L'insegnamento della matematica e delle scienze integrate, 28B, 3, 251-273

Dall'Aritmetica di Peano all'Aritmetica di Robinson: numeri e polinomi per una riflessione didattica

GIORGIO T. BAGNI

DIPARTIMENTO DI MATEMATICA E INFORMATICA
UNIVERSITÀ DI UDINE

Abstract In this paper we consider Robinson's theory *Q*, the subtheory of first-order Peano Arithmetic *PA*; some well known theorems and conjectures can be interpreted over the standard model of *PA* and over one model of *Q* given by a universe of polynomials. With respect to nonconstant polynomials, some proofs by elementary methods are given.

Sommario Nel presente lavoro si considera la teoria di Robinson *Q*, sottoteoria dell'Aritmetica di Peano del primo ordine *PA*; alcuni noti teoremi e congetture possono essere interpretati nel modello standard di *PA* e in un modello di *Q* costituito da un insieme di polinomi. Alcuni risultati riferiti a polinomi non costanti sono dimostrati con metodi elementari.

Dall'Aritmetica di Peano all'Aritmetica di Robinson: numeri e polinomi per una riflessione didattica

GIORGIO T. BAGNI

DIPARTIMENTO DI MATEMATICA E INFORMATICA
UNIVERSITÀ DI UDINE

1. INTRODUZIONE

A nessun matematico e a nessun insegnante di Matematica sfugge l'importanza del ragionamento analogico: certamente esso è utilizzato, con efficacia spesso decisiva, ad esempio nella formulazione di congetture, la cui correttezza verrà successivamente esaminata per giungere a dimostrazioni complete.

Non possiamo però non rilevare alcune possibili difficoltà: ad esempio, la primaria importanza della citata fase di controllo viene talvolta sottovalutata da alcuni allievi. Dunque, dal punto di vista didattico, la ricerca (e l'esame critico) di analogie e di differenze costituisce un argomento chiaramente interessante, anche per ribadire la necessità di evitare generalizzazioni improprie[1].

Nel presente lavoro proporremo alcuni problemi considerati con riferimento all'insieme **N** dei numeri naturali e ad un insieme di polinomi[2]. Tale scelta sarà motivata da osservazioni collegate ai modelli delle teorie aritmetiche e potrà essere illustrata e discussa, se non direttamente con gli allievi, ad esempio con

[1] Indichiamo ad esempio: Markovitz, Eylon & Bruckheimer, 1986. Lo studio sperimentale di alcuni casi di generalizzazione impropria si trova in: Bagni, 2000.

[2] Alcune delle considerazioni esposte nel presente lavoro sono state oggetto di due comunicazioni dell'autore al XVII Congresso dell'Unione Matematica Italiana (Milano, 10 settembre 2003, in particolare per quanto riguarda la prima parte dell'articolo: Bagni, 2003a) e al VIII Convegno della Società Matematica Austriaca (Bolzano, 25 settembre 2003, per la seconda parte: Bagni, 2003b).

gli insegnanti in formazione. Particolare rilievo sarà dato a teoremi ed a congetture concernenti i numeri primi[3].

Ricordiamo innanzitutto alcune considerazioni collegate alle principali teorie aritmetiche[4]. *l'Aritmetica di Robinson* (introdotta da Tarski, Mostowski e Robinson nel 1953 e generalmente indicata da *Q*) è più debole *dell'Aritmetica di Peano* (*PA*, del primo ordine; si veda: Mendelson, 1972, pp. 128 e 187); *Q* può essere ottenuta da *PA* se lo schema di induzione:

$$\varphi(0)\wedge(\forall y)(\varphi(y)\rightarrow\varphi(s(y)))\rightarrow(\forall y)\varphi(y)$$

(nel linguaggio {+, ·, s, 0}, s è la funzione "successore") viene sostituito dall'assioma:

$$(\forall y)(y \neq 0\rightarrow(\exists z)(y = s(z)))$$

che è un teorema di *PA* (si prova facilmente per induzione). Com'è noto, l'induzione è uno *schema di assiomi*, dunque costituisce un assioma per ogni formula φ con una variabile libera: da ciò segue che *PA* ha infiniti assiomi, mentre *Q* ne ha un numero finito (nel 1952, Ryll-Nardzewski ha provato che la teoria *PA* del primo ordine non è finitamente assiomatizzabile, cioè non può essere formalizzata mediante alcun insieme finito di assiomi: Hájek & Pudlák, 1993, p. 2). Sia *PA* che *Q* sono teorie incomplete e nessuna loro estensione finita (ottenuta cioè per aggiunta di un numero finito di assiomi) è completa; per quanto riguarda le sottoteorie di *PA*, ricordiamo che una teoria completa è stata introdotta da Presburger nel 1929 (essa è denominata talvolta *Teoria Additiva*

---

[3] La considerazione del ruolo essenziale dei numeri primi è un argomento didatticamente molto interessante: ad esempio, esso rende possibile l'esame della notevole asimmetria tra le operazioni di addizione e di moltiplicazione. Per quanto riguarda la moltiplicazione (con elemento neutro 1) esistono infatti infiniti elementi "atomici", i numeri primi (e l'antica dimostrazione euclidea di tale infinità costituisce certamente una delle pagine più eleganti di tutta la storia della Matematica); la fattorizzazione di un numero come prodotto di elementi atomici è particolarmente interessante e costituisce una semplificazione del numero in esame. Al contrario, se consideriamo l'addizione (con elemento neutro 0), esiste uno ed un solo elemento "atomico", 1; l'espressione di un numero naturale come somma di elementi atomici è banale (1+1+…+1).

[4] In un recente lavoro (Bagni, 2002) abbiamo proposto alcuni risultati che citeremo nel presente articolo. Sottolineiamo ancora che il nostro punto di vista è essenzialmente didattico; per un approfondimento teorico delle aritmetiche deboli segnaliamo ad esempio: Macintyre, 1987 ed i riferimenti bibliografici riportati.

dei Numeri): essa è assiomatizzata nel linguaggio {+, s, 0} e lo schema di induzione è ristretto a formule scritte in tale linguaggio (Chang & Keisler, 1973, p. 43).

Possiamo così riassumere quanto sopra affermato[5]:

Teoria PA di Peano	*Teoria Q di Robinson*	*Teoria di Presburger*
incompleta	incompleta	completa
non finitamente assiomatizzabile	finitamente assiomatizzabile	non finitamente assiomatizzabile

Nel presente lavoro ci occuperemo di alcuni modelli delle teorie aritmetiche *PA* e *Q* (per un approfondimento teorico indichiamo ad esempio: Robinson, 1974 e Kaye, 1991).

