che fece Fermat:

$k = 0 \implies F_0 = 2^{2^0} + 1 = 3$
$k = 1 \implies F_1 = 2^{2^1} + 1 = 5$
$k = 2 \implies F_2 = 2^{2^2} + 1 = 17$
$k = 3 \implies F_3 = 2^{2^3} + 1 = 257$
$k = 4 \implies F_4 = 2^{2^4} + 1 = 65\,537$

E si fermò qui. Un secolo dopo Eulero provò che F_5 non è primo:
"$F_5 = 2^{2^5} + 1 = 4294\,967\,297$ è divisibile per 641"

Ad oggi non si sono trovati primi di Fermat per $k > 5$. Si pensa che per $k > 5$ non ci siano primi di Fermat, ma nessuno lo ha dimostrato; si tratta quindi di una congettura inversa rispetto a quella di Fermat che si può esprimere così:

Congettura 2 : $\forall k > 5, F_k = 2^{2^k} + 1$ *non è primo.*

Facciamo un ulteriore passo e consideriamo ora il caso in cui sia $b = -1$ nella formula 1. Consideriamo i numeri della forma

$$a^n - 1.$$

In analogia a quanto fatto prima, osserviamo che il polinomio $a^n - 1$ è divisibile per $a-1$; quindi se $a > 2$ il numero $a^n - 1$ non è certamente primo. Consideriamo allora il caso $a = 2$. Procediamo con le nostre osservazioni. I numeri $2^n - 1$ hanno una qualche speranza di essere primi? C'è qualche condizione su n? Osserviamo subito che se n non è primo vuol dire che posso scrivere $n = h \cdot k$ con h, k maggiori di 1. Segue che:

$$2^n - 1 = \left(2^h\right)^k - 1 = x^k - 1 = (x-1) \cdot \left(x^{k-1} + \cdots\right)$$

e quindi $2^n - 1$ è divisibile per $x - 1 = 2^h - 1$ che è sicuramente maggiore di 2. Si tratta di considerare solo gli n primi.

Chiameremo numeri di Marsenne i numeri del tipo:

$$M_p = 2^p - 1 \text{ con } p \text{ primo}$$

Qualche prova:

$$\begin{aligned}
p = 2 &\implies M_2 = 2^2 - 1 = 3\\
p = 3 &\implies M_3 = 2^3 - 1 = 7\\
p = 5 &\implies M_5 = 2^5 - 1 = 31\\
p = 7 &\implies M_7 = 2^7 - 1 = 127
\end{aligned}$$

Non è vero che si trovano sempre primi. Per esempio per $p = 23$ non si ottiene un numero primo.

Mersenne disse che M_p era primo per una serie di numeri p. Si sono trovati 5 errori. Per $p = 61, 67, 89, 107, ?$ M_p non è primo.

E' pur vero che tutti i primi più grandi che si sono trovati sono della forma di Mersenne. Per $p = 44497$ si ottiene un M_p primo $2^{44497} - 1$. Da quante cifre è fatto M_{44497}? Un conto grossolano: $2^{44497} = (2^{10})^{4497} > (10^3)^{4497} = 10^{13491}$ quindi M_{44497} ha almeno 13491 cifre! Ad oggi si sono scoperti numeri p a 8 cifre che danno M_p primo.

Esistono comunque dei criteri per capire se M_p è primo. Per esempio, se $(2p + 1)$ è primo esso stesso allora M_p non è primo ma è divisibile per $2p + 1$.

Ma c'è un'espressione che dà sempre numeri primi? Dove finiscono i primi? Nella classe $4h + 3$ o nella classe $4h + 1$? In realtà i primi si equi-dividono; cioé le due classi hanno infiniti numeri primi. Esistono infiniti primi della forma $4h + 1$ e della forma $4h + 3$. I numeri di Mersenne sono del tipo $4h + 3$. Che i primi della forma $4h + 3$ sono infiniti è facile da dimostrare.

Per quanto riguarda i primi che appartengono alla classe $4h + 1$ si può dire che essi si possono scrivere come somme di due quadrati:

$$\begin{aligned}
5 &= 2 \cdot 2 + 1 = 2^2 + 1^2\\
41 &= 2 \cdot 20 + 1 = 5^2 + 4^2
\end{aligned}$$

Mentre nessun numero del tipo $4h + 3$ si può scrivere come somma di due quadrati.

Se i quadrati da sommare sono più di due si può fare di meglio. Per esempio vale il teorema di Lagrange, che venne dopo Eulero:

Teorema 4 *(di Lagrange): Ogni intero si può scrivere come somma di 4 quadrati.*

Proviamo:

$5 = 2^2 + 1^2 + 0^2 + 0^2$ (ho usato solo 2 numeri)
$7 = 2^2 + 1^2 + 1^2 + 1^2$ (qui ne ho usati 4, di meglio non si può fare)
$11 = 3^2 + 1^2 + 1^2 + 0^2$ (qui ne ho usati 3)

Vale anche il teorema di Dirichlet che è un teorema dell'800:

Teorema 5 *(di Dirichlet): Per infiniti n se $MCD(a, b) = 1$ allora $a \cdot n + b$ è primo.*

Se infatti costruiamo la progressione $a \cdot n + b$ con a e b primi tra loro allora si "acchiappano" infiniti primi.

2.3 Terza lezione

Ho sempre parlato di numeri primi o irriducibili. I due termini fanno riferimento a concetti differenti. Cosa vuol dire che p è irriducibile? Che p è divisibile solo per 1 e per se stesso (si tratta dei mattoni dell'aritmetica).

Cosa vuol dire che p è primo? La definizione corretta è la seguente:

Definizione 5 *: p primo significa che se $p \mid n \cdot m$ allora $p \mid n$ o $p \mid m$.*

Facciamo qualche esempio:

$3 \mid 6 \cdot 2 \implies 3 \nmid 2$ ma $3 \mid 6$
$3 \mid 4 \cdot 3 \implies 3 \nmid 4$ ma $3 \mid 3$

La proprietà non vale per 4:
$4 \mid 6 \cdot 2$ *ma* $4 \nmid 6$ e $4 \nmid 2$ (cioé divide il prodotto senza dividere i due fattori, quindi non è primo; si può dire che il numero 4 si "spezza", cioé un pò "entra" nel 6 e un pò nel 2).