L'insieme **N** dei numeri naturali con l'addizione e la moltiplicazione è il modello standard di *PA*, <**N**, +, ·, s, 0> ed è anche un modello di *Q*: l'esistenza di modelli non-standard di *PA* (cioè modelli non isomorfi a <**N**, +, ·, s, 0>) è stata dimostrata nel 1934 da Skolem. I modelli non-standard di *PA* non sono semplici da proporre ad allievi della scuola secondaria, ma può essere interessante presentare modelli di *Q* non isomorfi a **N**: ad esempio, indicheremo con $Z^*[x]$ l'insieme al quale appartengono 0 e tutti i polinomi a coefficienti interi con il coefficiente direttivo positivo (dunque anche i polinomi costanti positivi): $Z^*[x]$ con l'addizione e la moltiplicazione è un modello di *Q*, $<Z^*[x], +, \cdot, s, 0>$ (si veda: Mendelson, 1972, p. 188; Bagni, 2002).

2. UN CONFRONTO TRA $<Z^*[x], +, \cdot, s, 0>$ E <N, +, ·, s, 0>

Sottolineiamo innanzitutto che $<Z^*[x], +, \cdot, s, 0>$, modello di *Q*, non è un modello di *PA*; ad esempio, è immediato notare che:

$$(\forall y)(\exists z)(z+z = y \vee z+z = y+1)$$

dimostrabile per induzione per i numeri naturali, non vale in $Z^*[x]$ (ogni polinomio non costante di $Z^*[x]$ i cui coefficienti diversi dal termine noto non siano tutti pari può essere considerato come controesempio). Pertanto i modelli $<Z^*[x], +, \cdot, s, 0>$ e <**N**, +, ·, s, 0> non sono elementarmente equivalenti.

---

[5] Il ruolo dello schema di induzione e l'incompletezza in *PA* e nelle sottoteorie costituiscono un importante settore della ricerca contemporanea (si veda ad esempio: Hájek & Pudlák, 1993, dove sono studiati alcuni importanti "frammenti" di *PA* ottenuti restringendo lo schema di induzione a classi particolari di formule.

Troveremo anche proposizioni vere con riferimento al modello polinomiale che risultano false per quello numerico (ciò può essere affermato anche dal punto di vista teorico: se così non fosse <**N**, +, ·, s, 0> e <$Z^*[x]$, +, ·, s, 0> sarebbero elementarmente equivalenti e non è vero: Chang & Keisler, 1973, p. 32).

3. ORDINE IN $Z^*[x]$

In base ad un assioma di Q, l'ordine si definisce in $Z^*[x]$ nel modo seguente:

$f(x) \le g(x)$ se e solo se (def.) $g(x)–f(x) \in Z^*[x]$
$f(x) < g(x)$ se e solo se (def.) $0 \ne g(x)–f(x) \in Z^*[x]$

Indichiamo alcune proprietà: siano $f(x)$, $g(x)$, $h(x)$ elementi di $Z^*[x]$:

se $f(x) \le g(x)$ allora $f(x)+h(x) \le g(x)+h(x)$
se $f(x) < g(x)$ allora $f(x)\cdot h(x) < g(x)\cdot h(x)$
se $f(x) \le g(x)$ allora $f(x)+h(x) \le g(x)+h(x)$
se $f(x) < g(x)$ allora $f(x)\cdot h(x) < g(x)\cdot h(x)$ (essendo $h(x) \ne 0$)

Siano $f(x)$, $g(x)$, $h(x)$, $h(x)–f(x)$, $h(x)–g(x)$ elementi di $Z^*[x]$:

se $f(x) \le g(x)$ allora $h(x)–g(x) \le h(x)–f(x)$
se $f(x) < g(x)$ allora $h(x)–g(x) < h(x)–f(x)$

Per quanto riguarda il minimo di $Z^*[x]$, per ogni $f(x) \in Z^*[x]$ risulta: $0 \le f(x)$.

Non sarà inutile ricordare che proprietà come queste valgono in $Z^*[x]$ in quanto sono dimostrabili in Q: la loro verifica diretta in $Z^*[x]$, sulla base delle definizioni sopra date, può però essere didatticamente utile. Inoltre si prova:

PROPOSIZIONE 1. Se $f(x)$, $g(x) \in Z^*[x]$, allora $f(x) \le g(x)$ o $g(x) \le f(x)$.

DIMOSTRAZIONE. Se $f(x) \le g(x)$ è falso, allora $g(x)–f(x) \notin Z^*[x]$, dunque il coefficiente direttivo di $g(x)–f(x)$ è negativo. Pertanto il coefficiente direttivo di $f(x)–g(x)$ è positivo e quindi $f(x)–g(x) \in Z^*[x]$ e $g(x) \le f(x)$. ■

PROPOSIZIONE 2. Se $f(x)$, $g(x) \in Z^*[x]$ e $f(x) < g(x) \le f(x)+1$, allora $g(x) = f(x)+1$.

DIMOSTRAZIONE. Dall'ipotesi segue: $f(x)+1–g(x) < f(x)+1–f(x) = 1$. Dunque $f(x)+1–g(x) = 0$ e $g(x) = f(x)+1$. ■

PROPOSIZIONE 3. Se $f(x) \in Z^*[x]$, $g(x)$ non è un elemento costante di $Z^*[x]$, $f(x) < g(x)$ e $g(x)–f(x)$ non è costante, allora per ogni n, k numeri naturali è $f(x)+n < g(x)–k$.

DIMOSTRAZIONE. Se $f(x) < g(x)$, allora $0 \neq g(x)–f(x) \in Z^*[x]$; dunque risulta: $0 \neq g(x)–f(x)–k–n \in Z^*[x]$ e dalla $0 \neq g(x)–k–[f(x)+n] \in Z^*[x]$ concludiamo: $f(x)+n < g(x)–k$. ■

Quest'ultima proprietà è degna di nota: in base ad essa possiamo considerare infinite coppie di $f, g \in Z^*[x]$ tali che $f < g$ ed infinite coppie di $n, k \in Z^*[x]$ tali che $f+n < g–k$. Si tratta evidentemente di una proprietà che vale nel modello polinomiale, ma che non vale in **N**. Abbiamo dunque trovato un'affermazione vera con riferimento al modello polinomiale ma non a quello numerico? Una difficoltà è costituita dall'espressione di tale proprietà: i quantificatori logici sono finitari, e ciò ci impedisce di usare infiniti quantificatori esistenziali nella stessa proposizione.

Sottolineiamo un aspetto didatticamente interessante: ogni $g(x) \in Z^*[x]$ non costante potrebbe essere considerato un elemento *infinito* (nel senso, intuitivo, di "preceduto da infiniti elementi"); infatti per ogni naturale n possiamo scrivere $n < g(x)$ (in base alla Proposizione 3). Quindi in $Z^*[x]$ esistono diversi elementi "infiniti" in tale senso, come x, $x+1$, x^2, x^2+1 e così via[6].

Per ogni $n \in \mathbf{N}$, $a \in \mathbf{Z}$ risulta: $n<x+a$; dunque abbiamo, in $Z^*[x]$:

$$0 < 1 < 2 < \ldots < x–2 < x–1 < x < x+1 < x+2 < \ldots$$

Se con $[x]$ indichiamo $\ldots x–1, x, x+1, x+2 \ldots$ ("copia di **Z**"), scriviamo:

$$Z^*[x] = \{\mathbf{N}, [x]\}$$

con ciò esprimendo, inoltre, che la copia di **Z** $[x]$ è "adiacente" a **N**. Infatti:

PROPOSIZIONE 4. Nessun elemento $f(x) \in Z^*[x]$ di grado 1 e coefficiente direttivo maggiore di 1, o di grado maggiore di 1, è tale che $n < f(x) < x+a$, $n \in \mathbf{N}$, $a \in \mathbf{Z}$.

DIMOSTRAZIONE. Risulterebbe $0 \neq x+a–f(x) \in Z^*[x]$ e ciò sarebbe assurdo, per la negatività del coefficiente direttivo di $x+a–f(x)$. ■

PROPOSIZIONE 5. Se il grado di $f(x) \in Z^*[x]$ è minore del grado di $g(x) \in Z^*[x]$, allora $f(x) < g(x)$.

DIMOSTRAZIONE. Dall'ipotesi: $0 \neq g(x)–f(x) \in Z^*[x]$. ■

PROPOSIZIONE 6. Se il grado di $f(x) \in Z^*[x]$ è uguale al grado di $g(x) \in Z^*[x]$ e se il coefficiente direttivo di $f(x)$ è minore i quello di $g(x)$, allora $f(x) < g(x)$.

---

[6] Un esempio come questo può forse essere utile per superare la diffusa misconcezione secondo la quale "c'è un solo infinito". Ma non approfondiamo in questa occasione tale possibilità.

DIMOSTRAZIONE. Dall'ipotesi: $0 \neq g(x)–f(x) \in Z^*[x]$. ■

PROPOSIZIONE 7. Siano $f(x)$, $g(x)$ elementi non costanti di $Z^*[x]$ aventi lo stesso grado e lo stesso coefficiente direttivo; sia n il massimo grado per il quale i coefficienti a_n di $f(x)$ e b_n di $g(x)$ non sono uguali; se $a_n < b_n$, allora $f(x) < g(x)$.

DIMOSTRAZIONE. Dall'ipotesi: $0 \neq g(x)–f(x) \in Z^*[x]$. ■

Siamo dunque in grado di scrivere $Z^*[x]$ nel modo seguente, con riferimento alle "copie (ordinate) di **Z**":

$$\begin{aligned} Z^*[x] = \{&\mathbf{N}, [x], [2x], [3x] \ldots \\ &\ldots [x^2–2x], [x^2–x], [x^2], [x^2+x], [x^2+2x] \ldots \\ &\ldots [2x^2–2x], [2x^2–x], [2x^2], [2x^2+x], [2x^2+2x] \ldots \\ &\ldots \ldots [x^3] \ldots\} \end{aligned}$$

4. ELEMENTI PRIMI DI $Z^*[x]$

Prima di considerare alcune proposizioni in **N** e in $Z^*[x]$, osserviamo che i polinomi costanti non negativi possono essere interpretati come numeri naturali (più precisamente, **N** e il sottoinsieme degli elementi costanti di $Z^*[x]$ sono legati da un isomorfismo), per cui **N** è un sottomodello di $Z^*[x]$ (Chang & Keisler, 1973, p. 21): da ciò segue che ogni proposizione con un singolo quantificatore esistenziale vera in **N** è vera anche in $Z^*[x]$, e ogni proposizione con un singolo quantificatore universale vera in $Z^*[x]$ è vera anche in **N**.

Diamo la definizione seguente: $p \in Z^*[x]$ è *primo* se è diverso da 0 e da 1 e se non esistono due elementi di $Z^*[x]$, entrambi diversi da 1, il cui prodotto è p; dunque un polinomio non costante è primo se e solo se è contemporaneamente irriducibile e primitivo (cioè se il MCD dei suoi coefficienti è 1). Possiamo esprimere Pr(y) ("y è primo") nel modo seguente:

$$y \neq 0 \wedge y \neq 1 \wedge (\neg(\exists a)(\exists b)(a \neq 1 \wedge b \neq 1 \wedge ab = y))$$

Per quanto riguarda il confronto tra gli ambienti numerico e polinomiale, puntualizzeremo alcune evidenti differenze.

PROPOSIZIONE 8. In $Z^*[x]$, ogni polinomio di primo grado primitivo è primo; un polinomio di primo grado i cui coefficienti abbiano MCD $h>1$ può essere scritto come somma di h polinomi primi.

DIMOSTRAZIONE. La prima parte segue dalla definizione di elemento primo in $Z^*[x]$; per la seconda, si consideri il polinomio $mhx+nh$ con m, n coprimi e $h>1$, che può essere scritto come somma di h polinomi primi $mx+n$. ■

Dalla proposizione precedente segue ad esempio che per ogni intero k il polinomio $x+k$ è primo, mentre se un naturale $n>2$ è primo, il suo successore, pari, non è primo. Questa osservazione è interessante; infatti, scrivendo:

$$(\exists y)(y \neq 2 \wedge \mathrm{Pr}(y) \wedge \mathrm{Pr}(y+1))$$

abbiamo individuato un'affermazione vera con riferimento al modello polinomiale ma non a quello numerico.

Esaminiamo il ruolo degli elementi primi in $Z^*[x]$. In particolare, sottolineiamo che $Z^*[x]$ è fattoriale[7]: infatti se D (commutativo) è fattoriale, tale è anche $D[x]$ (Jacobson, 1974, pp. 146-147); immediata conseguenza di ciò è che $\mathbf{Z}[x_1, x_2, \ldots, x_r]$ è fattoriale (Jacobson, 1974, p. 148). Didatticamente può essere interessante la dimostrazione di risultati di esistenza (ogni q di $Z^*[x]$, $q \neq 0$ e $q \neq 1$, può scriversi come prodotto di primi di $Z^*[x]$) o di unicità con metodi elementari.

Come si trovano elementi primi di **N**? Si può fare ciò con metodi elementari come il crivello di Eratostene se consideriamo una limitazione superiore (Ribenboim, 1995, p. 14); questo celebre procedimento non può però essere applicato, in generale, in $Z^*[x]$: nel paragrafo precedente abbiamo sottolineato la differenza tra l'ordine in **N** e in $Z^*[x]$ e tale differenza è elemento essenziale del confronto tra **N** e $Z^*[x]$. Mentre un intervallo $a \leq n \leq b$ comprende un numero finito di naturali, un'analoga condizione in $Z^*[x]$ può indicare infiniti elementi: per la Proposizione 3, assegnato un polinomio non costante $b(x) \in Z^*[x]$, esistono infiniti elementi $y \in Z^*[x]$ tali che $0 \leq y \leq b(x)$.