Si deve ad Euclide il seguente teorema:

Teorema 6 *(Secondo di Euclide): primo e irriducibile sono la stessa cosa.*

In altre strutture mentre primo$\Longrightarrow$irriducibile, non è vero il contrario.

Dimostrazione. Proviamo che un irriducibile p è un primo. Supponiamo che $p \mid n \cdot m$.

Se $p \mid n$ allora ho finito!

Se $p \nmid n$ allora devo far vedere che $p \mid m$.

Se $p \nmid n$ allora $MCD(p, n) = 1$.

Piccola finestra. Ricordiamo che se $MCD(a, b) = 1$ allora $\exists x, y \in \mathbb{Z} t.c. ax + by = 1$.

Riprendiamo: se $MCD(p, n) = 1 \Longrightarrow$

$$\exists x, y \in \mathbb{Z} t.c. px + ny = 1. \tag{2}$$

Ora ci vuole l'intuizione geniale! Uno deve avere un'idea altrimenti non va avanti.

Osserviamo che per ipotesi $p \mid n \cdot m$. Se moltiplicassi tutto per m cosa accade alla 2?

$$m \cdot px + m \cdot ny = m$$

Cosa osserviamo:

$$\underbrace{m \cdot p \cdot x}_{\substack{p \text{ divide questo numero perché} \\ \text{compare esplicitamente}}} \qquad + \qquad \underbrace{m \cdot n \cdot y}_{\text{qui dentro c'è } p} \qquad = m$$

Segue che $p \mid (m \cdot px + m \cdot ny)$ cioé $p \mid m$. .

Un'altra stranezza dei numeri primi è la loro distribuzione: sono molto irregolari. Si parla di irregolarità di rarefazione.

Iniziamo con i primi gemelli. 11 e 13 sono primi gemelli perché distano di 2. Chiaramente tre dispari di fila non ci possono essere perché uno sarebbe multiplo di 3 e quindi non primo. Si potrebbero esaminare le terne del tipo 17, 19, 23.

Stiamo entrando in un campo pieno di congetture.

Congettura 3 : *I primi gemelli sono inifiniti.*

In altri termini: esistono infiniti p primi tali che $p + 2$ è ancora primo.

Non si, ad oggi, ancora nulla sulla verità di questa affermazione. Chen, nel 1973, è arrivato al risultato che $p + 2$ o è primo o è il prodotto di 2 primi. Si parla, in questi casi, di quasi-primi. Il teorema suona così:

Teorema 7 : *Esistono infiniti p primi tali che $p + 2$ è un quasi-2primo: $p + 2 = p_1^{a_1} \cdot p_2^{a_2}$ con $a_1 + a_2 \leq 2$, con p_1 e p_2 primi.*

o in altri termini:

$p + 2 = p'$ o $p + 2 = \left(p'\right)^2$ o $p + 2 = p' \cdot q'$ con p e q primi.

L'altra stranezza è che si possono trovare intervalli $[n, n + k]$ senza primi. All'interno dei numeri reali si posso quindi trovare intervalli privi di primi e primi molto vicini!

Un'altra congettura è la seguente:

Congettura 4 *: Esistono infiniti primi della forma* $p = n^2 + 1$

Più in generale:

Congettura 5 *: Esistono infiniti primi della forma* $p = an^2 + bn + c$ *con* $a, b, c \in \mathbb{N}$ *con le condizioni:*

$$\begin{cases} MCD(a,b,c) = 1 \\ (a+b) \;\; e \; c \; non \; entrambi \; pari \\ \Delta = b^2 - 4ac < 0 \end{cases}$$

Nel 1740 Goldbach scrive ad Eulero che:

Congettura 6 *(di Goldbach):*

(1) ogni intero pari maggiore o uguale di 4 è somma di due primi (e questa affermazione, fino ad oggi sembra vera, almeno fin dove siamo riusciti a fare i conti)

(2) ogni ntero dispari maggiore o uguale a 7 è somma di tre primi.

Nel 1930 la congettura è stata quasi risolta da Vinogradov che ha domostrato il teorema:

Teorema 8 *: Ogni intero dispari, da un certo punto in poi, è somma di 3 primi.*

Cioé esiste un $n_0 \in \mathbb{N}$ a parti dal quale la relazione è vera. Purtroppo n_0 è troppo grande, è così grande che c'è un buco di numeri non verificabile con il calcolatore.

Notiamo che (1) $\Longrightarrow$ (2) mentre (2) $\not\Rightarrow$ (1).

Nel 1973 Chen dimostra che esistono infiniti pari $n = 2k$ tali che $m = p + n$ è quasi 2 primo.

Passiamo alle terne pitagoriche. Si tratta di terne (n, m, k) che verificano la relazione $n^2 + m^2 = k^2$.

Le terne pitagoriche si conoscono tutte e sono della forma:

$$\begin{cases} n = l^2 - h^2 \\ m = 2lh \\ k = l^2 + h^2 \end{cases}$$

Esiste una congettura (sebbene Fermat diceva di averlo dimostrato) che è passato alla storia come ultimo teorema di Fermat

Teorema 9 *: Terne pitagoriche con esponente maggiore di 2 non esistono; ovvero* $x^k + y^k = z^k$ *con* $x, y, z \in \mathbb{N}$ *non ha soluzioni per* $k \geq 3$.

Eulero lo provò per $k = 3$.

Bisogna aspettare Wiles per la dimostrazione. La prima è del 1993 e conteneva un errore corretto nel 1995. Wiles provò che la congettura è vera. Si trattava di provarla per $k = 4$ e per k primo.

Per finire, è stato dimostrato che:

Teorema 10 *(di Tao –Green): Per ogni n esiste una progressione aritmetica di n numeri primi*

Per esempio:
per $n = 3$ esiste la progressione $3, 5, 7$ con $d = 2$;
per $n = 4$ esiste la progressione $11, 17, 23, 29$ con $d = 6$.