Un importante risultato esprime una condizione necessaria e sufficiente di primalità in **N**: il teorema di Wilson, secondo il quale $(p-1)!+1$ è un multiplo di p se e solo se p è primo (Hardy & Wright, 1979, p. 68): è possibile applicare un analogo teorema in $Z^*[x]$? Purtroppo non ha molto senso considerare $q(x)!$ essendo $q(x)$ un polinomio non costante: come potremmo definire "il prodotto di tutti gli elementi non nulli di $Z^*[x]$ non maggiori di $q(x)$"? Dunque anche il teorema di Wilson non può essere applicato, in generale, in $Z^*[x]$.

Nonostante queste iniziali delusioni, risulta semplice considerare altre proposizioni aritmetiche in $Z^*[x]$ (Bagni, 2002; per le congetture aritmetiche si può fare riferimento a: Guy, 1994). Consideriamo la presenza di primi in una progressione aritmetica (secondo il teorema provato nel 1837 da Dirichlet, se $h>1$ ed $a \neq 0$ sono coprimi, allora la progressione: a, $a+h$, $a+2h$, $a+3h$, … include infiniti numeri primi: Ribenboim, 1989, p. 205). Per quanto riguarda i

[7] Ricordiamo la definizione: sia M un monoide commutativo nel quale vale la legge di cancellazione; esso è detto *fattoriale* se ogni suo elemento diverso da 0 e da 1 ammette una fattorizzazione essenzialmente unica (dunque a parte l'ordine dei fattori) in elementi irriducibili (Jacobson, 1974, p. 136).

polinomi, è banale trovare progressioni aritmetiche interamente costituite da elementi primi; ad esempio, se h è un intero, $h \neq 0$, tutti i polinomi della progressione x, $x+h$, $x+2h$, $x+3h$, … sono primi. Da ciò possiamo far seguire la versione della Congettura dei Primi Gemelli in $Z^*[x]$[8]: è immediato verificare che esistono infinite coppie di elementi primi $(p(x); q(x))$ in $Z^*[x]$ tali che $q(x) = p(x)+2$ (ad esempio $p(x) = x+k$, $q(x) = x+k+2$, per ogni $k \in \mathbf{Z}$). Un'altra nota interessante si riferisce agli elementi primi della forma n^2+1: sono infiniti? Si tratta di un problema aperto in **N** (2003); ma è semplice mostrare che esistono infiniti elementi $p(x) \in Z^*[x]$ tali che $[p(x)]^2+1$ è un elemento primo di $Z^*[x]$ (ad esempio $p(x) = x+k$ per ogni $k \in \mathbf{Z}$: Bagni, 2002).

Una forma più generale della precedente congettura in **N** è la seguente: se a, b, c sono coprimi, a è positivo, $a+b$ e c non sono entrambi pari e b^2-4ac non è un quadrato, allora esistono infiniti primi della forma an^2+bn+c (Hardy & Wright, 1979, p. 19). Per quanto riguarda $Z^*[x]$, proviamo il risultato seguente.

PROPOSIZIONE 9. Se a, b, c sono coprimi, a è positivo, b^2-4ac non è un quadrato, allora esistono infiniti $p(x) \in Z^*[x]$ tali che $a[p(x)]^2+bp(x)+c$ è un elemento primo di $Z^*[x]$.

DIMOSTRAZIONE. Consideriamo ancora $p(x) = x+k$ per ogni $k \in \mathbf{Z}$. Si ha:

$$a[p(x)]^2+bp(x)+c = a(x+k)^2+b(x+k)+c = ax^2+(2ak+b)x+ak^2+bk+c$$

che appartiene a $Z^*[x]$, avendo il coefficiente direttivo a positivo, ed è primo, essendo primitivo (a, b, c sono coprimi) e irriducibile; infatti:

$$\Delta(a, b, c, k) = (2ak+b)^2-4a(ak^2+bk+c) = b^2-4ac$$

e b^2-4ac non è un quadrato. ■

Molte questioni di teoria dei numeri riguardano i numeri di Fermat $F_n = 2^{(2^n)}+1$ e di Mersenne, $M_q = 2^q-1$, con q primo (Ribenboim, 1989, pp. 71-81): ad esempio non è noto se F_n è primo per infiniti valori di n, se F_n è composto per

---

[8] Dal punto di vista formale, sottolineiamo nuovamente che i quantificatori logici sono finitari, mentre la congettura dei Primi Gemelli fa riferimento all'esistenza di *infinite* coppie di numeri primi gemelli; dunque essa può essere espressa, per i naturali, nel modo seguente: $(\forall n)(\exists p)[\mathrm{Pr}(p) \wedge \mathrm{Pr}(p+2) \wedge (p>n)]$ (dove $\mathrm{Pr}(m)$ significa "m è primo"). Interessante è ricordare che non sappiamo se esistono infiniti primi gemelli (2003), ma nel 1919 Brun ha dimostrato che la somma dei reciproci dei primi gemelli converge a 1.902160577783278… (la cosiddetta costante di Brun). Nel 2001 Underbakke e Carmody hanno verificato che $318032361 \cdot 2^{107001} \pm 1$ sono numeri primi.

infiniti valori di n, se F_n non ha divisori quadrati per ogni n; tali problemi sono aperti (2003) anche per M_q[9]. Tuttavia la considerazione dei problemi citati in $Z^*[x]$ non appare molto significativa, in quanto elevando un polinomio ad un esponente polinomiale non si ottiene, in generale, un polinomio[10].

5. LA TEORIA ADDITIVA DEI NUMERI

È interessante considerare in $Z^*[x]$ alcuni risultati della teoria additiva dei numeri (è generalmente così denominato quel settore della teoria dei numeri in cui si considerano insiemi A di interi ed insiemi delle somme di h elementi di A)[11]. Ad esempio, il teorema di Lagrange che afferma che ogni naturale è la somma di quattro quadrati (Nathanson, 1996b)[12] non vale in $Z^*[x]$.

PROPOSIZIONE 10. Esistono elementi di $Z^*[x]$ che non possono essere espressi come somma di elementi quadrati di $Z^*[x]$.

DIMOSTRAZIONE. È banale, ad esempio, verificare che un polinomio di primo grado di $Z^*[x]$ non può essere espresso come somma di quadrati di $Z^*[x]$. ■

Le precedenti considerazioni possono essere generalizzate. L'insieme $B \subseteq \mathbf{N}$ è chiamato *base di ordine h* se ogni $n \in \mathbf{N}$ può essere espresso come somma di h elementi di B; ad esempio, per il teorema di Lagrange l'insieme $\{n \in \mathbf{N}: n = x^2 \wedge$

---

[9] Per quanto riguarda i grandi primi di Mersenne, ricordiamo che nel 2001 Cameron, Kurowski e Woltman hanno verificato che $2^{13466917}-1$ è primo. Uno studio di molte questioni collegate all'esponenziazione è in: Macintyre, 1981.

[10] È possibile considerare in $Z^*[x]$ alcuni classici risultati collegati alle congruenze mod p? Invitiamo ad esempio il lettore a considerare la Legge di Gauss della Reciprocità Quadratica, secondo la quale, se p e q sono primi dispari diversi, il carattere quadratico di q rispetto a p (cioè il fatto che q sia o non sia residuo quadratico modulo p, ovvero che la congruenza $x^2 \equiv q \pmod{p}$ sia possibile o impossibile) è uguale a quello di p rispetto a q se e solo se almeno uno dei numeri p, q è della forma $4n+1$ (si veda: Hardy & Wright, 1979). Per valutare la sua eventuale estendibilità da **N** a $Z^*[x]$ il lettore può cercare di verificare tale celebre risultato ad esempio con riferimento ai polinomi: $p(x) = 16x^2+16x+1$ e $q(x) = x+1$.

[11] Naturalmente la denominazione "teoria additiva dei numeri" ora impiegata (che riprende ad esempio: Nathanson, 1006a e 1996b) non deve essere messa in relazione con la teoria di Presburger!

[12] Nel libro *Meditationes Algebraicae*, pubblicato nel 1770, Waring affermò (senza dimostrazione) che ogni numero naturale è la somma di quattro quadrati, nove cubi, diciannove quarte potenze etc. (Nathanson, 1996a, p. 37).

$x \in \mathbf{N}\}$ è una base di ordine 4. Un problema fondamentale della teoria additiva dei numeri è decidere se un assegnato insieme è una base di ordine finito; e se consideriamo l'insieme delle potenze k-esime non negative esso viene detto problema di Waring[13]; il teorema di Hilbert-Waring afferma che per ogni intero positivo k, l'insieme delle potenze k-esime non negative è una base di ordine finito (Nathanson, 1996a, pp. 75-93). Per quanto riguarda $Z^*[x]$, però, si prova:

PROPOSIZIONE 11. Per ogni intero $k>1$, esistono elementi di $Z^*[x]$ che non sono esprimibili come somma di elementi di $\{y \in Z^*[x]: y = x^k \wedge x \in Z^*[x]\}$.

DIMOSTRAZIONE. Ancora una volta è immediato mostrare che ogni polinomio di $Z^*[x]$ di primo grado non può essere espresso come somma di elementi di $\{y \in Z^*[x]: y = x^k \wedge x \in Z^*[x]\}$, con $k>1$. ■

6. IL TEOREMA DI SHRINEL'MAN E L'ULTIMO TEOREMA DI FERMAT

Possiamo ora considerare in $Z^*[x]$ il teorema di Shrinel'man (o di Shrinel'man-Goldbach, come ricordato in: Nathanson, 1996a, p. 177), dimostrato nel 1930, che afferma che ogni numero naturale diverso da 0 e da 1 può essere espresso come somma di un numero finito di primi.

PROPOSIZIONE 12. Ogni elemento di $Z^*[x]$ diverso da 0 e da 1 può essere espresso come somma di un numero finito di elementi primi di $Z^*[x]$.

DIMOSTRAZIONE. Se l'elemento di $Z^*[x]$ è una costante è possibile applicare direttamente il (provato) teorema di Shrinel'man in $\mathbf{N}$.

Altrimenti, consideriamo un polinomio non costante $f_n(x) \in Z^*[x]$:

$$f_n(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$

di grado n; esprimiamo $f_n(x)$ come somma dei seguenti polinomi di $Z^*[x]$:

$$f_1(x) = a_n x^n - p x^{n-1} - p x^{n-2} - ... - p x - p$$
$$f_{n-1}(x) = (a_{n-1}+p) x^{n-1} + (a_{n-2}+p) x^{n-2} + ... + (a_1+p) x + a_0 + p$$

dove p è un numero primo maggiore di a_n e di $|a_{n-1}|$ (affinché il coefficiente direttivo di $f_{n-1}(x)$ sia positivo). $f_1(x)$ è irriducibile per il criterio di Eisenstein (il primo p divide tutti i suoi coefficienti a parte quello direttivo e p^2 non divide l'ultimo p: Jacobson, 1974, p. 148); inoltre $f_1(x)$ è primitivo, dunque è primo.

---

[13] Secondo il teorema di Wieferich-Kempner, pubblicato nel 1909 e dimostrato completamente nel 1912, ogni numero naturale può essere espresso come somma di nove cubi (Nathanson, 1996a, pp. 37-38).

Applichiamo ora nuovamente il procedimento con riferimento al polinomio $f_{n-1}(x)$, di grado $n-1$: possiamo così esprimerlo come somma di un polinomio primo $f_2(x)$ e di un polinomio $f_{n-2}(x)$ il cui grado è $n-2$, entrambi appartenenti a $Z^*[x]$. Iterando il procedimento per un numero finito di passi (essendo finito il grado del polinomio inizialmente considerato), si otterrà infine un polinomio di $Z^*[x]$ di grado 1; esso, per la Proposizione 8, o è primo o può essere espresso come somma di un numero finito di polinomi primi di $Z^*[x]$. ■

Possiamo dire che il teorema di Shrinel'man è stato "esteso" da **N** a $Z^*[x]$; tuttavia è interessante rilevare che la dimostrazione precedente per gli elementi non costanti di $Z^*[x]$ è indipendente dalla dimostrazione del teorema in **N**.

Una situazione per molti versi analoga può essere descritta con riferimento all'Ultimo Teorema di Fermat. Una sua "estensione" da **N** a $Z^*[x]$ sarebbe banale: se esistessero tre polinomi non costanti $a(x)$; $b(x)$; $c(x)$ appartenenti a $Z^*[x]$ ed un naturale $n \geq 3$ tali che $[a(x)]^n+[b(x)]^n = [c(x)]^n$, potremo assegnare un valore alla x in modo che $a(x)$, $b(x)$, $c(x)$ siano contemporaneamente positivi (i loro coefficienti direttivi sono infatti positivi) e ciò contrasterebbe con il dimostrato Ultimo Teorema di Fermat in **N** (Bagni, 2002).

Per quanto riguarda elementi non costanti di $Z^*[x]$, si può però dimostrare l'Ultimo Teorema di Fermat anche indipendentemente dalla dimostrazione in **N**: si prova direttamente che l'equazione di Fermat $a^n+b^n = c^n$ non ha soluzioni polinomiali non costanti se $n \geq 3$ (la dimostrazione è in: Greenleaf, 1969; si noti che tale equazione ha soluzioni polinomiali non costanti per $n = 2$, ad esempio: $a = (x^2-1)^2$; $b = (2x)^2$; $c = (x^2+1)^2$, soluzione che richiama il procedimento di Platone per ricavare terne pitagoriche: Nathanson, 2000, p. 183).