3 La nostra attività

Con il prof. Puglisi ci siamo intrattenuti sia all'inizio che alla fine delle sue lezioni; egli ci ha invitato a porre, nelle ultime due ore di ogni lezione, alcune problematiche interessanti agli studenti che qui riportiamo. All'inizio del tirocinio non ci aspettavamo una richiesta del genere da parte del professore; pensavamo infatti che il nostro ruolo fosse di *osservatori* e di aiuto agli studenti nello svolgere attività proposte dal professore stesso; questi, invece, si è occupato solo della parte teorica, lasciando al suo collaboratore - non certo brillante come il professore - l'approfondimento di alcune questioni teoriche e la risoluzione di alcuni esercizi; a noi veniva affidato il compito di "stimolare" gli studenti e, nello stesso tempo, di coinvolgerci con loro. L'organizzazione in tarda serata e un certo grado di improvvisazione, sebbene abbiano prodotto un effetto positivo sugli studenti, sono sicuramente elementi da evitare in una futura organizzazione del laboratorio.

Riportiamo le attività svolte con gli studenti e alcuni commenti e osservazioni che le attività stesse ci hanno suggerito.

3.1 Le definizioni e prime dimostrazioni

Esercizio 11 *Dare una definizione di multiplo.*

Lo scopo di questo esercizio era di renderci conto della capacità degli studenti di formalizzare concetti. Con il professore i ragazzi erano stati introdotti al concetto di divisibilità, formalizzato con il simbolo $|$. Qui si chiedeva loro di inventare un simbolo per il termine *multiplo* e di esprimere tramite lettere la proprietà. Non è stato immediato per loro inventare un simbolo! Abbiamo quindi suggerito per *multiplo* il simbolo $\sqcup$. Cosa vuol dire allora che $a \sqcup b$? La risposta non è tardata: $a \sqcup b$ se $\exists c \in \mathbb{N}$ t.c. $a = c \cdot b$.

Esercizio 12 *Dare la definizione di numero pari e di numero dispari.*

In questo esercizio non ci sono stati problemi: i ragazzi hanno formalizzato subito e bene la definzione.

A partire da queste definizioni abbiamo posto i seguenti problemi:

Esercizio 13 *E' noto che $(n^2 + 4n + 1)$ è dispari. Cosa sai dire su n?*

Esercizio 14 *E' noto che $(n^3 + 10n + 1)$ è pari. Cosa sai dire su n?*

Con questi esercizi abbiamo cercato di stimolare in loro il gusto per la dimostrazione a partire da definizioni ben poste.

Una volta posto il problema alla lavagna abbiamo lasciato sufficiente tempo per la risoluzione. I ragazzi hanno lavorato in gruppi da 2 a 4 persone. Noi ci siamo resi disponibili: alcuni gruppi hanno avuto bisogno di qualche suggerimento e chiarimenti mentre altri hanno affrontato con successo e brillantemente i problemi, stupendoci per la precisione e il senso estetico che hanno dimostrato. Quando la maggior parte dei gruppi aveva finito l'attività, si chiamava qualcuno alla lavagna a scrivere e a discutere la dimostrazione.

Riportiamo le soluzioni degli studenti.

Nel primo esercizio è evidente che se (n^2+4n+1) è dispari allora $m = (n^2+4n)$ è pari; inoltre $m = n(n+4)$ quindi se n fosse dispari il numero m risulterebbe prodotto di due dispari e quindi a sua volta dispari (abbiamo chiesto il perché di questa proprietà[2]) contrariamente al fatto che m è pari; segue che n deve essere pari.

Nel secondo esercizio si può procede in modo analogo ma questa volta si deve ragionare su $m = n \cdot (n^2 + 10)$. Qualcuno ha osservato che il numero dispari $m = n^3 + 10n$ è la somma di n^3 con $10n$ (che è un numero sicuramente pari); segue che n^3 deve essere dispari e quindi n dispari.

Abbiano notato un grosso interesse verso questi esercizi per cui nella lezione successiva ne abbiamo posti alcuni dello stesso tipo:

Esercizio 15 *Provare che* $\forall n$, $(n^3 - n)$ *è divisibile per 6.*

Esercizio 16 *Se* a *non è divisibile nè per 2 e nè per 3 allora* $(a^2 - 1)$ *è divisibile per 24.*

Questi esercizi sono stati presi dal libro del Prodi "Matematica come scoperta" per il biennio delle scuole medie superiori. La conoscenza dei prodotti notevoli e della fattorizzazione dei polinomi consente di risolvere agevolmente questi esercizi.

Come già detto i ragazzi hanno risposto con molto interesse alle proposte. Abbiamo notato una certa abitudine alla formalizzazione, ma abbiamo osservato una genarale tendenza a non porsi il problema iniziale di base: "*Ma quello che mi stanno dicendo è vero? Proviamo a vedere qualche caso particolare*". Nessuno

[2] Un ragazzo, di fronte al prodotto di due numeri dispari, ha scritto:

$$\begin{aligned}(2k_1+1)\cdot(2k_2+1) &= 4k_1k_2 + 2(k_1+k_2) + 1\\ &= 2(2k_1k_2 + k_1 + k_2) + 1\\ &= 2k_3 + 1\end{aligned}$$

il tutto per dimostrare che il risultato è dispari. Eccesso di formalismo? Alcune volte conviene lasciare spazio all'intuizione; il formalismo rischia di bloccare la fantasia e un ragazzo finisce per sentrirsi "imbrigliato" da una serie di regole rigide, col risultato finale di allontanarsi dalla disciplina studiata. La formalizzazione è una conquista che è bene raggiungere a piccoli passi, altrimenti c'è il rischio anche di perdere il "gusto" di fare matematica.

faceva prove iniziali; ad esempio, nell'esercizio nessuno si è messo a sostituire qualche numero al posto della variabile n. I ragazzi si sono messi subito a cercare la dimostrazione, forse anche spinti dalla rivalità con altri loro coetanei provenienti da altre scuole. D'altra parte abbiamo osservato la tendenza a non disegnare niente, ma a ragionare solo formalmente (questo ci ha un po' sorpresi). Ad esempio nel caso $n^3 - n$, era da aspettarsi un disegno dei numeri su una retta. Una ragazza, invece, aveva fatto un'ellisse che racchiudeva i tre numeri e ha detto che *"comunque li pesco sicuramente ho un multiplo di 3, quindi presi tre numeri consecutivi a caso uno dei tre è sicuramente multiplo di 3"*; senza ricorrere a tecnicismi era riuscita a intuire una proprietà che pur aveva avuto modo di conoscere con il crivello di Eratostene. Uno di noi ha spinto la ragazza a generalizzare la proposizione a n numeri consecutivi, notando con piacere che anche gli altri studenti si trovavano meglio con questa impostazione.

A questo punto è doverosa una osservazione. Ogni insegnante ha il proprio modo di vedere le cose: c'è chi è più "visualizzatore" di altri! Non coinvolgendosi con gli studenti si rischia però di imporre una propria visione penalizzando gli studenti che invece sono facilitati da altri modi di vedere o ragionare. L'insegnante dovrebbe quindi oscillare tra le diverse impostazioni, in modo tale da non perdere parte della classe; ad esempio, se si pone troppa importanza su problemi che si risolvono agevolmente con la geometria, quei ragazzi che hanno difficoltà nella visualizzazione potrebbero capire che la matematica non è una disciplina a loro congeniale. Viceversa, se un insegnante pone troppa enfasi su dimostrazioni algebriche formali, rischia di perdere coloro che, seppur intuitivi e dotati per la disciplina, non riescono ad appassionarsi a causa della pedanteria eccessiva che contrasta con la creatività, indispensabile in questi campi.

Un altro punto interessante: i ragazzi dovrebbero essere abituati a porsi domande, e non limitarsi a risolvere le questioni che sono loro proposte.

Infine abbiamo proposto un problema *pratico*:

Esercizio 17 *Si ha a disposizione un foglio di carta quadrettata. Si vuole ricavare una cornice di forma rettangolare e dello spessore di un solo quadratino. Si vuole però che i quadratini della cornice siano tanti quanti i quadratini interni. E' possibile? Quante soluzioni sono possibili?*

L'esercizio è interessante perché chiede allo studente di modellare una situazione reale piuttosto che andare per tentativi. Qualche gruppo ha provato a fare alcuni disegni sul foglio quadrettato per trovare l'"ispirazione". I gruppi dei più "bravi" hanno iniziato ad usare diverse lettere e a scrivere equazioni: il desiderio di giungere per primi al risultato - così ci è sembrato - si è scontrato con qualche errore algebrico che conduceva a soluzioni non intere del problema. Interessante è stato il caso di un ragazzo - con evidenti capacità - che dopo aver trovato la soluzione e dopo il commento di uno di noi "non si può fare di meglio?" è ritornato sulla propria dimostrazione modificandola in modo da renderla esteticamente migliore: ha cambiato variabili riducendo la trattazione algebrica a poche righe.

A questi esercizi iniziali abbiamo aggiunto il seguente.

Esercizio 18 *Calcola il massimo comun divisore fra* 589 *e* 399 *sia utilizzando la fattorizzazione sia utilizzando l'algoritmo di Euclide.*

Lo scopo dell'esercizio era quello di evidenziare la potenza dell'algoritmo euclideo in contrapposizione al crivello di Eratostene e richiamare in qualche modo i criteri di divisibilità nonché problematiche riguardo alla computabilità di un algoritmo .Si è fatto cenno anche agli algoritmi non deterministici e ai test di primalità.

Esercizio 19 *Dimostrare che la frazione* $\frac{26n+11}{39n+10}$ *è irriducibile per ogni valore di* n.

E' possibile una generalizzazione del problema (cioè individuare il tipo di relazione che deve intercorrere in una frazione del tipo $\frac{an+b}{cn+d}$ fra a, b, c e d affinché la frazione sia irriducibile).

L'esercizio coinvolgeva le equazioni diofantee e la scomposizione in fattori primi.

3.2 Criteri di divisibilità.

E' stato dimostrato il criterio di divisibilità per 3 senza fare ricorso alle congruenze; è nostra convinzione, infatti, appoggiarsi a strumenti matematici sofisticati per affrontare problemi matematici solo in caso di assoluta necessità oppure come esempio di utilizzo degli stessi.

Un numero intero può essere scritto nella forma[3]:

$$x = a_n a_{n-1} a_{n-2} \dots a_1 a_0 = a_0 + a_1\,10 + a_2\,100 + \cdots + a_{n-1}\,10^{n-1} + a_n\,10^n \quad (3)$$

Abbiamo fatto subito notare che

$$10 = 3k_1 + 1 \;\; ; \;\; 100 = 3k_2 + 1 \;\; ; \;\; 1000 = 3k_2 + 1 \;\; ; \;\; \dots \quad (4)$$

e quindi che $10^z = 3k_z + 1$. Questo ci consente di scrivere la (3) nella seguente maniera:

$$x = a_0 + a_1 \cdot (3k_1 + 1) + a_2 \cdot (3k_2 + 1) + \cdots + a_n \cdot (3k_n + 1); \quad (5)$$

le quantità tra parentesi sono simili all'espressione dei numeri dispari $(2k + 1)$; l'analogia sta nel fatto che è possibile trovare valori k che rendono vera l'uguaglianza, ma non ci dobbiamo preoccupare della loro determinazione. La (5) è

[3]Talvolta si possono commettere errori nella (3) in quanto da un lato a_0 è l'ultima cifra, dall'altro è la prima ad apparire; è possibile scrivere anche

$$x = a_n a_{n-1} a_{n-2} \dots a_1 a_0 = a_n\,10^n + a_{n-1}\,10^{n-1} + \cdots + a_1\,10 + a_0$$

ma è forse consigliabile abituare gli studenti a ragionare prima di scrivere una formula, puntando così più sull'elasticità e meno sulla memorizzazione, inutile e fine a se stessa equivalente a:

$$x = a_0 + a_1 + a_2 + \cdots + a_n + 3 \cdot k \tag{6}$$

dove k è un opportuno numero; dunque è possibile analizzare la divisibilità di

$$a_0 + a_1 + a_2 + \cdots + a_n$$

anziché di x.

Il criterio di divisibilità per 9 è identico al precedente, in quanto cambiano soltanto i valori numerici k_j, ed è perciò possibile anche in questo caso utilizzare direttamente la (5).

Sarebbe stato molto interessante far vedere altri criteri di divisibilità, e soprattutto come generarli; è curioso trovare dei numeri che ammettono criteri molto semplici, come ad esempio 37, per il quale vale:

$$10^2 = -11 + 37 \cdot 3; \quad 10^3 = 1 + 37 \cdot 27\,;$$

per stabilire se un numero è divisibile per 37 basta quindi verificarlo per:

$$a_0 + 10a_1 - 11a_2 + a_3 + 10a_4 - 11a_5 + \ldots$$

Questo dovrebbe lasciare di stucco gli studenti, e forse potrebbe spingerli a cercare nuove relazioni di questo tipo.