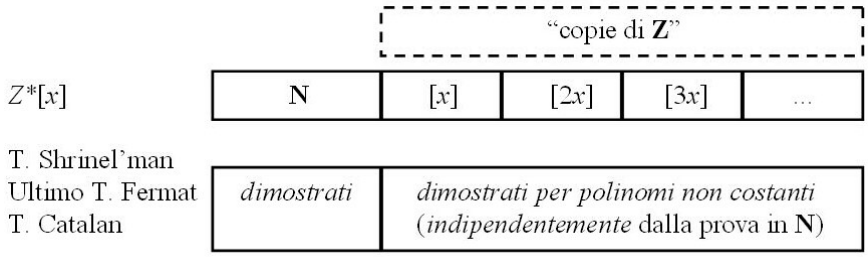
7. DUE CELEBRI PROBLEMI: LE CONGETTURE DI CATALAN E DI GOLDBACH

Ancora più recente è la vicenda della proposizione a lungo indicata come "congettura di Catalan". Essa (proposta nel 1844, dal matematico belga Eugène Charles Catalan, 1814-1894) afferma che 8 e 9 sono in **N** le uniche potenze consecutive (Nathanson, 2000, p. 186); equivalentemente, afferma che l'unica soluzione dell'equazione $x^m-y^n = 1$, con x, y, m, n numeri naturali maggiori di 1, è: $x = n = 3$, $y = m = 2$. Dimostrare o smentire questa congettura ha costituito un importante problema della teoria dei Numeri fino alla conclusiva sua dimostrazione, presentata da Preda Mihailescu nel 2002 (Weisstein, 2002)[14].

[14] Nel 1999, M. Mignotte aveva dimostrato che eventuali eccezioni a quanto espresso nella congettura di Catalan avrebbero dovuto essere tali che: $m > 7.15 \cdot 10^{11}$, $n > 7.58 \cdot 10^{16}$ (Peterson, 2000).

Naturalmente non cercheremo di dimostrare la congettura di Catalan in $Z^*[x]$ con metodi elementari: essa infatti implicherebbe la dimostrazione elementare della congettura in **N**. Sottolineiamo però che è possibile provare (Nathanson, 1974) che $x^m - y^n = 1$, con $m \geq 2$, $n \geq 2$ naturali, non ha soluzioni polinomiali non costanti. Dunque la congettura di Catalan è valida anche per tutti i polinomi non costanti di $Z^*[x]$ e la dimostrazione di ciò non richiede la dimostrazione della congettura in **N**.

Possiamo visualizzare la situazione nel modo seguente:



Un importante teorema della teoria additiva dei numeri è stato dimostrato nel 1937 da Vinogradov (Cudakov, 1947; Nathanson, 1996a, p. 211): ogni naturale dispari "abbastanza grande" è la somma di tre primi[15]. Non è però facile considerare questo risultato con riferimento a $Z^*[x]$: dovremmo infatti definire gli elementi "dispari" di $Z^*[x]$, ma la distinzione tra elementi pari e dispari in $Z^*[x]$ non può essere introdotta come nel caso dei numeri naturali. Da un lato, è plausibile chiamare *pari* un polinomio $p(x) \in Z^*[x]$ i cui coefficienti siano tutti pari, dunque in modo che sia possibile scrivere $p(x) = 2q(x)$ con $q(x) \in Z^*[x]$; ma la definizione di elemento *dispari* di $Z^*[x]$ potrebbe a questo punto far riferimento a tutti gli elementi di $Z^*[x]$ che non sono pari (ad esempio sarebbe dispari: $nx+1$, per ogni $n \in \mathbf{N}$); oppure potremmo chiamare *dispari* un elemento $Z^*[x]$ del tipo $2q(x)+1$, con $q(x) \in Z^*[x]$ e tali "definizioni" non sarebbero equivalenti (ad esempio, secondo quest'ultima definizione $nx+1$ sarebbe dispari se e solo se n è pari; altrimenti non sarebbe né pari né dispari).

Limitiamoci a considerare gli elementi pari di $Z^*[x]$ ed occupiamoci della congettura di Goldbach in $Z^*[x]$. Sottolineiamo subito che tale congettura

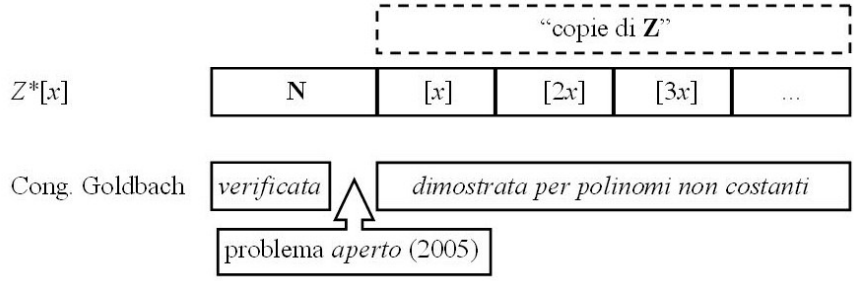
---

[15] Per quanto riguarda la valutazione numerica, nel 1956 Borodzkin dimostrò che $n > 3^{14348907}$; nel 1989 Chen e Wang provarono che $n > 10^{43000}$.

presenta un quantificatore universale[16]: ancora una volta ci occuperemo dunque solo dei polinomi non costanti.

In un recente lavoro (Bagni, 2002) abbiamo provato con metodi elementari che se il polinomio non costante $f(x) \in Z^*[x]$ non è primitivo, allora esistono due polinomi primi $f_1(x) \in Z^*[x]$, $f_2(x) \in Z^*[x]$ tali che $f(x) = f_1(x)+f_2(x)$. Da tale risultato segue che la congettura di Goldbach vale per tutti i polinomi non costanti di $Z^*[x]$ (dicendo *pari* un polinomio i cui coefficienti siano tutti pari).[17]

Possiamo riassumere quanto precedentemente espresso nella figura seguente. Rispetto a $Z^*[x]$ (ed alle "copie ordinate di **Z**"), osserviamo che la congettura di Goldbach è verificata empiricamente per un iniziale insieme finito di numeri naturali; quindi la sua validità non è dimostrata per infiniti naturali; infine essa vale per tutti i polinomi con costanti di $Z^*[x]$.



8. OLTRE I NUMERI NATURALI...

Abbiamo esaminato analogie e differenze tra un modello di *Q* e il modello standard di *PA*. Osserviamo ora la tabella seguente: nella prima colonna abbiamo

---

[16] Nella congettura di Goldbach non c'è solo un quantificatore universale: si afferma che per ogni intero pari n maggiore di 2 *esiste* una coppia di primi (p, q) tale che $p+q = n$. Ricordiamo che nella lettera originale di Goldbach a Euler del 1742 era congetturato che ogni naturale $n>5$ fosse la somma di tre primi; Euler rispose rilevando come ciò fosse equivalente ad affermare che ogni numero pari $n>2$ è la somma di due primi. Per quanto riguarda i risultati collegati alla congettura, uno dei più famosi è il teorema di Chen (1966-1973), che afferma che ogni naturale pari "abbastanza grande" può essere espresso da una somma di un primo e di un altro numero che o è primo o è il prodotto di due primi (Nathanson, 1996a, p. 271). Sul fronte dei test sperimentali, Richstein (1998) ha verificato la congettura fino a $4 \cdot 10^{14}$.

[17] Sulla congettura di Goldbach: Weyl, 1942; Erdös 1965; Wang, 1984.

indicato le teorie aritmetiche considerate (*PA* e *Q*); nella seconda i modelli di tali teorie. Ipotizziamo ora la presenza di due nuove colonne: in corrispondenza di **N** collochiamo $\mathbf{Q}^{+}\cup\{0\}$ (l'insieme dei razionali non negativi) e $\mathbf{R}^{+}\cup\{0\}$ (l'insieme dei reali non negativi); quali insiemi possiamo considerare in corrispondenza di $Z^*[x]$?

Indichiamo tali insiemi con $Q^*[x]$ e $R^*[x]\cup\{0\}$:

Teoria	*Modello*		
PA	**N**	$\mathbf{Q}^{+}\cup\{0\}$	$\mathbf{R}^{+}\cup\{0\}$
Q	sottoinsieme di $Z^*[x]$	$Q^*[x]$	$R^*[x]$

Come possiamo interpretare $Q^*[x]$ e $R^*[x]$? Prima di indicare una risposta ricordiamo che per esprimere un elemento $x\in\mathbf{Q}^{+}\cup\{0\}$ mediante elementi di **N** possiamo procedere in più modi (ad esempio con una coppia di naturali, il secondo dei quali non nullo); un interessante procedimento porta allo sviluppo del razionale considerato in frazione continua regolare limitata mediante l'algoritmo di Euclide[18]. Ricordiamo che una frazione continua regolare è un'espressione:

$$n_0+\cfrac{1}{n_1+\cfrac{1}{n_2+\cfrac{1}{n_3+\ldots}}}$$

in cui n_0, n_1, n_2, n_3, … sono interi, con $n_0\geq 0$, $n_1>0$, $n_2>0$, $n_3>0$, … (Lorentzen & Waadeland, 1992) Indicheremo una frazione continua regolare elencando solo n_0 e i denominatori: $[n_0, n_1, n_2, n_3, n_4, \ldots]$.

Ogni razionale positivo può essere espresso mediante una frazione continua regolare limitata (Lorentzen & Waadeland, 1992, p. 404). Ciò ci suggerisce di interpretare un elemento di $\mathbf{Q}^{+}\cup\{0\}$ come una *n*-pla ordinata di naturali. In termini analoghi, con una *n*-pla ordinata di elementi di $Z^*[x]$ proponiamo di esprimere un elemento di $Q^*[x]$, dunque una frazione algebrica. Ad esempio:

$$x+\cfrac{1}{x+2+\cfrac{1}{x+1}}=\frac{x^3+3x^2+4x+1}{x^2+3x+3}$$

[18] Euclide *Elementi*, VII, 1-2. Per i passi dell'algoritmo: Hensley, 1994.

Dunque la frazione algebrica $\frac{x^3+3x^2+4x+1}{x^2+3x+3}$ può essere indicata mediante la sequenza del primo quoziente e dei denominatori della frazione continua limitata [x; x+2; x+1].

Consideriamo ora una successione (non limitata) di naturali: tali numeri potrebbero essere ad esempio le cifre dell'espressione decimale di un reale x; oppure potrebbero essere fissati con riferimento all'espressione di x mediante una frazione continua regolare non limitata. Infatti è noto che una frazione continua regolare non limitata converge ad un reale irrazionale positivo[19]: per ogni irrazionale positivo λ, esiste una ed una sola frazione continua regolare il cui valore è λ (Lorentzen & Waadeland, 1992, p. 404). Ad esempio:

$\sqrt{11}$ = [3, 3, 6, 3, 6, 3, 6, ...]

Per analogia, interpretiamo gli elementi di $R^*[x]$ come sequenze [z_0, z_1, z_2, z_3, …] non necessariamente limitate di elementi di $Z^*[x]$. Ad esempio: [x+3, 3, 6, 3, 6, …] è un elemento di $R^*[x]$ (si tratta di: $x+\sqrt{11}$, ricordando il precedente sviluppo).

In generale il procedimento ora segnalato non porta a frazioni algebriche. Proponiamo un altro esempio; la seguente scrittura:

$$\sqrt{[P(x)]^2+1} = P(x) + \cfrac{1}{2P(x) + \cfrac{1}{2P(x) + \cfrac{1}{2P(x)+...}}}$$

può essere collegata al metodo di Cataldi per il calcolo della radice quadrata di un numero (il suo *Trattato* è stato pubblicato nel 1613: Olds, 1963). Possiamo interpretare $\sqrt{[P(x)]^2+1}$ con la successione: [$P(x)$, 2$P(x)$, 2$P(x)$, 2$P(x)$, …].

Dal punto di vista didattico può essere interessante proporre alcuni esempi. Considerando P(x) = x^2–x+1, presenteremo i diagrammi delle funzioni:

(a) $y = \sqrt{(x^2-x+1)^2+1}$ (funzione f da sviluppare)

(b) $y = x^2 - x + 1$ (I approssimazione)

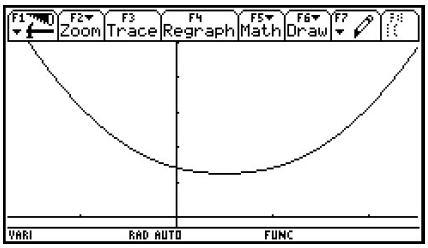
(c) $y = x^2 - x + 1 + \frac{1}{2x^2-2x+2}$ (II approssimazione)

---

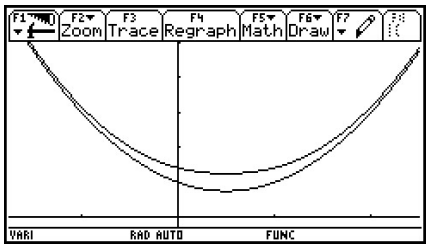
[19] Proprio per provare l'irrazionalità di e, ad esempio, Leonhard Euler (1707-1783) dimostrò (1737) che: e–1 = [1, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8 …].

(d) $$y = x^2 - x + 1 + \cfrac{1}{2x^2 - 2x + 2 + \cfrac{1}{2x^2 - 2x + 2}}$$ (III approssimazione)

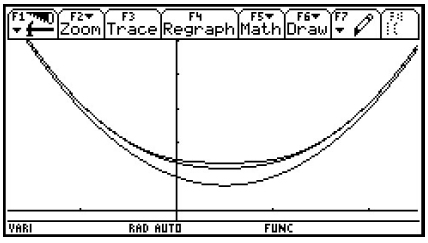
Per la visualizzazione possiamo utilizzare didatticamente una calcolatrice grafica, ma la limitata risoluzione può costituire un ostacolo (si noti che i grafici seguenti non sono monometrici).