Una proposta didattica interessante in questa direzione potrebbe essere questa: dividere la classe in piccoli gruppi e far trovare loro dei criteri di divisibilità con numeri non troppo elevati. Alcune prove dovrebbero convincere i ragazzi del fatto che è difficile trovare numeri con criteri pratici (come 3 e 9), ma è bene chiarire che, anche se il discorso il più delle volte ha carattere puramente teorico, ogni numero ha il "suo personale" criterio di divisibilità. In questo modo viene "svelato" il mistero che circonda i (pochi) criteri di divisibilità conosciuti dagli studenti.

Questi esercizi hanno, in più, il pregio di sviluppare abilità di calcolo sulle congruenze (le potenze di 10 modulo il numero considerato di volta in volta); in questo modo i ragazzi hanno l'opportunità di vedere un'altra applicazione concreta di questi (del tutto nuovi per alcuni di loro) strumenti algebrici.

3.3 Formule generatrici!

Abbiamo anche lanciato una sfida riguardante le formule che *generano* i numeri primi. E' stato interessante presentare ai ragazzi la seguente formula:

$$p(n) = n^2 - n + 41 \tag{7}$$

dicendo loro che se al posto della variabile n si sostituiscono valori interi positivi si ottengono numeri primi! Chiaramente la formula genera numeri primi fino a $n = 40$, in quanto $p(41) = 41^2$, ma questo era lasciato come scoperta ai ragazzi.

Anche l'espressione

$$q(n) = n^2 - 79n + 1601 \tag{8}$$

fornisce numeri primi fino a $n = 79$: $q(80) = 41^2$.

La relazione tra le due espressioni (7) e (8) è la seguente:

$$p(40 - n) = q(n) \tag{9}$$

cioè

$$(40 - n)^2 - (40 - n) + 41 = n^2 - 79n + 1601\,.$$

La cosa difficile da capire, forse, è il fatto che la ricerca di formule semplici che forniscano soltanto numeri primi è stata una fatica inutile.

Per mancanza di tempo non abbiamo potuto fare questa osservazione: dati n numeri primi (consecutivi oppure no), è possibile trovare un polinomio $f(x)$ di grado $n - 1$ a coefficienti razionali tale che:

$$f(1) = p_1 \quad ; \quad f(2) = p_2 \quad ; \quad \ldots \quad ; \quad f(n) = p_n$$

in ogni caso non possiamo trovare un'espressione che fornisca *tutti* i numeri primi. Visto che i ragazzi studiano l'interpolazione polinomiale, quest'ultimo esercizio, può essere interessante.

3.4 Numeri primi consecutivi

Un esercizio interessante che abbiamo scelto di presentare agli studenti è stato il seguente:

Esercizio 20 *Dato n, trovare n numeri consecutivi non primi.*

Abbiamo notato che i ragazzi non sono abituati a riflettere bene sulle definizioni, o sui testi in generale. All'inizio non sono rimasti colpiti dall'affermazione (forse erano stanchi dopo tre giorni di Settimana Matematica); uno di noi ha dovuto esibire alcuni esempi che illustrassero la difficoltà insita in quell'affermazione. Non è stato facile inoltre far capire l'importanza di quel "dato n"; un'analogia con l'analisi matematica è risultata utile (molti ragazzi sono nella classe quinta e hanno studiato la definizione di continuità o di limite di una successione): la frase "per ogni ϵ esiste δ etc" può essere letta ed interpretata anche in termini di "scommessa" tra due giocatori, uno dei quali sfida l'altro a trovare un valore di δ che abbia determinate caratteristiche in funzione di ϵ. Allo stesso modo, nel nostro caso, l'obiettivo è quello di far vedere che, se veniamo "sfidati" da un'altra persona a trovare n numeri consecutivi non primi, noi siamo in grado di trovare questi numeri.

Un'altra cosa difficile da capire è che non possiamo essere certi che questi numeri che troviamo sono quelli più piccoli con quelle caratteristiche; potrebbero essercene tante altre (sempre però in numero finito) prima della nostra serie di numeri.

L'enunciato è stata quindi la cosa più difficile da chiarire e sinceramente non sappiamo quanti ne abbiano davvero capito fino in fondo il valore e la complessità.

Non abbiamo fatto cimentare i ragazzi con l'esercizio ma abbiamo fornito la dimostrazione partendo da un esempio numerico. Considerando $n = 100$ vogliamo determinare 100 numeri consecutivi che sono sicuramente non primi. L'idea è quella di usare il fattoriale. Il numero 100! è infatti pari a:

$$100! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot 100$$

quindi $100! + 2$ si può scrivere come:

$$\begin{aligned} 100! + 2 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot 100 + 2 \\ &= 2 \cdot (1 \cdot 3 \cdot 4 \cdot \cdots \cdot 100 + 1) \end{aligned}$$

e quindi non è primo perché divisibile per 2. Analogamente per $100! + 3$:

$$\begin{aligned} 100! + 3 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot 100 + 3 \\ &= 3 \cdot (1 \cdot 2 \cdot 4 \cdot \cdots \cdot 100 + 1) \end{aligned}$$

che è multiplo di 3.

I numeri:

$$n! + 2; \quad n! + 3; \quad n! + 4 \quad \ldots \quad n! + n$$

non sono quindi primi. Non possiamo sapere, in generale, se $(n!+1)$ e/o $(n!+n+1)$ sono numeri primi, ma sicuramente i numeri appena scritti non lo sono.

Anche qui abbiamo notato nei ragazzi l'abitudine a voler concludere subito, animati da una fretta a volte francamente eccessiva. Prevale l'*eseguire* sul *riflettere* e sul *capire*: gli studenti non hanno molta voglia di "subire" commenti ad un teorema, loro lo applicano punto e basta. Spesso passa per bravo lo studente che sa applicare correttamente un teorema o una formula, anche se poi, indagando più a fondo, scopriamo che spesso non ha capito cosa sta in effetti facendo. Da questo punto di vista, dovremmo fornire in classe le risposte a domande del tipo: "*Perché si studia questo teorema?*", "*In quali situazioni serve davvero? Quando se ne può fare a meno?*"

3.5 Problemi interessanti non proposti

La mancanza di tempo non ci ha consentito di organizzare un percorso sulle equazioni diofantee. Qui proponiamo alcuni suggerimenti.