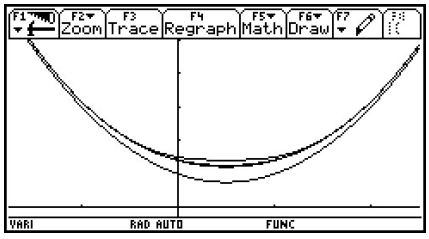
la sola funzione *f* da sviluppare



f e la prima approssimazione

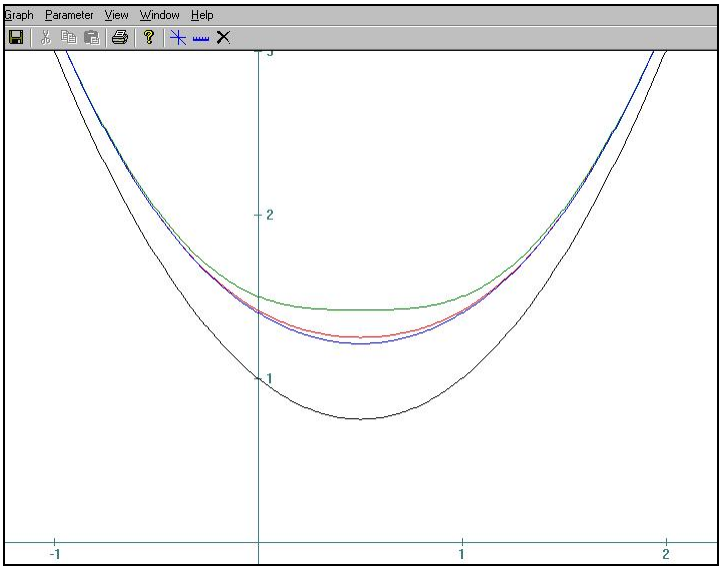


f e le prime due approssimazioni



f e le prime tre approssimazioni

Nella figura seguente, ottenuta con un programma per tracciamento di grafici per computer, procedendo dall'alto, i diagrammi sono ordinatamente riferiti alle funzioni (c), (a), (d), (b).



Allo studio elementare di $R^*[x]$ potranno essere dedicate ulteriori ricerche[20].

Bibliografia

Bagni, G.T. (2000), «Simple» rules and general rules in some High School students' mistakes, *Journal fur Mathematik Didaktik*, 21 (2000), 2, 124-138.

Bagni, G.T. (2002), Congetture e teorie aritmetiche, *Archimede*, 2, 96-100.

Bagni, G.T. (2003a), Numeri e polinomi: un modello dell'Aritmetica di Robinson, *Conferenze e Comunicazioni XVII Congresso Unione Matematica Italiana*, 384.

Bagni, G.T. (2003b), Numbers and Polynomials: a Model of Robinson Arithmetics in Mathematics Education, *8. Oesterreichisches Mathematikertreffen*, 55.

Chang, C.C. & Keisler, H.J. (1973), *Model Theory*, North-Holland, Amsterdam-London.

Cudakov, N.G. (1947), On Goldbach-Vinogradov theorem, *Ann. Math.*, 2, 48, 515-545.

Erdös, P. (1965), Some recent advances and current problems in number theory, *Lectures on modern mathematics*, 3, 196-244, Wiley, New York.

Guy, R.K. (1994), *Unsolved Problems in Number Theory*, 2nd edition, Springer-Verlag, Berlin-Heidelberg-New York.

[20] L'autore ringrazia il Prof. Claudio Bernardi, il Prof. Maurizio Fattorosi Barnaba dell'Università di Roma "La Sapienza" e il Prof. Mario Ferrari dell'Università di Pavia per le acute osservazioni e i preziosi suggerimenti; ringrazia inoltre il Dott. Andrea Vietri per un'attenta lettura critica di una prima versione del presente lavoro.

Hájek, P. & Pudlák, P. (1993), *Metamathematics of First-Order Arithmetic*, Springer-Verlag, Berlin-Heidelberg-New York

Hardy, G.H. & Wright, E.M. (1979), *An Introduction to the Theory of Numbers*, 5th edition, Clarendon Press, Oxford (edizione originale: 1938).

Hensley, D. (1994), The number of Steps in the Euclidean Algorithm, in: *Journal of Number Theory*, 49, 2, 11/94, 142-182.

Jacobson, N. (1974), *Basic Algebra I*¸ Freeman, San Francisco.

Kaye, R.W. (1991), *Models of Peano Arithmetic*, Clarendon Press, Oxford.

Lorentzen, L. & Waadeland, H. (1992), *Continued Fractions with Applications*, North-Holland, Amsterdam.

Macintyre, A. (1981), The laws of exponentiation, *Model theory and arithmetic* (Paris, 1979-1980), Springer-Verlag, Berlin-Heidelberg-New York, 185-197.

Macintyre, A. (1987), The strength of weak systems, *Schriftenreihe der Wittgenstein-Gesellschaft* 13, Logic, Philosophy of Science and Epistemology, Wien, 43-59.

Markovitz, Z.; Eylon, B. & Bruckheimer, N. (1986), Functions today and yesterday, *For the learning of mathematics*, 6 (2), 18-24.

Mendelson, E. (1997), *Introduction to mathematical logic*, 4th edition, Van Nostrand, Princeton.

Nathanson, M.B. (1996a), *Additive number theory. The classical bases*, Springer-Verlag, Berlin-Heidelberg-New York.

Nathanson, M.B. (1996b), *Additive number theory. Inverse problems and geometry of sumsets*, Springer-Verlag, Berlin-Heidelberg-New York

Niven, I. (1961), *Numbers: rational and irrationals*, Random House, New York.

Olds, C.D. (1963), *Continued Fractions*, Random House, New York.

Peterson, I. (2000), *MathTrek: Zeroing In on Catalan's Conjecture*, Dec. 4, 2000: http://www.sciencenews.org/20001202/mathtrek.asp.

Ribenboim, P. (1995), *The Book of Prime Number Records*, 3rd edition, Springer-Verlag, Berlin-Heidelberg-New York.

Robinson, A. (1974), *Introduzione alla teoria dei modelli e alla metamatematica dell'algebra*, Boringhieri, Torino (edizione originale: 1963).

Wang, Y. (1984), *Goldbach Conjecture*, World Scientific Publishers, Singapore.

Weisstein, E.W. (2002), Draft Proof of Catalan's Conjecture Circulated, *MathWorld Headline News*, May 5, 2002.

Weyl, H. (1942), A half-century of mathematics, *American Math. Monthly*, 58, 523-553.