3.5.1 Equazioni diofantee.

Un problema che sarebbe stato adatto per questi tre giorni è il seguente:

Esercizio 21 *Al cinema XYZ gli uomini entrano pagando* 8 *euro, le donne con* 4 *euro. Sapendo che l'incasso è stato di* 130 *euro, quanti uomini e quante donne sono entrate?*

Sarebbe stato interessante analizzare le varie impostazioni risolutive del problema; con questo quesito pratico è possibile verificare se gli studenti hanno compreso l'importanza delle equazioni diofantee nella vita quotidiana e se hanno capito che, affinché l'equazione abbia soluzione, il MCD tra i due numeri deve essere un divisore del termine noto.

Interpretazione geometrica delle equazioni diofantee: possiamo interpretare un'equazione diofantea del tipo

$$ax + by = c \tag{10}$$

in questi termini geometrici: considerata nel piano cartesiano la retta che ammette equazione 10, dobbiamo trovarne i punti a coordinate intere. E' molto illuminante far vedere che l'algebra fornisce facilmente un criterio per stabilire se una retta contiene oppure no punti a coordinate intere; per esempio la retta

$$4\,x - 6\,y = 8$$

ammette infiniti punti a coordinate intere, mentre la retta

$$4\,x - 6\,y = 7$$

non ne contiene nessuno. E' importante far riflettere sul fatto che, se una retta contiene un punto con tale proprietà, allora ne esistono infiniti. Questo collegamento tra algebra e geometria non va assolutamente trascurato, in quanto i ragazzi devono abituarsi a vedere i vari argomenti matematici da più punti di vista, scoprendo le relazioni che vi intercorrono. Alla luce di quanto detto, l'esercizio 21 può essere quindi interpretato nel modo seguente:

trovare i numeri interi positivi x e y che rendono vera l'equazione:

$$8\,x + 4\,y = 130 \tag{11}$$

L'algebra ha metodi molto semplici ma allo stesso tempo molto efficaci in quanto è sufficiente verificare che 4 (=MCD(8,4)) non divide 130 per poter affermare con certezza che la retta (11) non contiene punti a coordinate cartesiane intere.

Possiamo modificare l'esercizio precedente nel seguente modo:

Esercizio 22 *Al cinema XYZ gli uomini entrano pagando 8 euro, le donne con 4 euro e i bambini 2 euro. Sapendo che in tutto le persone sono 26 e che l'incasso è stato di 144 euro, quanti uomini, quante donne e quanti bambini sono entrati?*

Per risolvere questo esercizio è necessario saper calcolare il MCD di tre numeri; è allora opportuno far vedere come l'algoritmo euclideo si presta bene anche in questi casi.

Anche l'esercizio 22 ammette un'interpretazione geometrica, non nell'ordinario piano cartesiano bensì nello spazio tridimensionale. Il problema è equivalente, infatti, al seguente: trovare i punti con coordinate intere positive (≥ 0) in $\mathbb{R}^3$

appartenenti alla retta di equazione

$$\begin{cases} x + y + z = 26 \\ 8\,x + 4\,y + 2\,z = 144 \end{cases}$$

Da far osservare che il metodo risolutivo per le equazioni diofantee fornisce tutte le soluzioni intere, e se vogliamo applicarlo in situazioni reali dobbiamo assicurarci che le soluzioni trovate abbiano senso (in questo caso le tre coordinate devono essere positive).

Il prossimo esempio illustra una situazione in cui molti studenti potrebbero essere in difficoltà.

Esercizio 23 *Tizio compra quaderni a* 3 *euro l'uno, mentre Caio compra quaderni a* 6 *euro l'uno. Sapendo che in totale hanno speso* 22 *euro, quanti quaderni ha comprato ciascuno di essi?*

Il metodo risolutivo fornisce le soluzioni

$$x = -39 + 11k \ \ ; \ \ y = 26 - 7\,k \quad \text{con } k \text{ intero} \tag{12}$$

Un rapido sguardo al grafico delle due rette mostra che non ci sono valori interi di k per cui x e y sono entrambi positivi. Il problema 23 non ha quindi soluzione. Il vincolo intero e positivo è molto "forte", nel senso che è una "pretesa" di non poco conto. La retta $3\,x + 6\,y = 22$ giace quasi interamente nel secondo e nel quarto quadrante; ha, quindi, una bassa probabilità di avere punti a coordinate intere. Le soluzioni intere (12) sono dunque tutte nel secondo e quarto quadrante: queste non hanno senso (il numero di quaderni è positivo). L'esempio 23, se affrontato senza il vincolo intero positivo, ma solo con il vincolo intero, ammette infinite soluzioni: la questione è molto delicata e gli studenti si possono sentire disorientati da questa nuova impostazione.

Nella scuola superiore non si trovano o non viene dato il giusto spazio a problemi con soluzione vincolata; gli studenti sono addestrati ad impostare il sistema e talvolta capita di trovare soluzioni del tipo "1,4 tavoli" oppure "5,7 sedie"! Anche in fisica può capitare di trovare soluzioni prive di senso: il mancato controllo dei risultati da parte dei ragazzi è un segnale molto negativo.

4 Sviluppi

Questa sezione è stata curata da Ester Balducci.

L'esperienza del tirocinio ha certamente mostrato che questo argomento presenta un estremo fascino e che attraverso di esso si possono fare interessanti percorsi didattici. I numeri sono il nostro mondo. Abbiamo a che fare con loro sempre. Con essi contiamo, misuriamo, li digitiamo ogni giorno su tastiere di tutti i generi. Con essi possiamo giocare, sono una fonte inesauribile di divertimento.

Ho dunque cercato di vedere quali possibili sviluppi possano derivare dalla trattazione dei numeri primi e dei numeri in generale e, fra i vari percorsi presenti nella letteratura di divulgazione, ho trovato diverse proposte, alcune già da me direttamente sperimentate sia nella scuola primaria che secondaria. Sono elencati alcuni percorsi che richiedono un coinvolgimento interdisciplinare. Sono percorsi di solito più difficili da realizzare. Quando però ci sono riuscita, questa a attività mi è sempre risultata un momento di grande arricchimento. I percorsi qua sotto elencati non pretendono di essere originali. Ho solo esposto le idee di base che li guidano e naturalmente è stato mio compito dare il taglio opportuno a seconda della classe con cui ho avuto a che fare.

Percorso 1 Divisioni, multipli, divisori e numeri primi.

Primi algoritmi per riconoscere se un numero è primo, Criteri di divisibilità. Crivello di Eratostene. Il computer ci può aiutare ? Come e fino a che punto? Difficoltà di testare numeri grandi. Algoritmi non deterministici. Test di primalità.

Percorso 2.L'algoritmo di Euclide per il M.C:D. di due numeri.

Definizione di numeri primi fra loro. Interpretazione geometrica della nozione di numeri primi fra loro. (un numero n è primo con un numero m di esso minore se il poligono stellato ad n vertici congiunti di m in m è tracciato senza soluzione di continuità). Aritmetica modulare. Criteri di divisibilità. La funzione di Eulero, il periodo delle frazioni.

Percorso 3. Comunicare con le altre civiltà..I messaggi di Arecibo.

Nel 1961 Bernard Oliver, studioso della teoria dell'informazione, presentò all'istituto degli ingegneri delle telecomunicazioni un messaggio di sua creazione, che mostrava quel che poteva essere un segnale extraterrestre. Si trattava di una sequenza di 1271 bit. Quando la disponiamo in un rettangolo 31 X 41 (41 di larghezza) si ottiene la figura 1.

Figura 1: Sequenza di 1271 bit (31×41).

Oliver riteneva che la figura fornisse un'informazione su una razza di bipedi terrestri intelligenti (in quanto consapevoli dell'esistenza di numeri primi) in un sistema biologico in cui c'era un sole,che forniva energia, acqua, con animali e stelle... naturalmente si può far dire agli studenti che tipo di informazione ricaverebbero da questa slide.

Il fatto è che poi nel 1965 tale messaggio fu sigillato in una capsula progettata per aprirsi fra 5000 anni e sotterrato nella sede dell'Esposizione Universale di New YorkTuttavia nel 1974 il progetto S.E.T.I. riprese questa idea, e costruì un messaggio lungo 1679 bit tramutabili in un rettangolo 73x23 (con 23 base del rettangolo) riportato in figura 2.

Figura 2: Sequenza di 1679 bit (72 × 23).

Esso in questo caso fornisce informazioni, che naturalmente è bene far ricavare ai ragazzi,ma che sostanzialmente sono le seguenti:Inizialmente elenca i numeri da 1 a 10 in notazione binaria per far capire al ricevente del sistema di numerazione impiegato., si fornisce poi il numero atomico degli elementi su cui si fonda la chimica della vita (in arancione) si leggono da destra a sinistra idrogeno, carbonio, azoto, ossigeno e fosforo. Rispettando tale ordine il messaggio indica il numero di questi atomi in tutte le molecole costitutive del DNA (in malva) Si riconoscono sui lati le due catene verticali di desossiribosio fosfato che costituiscono lo scheletro della doppia elica disegnata sotto in blu, e al centro le 4 basi del DNA dell'uomo nelle coppie A.T e C-G. Il messaggio prosegue indicando il numero di coppie di basi del DNA umano e la nostra figura con statura media, il numero di esseri umani sul pianeta, poi la schematizzazione del sistema solare in cui risalta la nostra posizione, la terza dal Sole, in calce la rappresentazione del radiotelescopio con cui questa serie di bit fu spedita nello spazio.

Questo è in po' il retroscena in cui collocare questa attività che vede immediatamente un tipo di interrelazione con altre discipline come la biologia, la fisica, la chimica e l'informatica. Dal nostro punto di vista è un modo per giocare con la notazione binaria e per cominciare a far vedere come la matematica sia un linguaggio universale. Per la cronaca, il messaggio fu davvero inviato nello spazio nel 1974 mediante il radiotelescopio di Arecibo a Porto Rico. Il messaggio è stato emesso in direzione dell'ammasso globulare di M13 a 25 000 anni luce dalla Terra. Sapremo fra 50000 anni se lì esista una qualche forma di intelligenza in grado di comprendere il significato del messaggio e desiderosa di rispondere. A tal proposito potremmo avere anche una interazione con l'insegnante di Italiano. La consegna potrebbe essere quella di inventare una storia ambientata sulla Terra fra 50000 anni. Precisiamo inoltre che l'idea di un messaggio avente come lunghezza il prodotto di due numeri primi, fu testata su alcuni esseri umani, ovviamente non avvertiti del tipo di codifica. Nella maggior parte dei casi le persone decifrarono messaggi così costruiti.

Percorso 4. I numeri primi in Fisica

L'impiego dei numeri primi non è relegato ai giochi intellettuali ; li troviamo anche in alcune applicazioni di problemi di meccanica. L'antica orologeria, con i suoi ingranaggi è innanzi tutto una scienza aritmetica, elenchiamo solo alcuni risultati e da questi risulterà chiaro quali tipi di percorso ritagliare per continuare a giocare con questi numeri straordinari.

a) se due ruote, rispettivamente a m e ne denti, girano una contro l'altra,il numero di giri che deve effettuare la prima (rispettivamente la seconda) perché esse ritornino alla posizione iniziale in simultaneità è

$$\frac{m.c.m.\,(n,m)}{n} = \frac{m}{M.C.D\,(n,m)}$$

ovviamente m e n sono interscambiabili. Ad esempio due ruote, rispettivamente di 15 2 20 denti ciascuna, tornano alla posizione iniziale dopo 3 giri della seconda e 4 della prima. Se m e n sono primi fra loro, allora non appena la prima ruota, ha compiuto un numero di giri pari ai denti della seconda avremo il ritorno alla posizione iniziale. La fisica tratta di problemi di sincronizzazione ogni momento : fenomeni periodici come pendoli, satelliti, onde... l'aritmetica elementare fornisce risultati che, come negli ingranaggi, si fondano su concetti come il massimo comun divisore e il minimo comune multiplo. C'è da osservare inoltre, che i ragazzi lavorano molto di più con il minimo comune multiplo che col massimo comun divisore e allargare le loro conoscenze sull'utilizzo di tale elemento sarebbe auspicabile.

Percorso 5. Numeri Primi e Biologia.

Nella parte orientale degli Stati Uniti vivono parecchie specie di Cicale, la cui pupa resta sotto terra per 17 anni, nutrendosi della linfa contenuta nelle radici degli alberi. Negli Stati Uniti del Sud una specie ad essa affine è caratterizzata da un periodo di vita sotterraneo di 13 anni. Ogni 17 anni (ed ogni 13 al Sud) milioni di ninfe, pervenute alla maturità, escono da terra, subiscono la metamorfosi si accoppiano, depongono le uova nel terreno e muoiono tutto nel giro di una settimana. Talvolta, in una medesima zona si trovano differenti specie di periodo diverso e dopo alcuni cicli escono tutte allo stesso tempo. Perché ci sono cicale da 13 e 17 anni? 13 e 17 hanno un punto in comune. Sono numeri abbastanza elevati da superare la speranza di vita dei possibili predatori e nello stesso tempo sono entrambe numeri primi. La maggior parte dei predatori ha un ciclo vitale dai 2 ai 5 anni. E' dunque semplice osservare che quantunque possa esserci un momento in cui i loro cicli si sovrappongano cioè ad esempio che le mantidi religiose (predatori voraci di cicale con 5 anni di ciclo) escano insieme alle cicale, tale lauto banchetto potrà ripetersi fra 65 anni o fra 85.

Quindi i cicli di 13 e 17 anni forniscono alle cicale una forma di protezione, grazie alla primalità di questi numeri. Ovviamente in natura sono presenti molti esempi di questo genere. C'è un'orchidea, ormai piuttosto rara, che cresce proprio in Toscana che ha un ciclo di 23 anni prima di fiorire la prima volta. Dopo la prima fioritura, fiorisce ogni 2 anni. La condizione però per cui ciò accada, è che non venga disturbata, ribaltata in qualche modo dalla lavorazione dei terreni. Non conosco spiegazione del fatto che sia per lei favorevole il numero 23 certo è che anche questo è primo.

Percorso 6. Realizzazioni di immagini mediante i numeri primi

Non mi sono mai dedicata a questo argomento, anche se ne conosco l'esistenza perché collegato anche alla crittografia. Conto di dedicare un laboratorio negli anni futuri da presentare durane la Settimana Scientifica.

Percorso 7.I numeri primi nella storia della matematica.

L'osso di Ishango (8000 anni fa in cui sono incisi 11 13 17 19), egiziani, babilonesi, Pitagora,Platone Aristotele Euclide Eratostene, Diofanto, Bachet de Meziriac, Mersenne Fermat, Pascal, Goldbach eulero bezout, gauss Legendre, Dirichlet, Tchebichev, riemann, Lucas, Hadamard, Poussin, Hilbert

Percorso 8.La distribuzione dei primi:

Probabilità. La storia del più grande numero primo calcolato senza l'aiuto del computer (1951) da Ferrier

$$\frac{2^{148}+1}{17}$$

che non è un primo di Mersenne.

Percorso 9. Numeri primi e crittografia.

Un percorso divertente in cui possiamo introdurre le congruenze, spesso tralasciate nei programmi di algebra, in cui si può introdurre la conoscenza della Φ di Eulero, e i vari algoritmi di criptazione e decriptazione possono fornire un buon campo di esercizio di programmazione che utilizza matrici, stringhe e liste.

Percorso 10. Lo scarto fra numeri primi : le costellazioni.

Questo tipo do percorso è stato anche accennato dal prof. Puglisi nelle sue lezioni ai ragazzi del Laboratorio.

Dopo aver comunque visto che per quanto lontani sulla retta reale si possa andare, troviamo sempre due primi con lo scarto di 2 sorge ovviamente la domanda se analogamente esistono primi consecutivi con un certo scarto fra loro che siano più di due. Cioè, quali sono le sequenze possibili degli scarti ? Si può cominciare a vedere se ci sono sequenze di tre numeri primi con un dato scarto: 3,5,7 fornisce una sequenza con scarto 2. Possiamo studiare la sequenza, generalizzarla in p, p+2, p+4 e ragionare se una tale sequenza è in qualche modo ritrovabile più lontano. In realtà si dimostra abbastanza facilmente che in una sequenza del genere almeno uno dei tre è divisibile per 3, ma si scopre per contro che (p, p+2, p+6)e (p, p+4, p+6) sono forme possibili per tre numeri primi consecutivi. Le sequenze di numeri primi consecutivi che corrispondono ad una forma possibile si chiamano costellazioni di numeri primi. La forma più semplice di costellazione è quella dei primi gemelli che corrisponde alla costellazione (p, p+2).

La congettura sulle costellazioni, che anche il prof. Pugliesi ha enunciato al corso, è la seguente :*Qualunque sia la forma possibile data, esistono infinite costellazioni a essa associate.*

Percorso 11.

E' un percorso di puro gioco, un po' come gli anagrammi nella lingua italiana, le filastrocche e tutto ciò che può far giocare i ragazzi, ma nel contempo farli familiarizzare con regole e tecniche. Questo percorso riguarda **Le curiosità sui numeri primi** come i **repunit,** (ripetizioni di 1 alcuni numero primi sono così fatti 11, 1111111111111111111, 11111111111111111111111, questi sono tutti repunit), i **palindromi** (101, 131, 151 etc curiosità .....la somma di palindromi è un palindromo) i **permutabili** (79, 97, 113 311 131) i **circolari** (3779, 9773,divertente modo per introdurre anche le permutazioni) **economi e prodighi** (economi = un numero la cui fattorizzazione richieda un numero minore di cifre a quello della sua scrittura decimale 492075 $=3^9\ 5^2$ è economo, prodigo è invece 34=2 x17 ... un modo divertente per esercitare la tecnica della scomposizione in fattori)), **accorciabili a destra** 73939133 sono tutti primi fino a 7 e **accorciabili a sinistra** 357686312646216567629137 questo primo fino a 7. Il gioco può diventare più sofisticato: per esempio fare un programma che vada a scovare un numero primo con una certa caratteristica....