Appendice B

Teorie aritmetiche e modelli

In questa appendice riprenderemo alcune osservazioni sulle teorie (ci riferiremo in particolare alle teorie per l'aritmetica) e sui modelli.[1]

La teoria più nota per l'aritmetica (i numeri naturali con le usuali operazioni) è l'aritmetica di Peano, *PA* (si veda ad esempio: Mendelson, 1972, p. 128); una teoria più debole è la teoria *Q* di Robinson (Mendelson, 1972, p. 187). *Q* si ottiene da PA togliendo il principio di induzione:

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

(dove *S* è la funzione unaria successore) ed aggiungendo l'assioma:

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

che è un teorema di *PA* (lasciamo al lettore la facile dimostrazione per induzione). Ricordiamo che dal punto di vista formale il principio di induzione è uno schema di assiomi perché porta ad un assioma per ogni formula φ con una variabile libera: pertanto mentre *Q* ha un numero finito di assiomi, *PA* ha infiniti assiomi.

Una teoria, in genere, ha più modelli: l'insieme **N** dei numeri naturali con l'addizione e la moltiplicazione è il modello standard di *PA*; la costruzione di modelli di *PA* non isomorfi a **N** è complicata e non può essere proposta a livello di scuola secondaria. Invece è semplice trovare modelli di *Q* non isomorfi a **N**: ad esempio, nel presente lavoro indicheremo con $Z^*[x]$ l'insieme costituito dal polinomio nullo e dai polinomi a coefficienti interi con il coefficiente direttivo positivo: $Z^*[x]$ è un modello di *Q* (Mendelson, 1972, p. 188).

Ogni enunciato dimostrabile in *Q* è dimostrabile anche in *PA*; ci sono però enunciati dimostrabili in *PA* che non sono dimostrabili in *Q*; tuttavia un enunciato dimostrabile in *PA* non è mai confutabile in *Q*.[2]

---

[1] Ci collegheremo a Bagni, 2002, da cui riportiamo alcuni risultati.

[2] Infatti se un enunciato fosse dimostrabile in *PA* e confutabile in *Q*, essendo *PA* un'estensione di *Q*, allora *PA* sarebbe inconsistente.

Uno dei più celebri problemi della storia della Matematica è l'Ultimo Teorema di Fermat, che afferma che non esistono una terna di naturali non nulli $(a; b; c)$ ed un naturale $n \geq 3$ tali che $a^n+b^n = c^n$. Passiamo ora a considerare per via elementare l'analoga proprietà polinomiale.

Proposizione. In $Z^*[x]$ non esistono una terna di polinomi $(A(x); B(x); C(x))$, ciascuno dei quali non identicamente nullo, ed un naturale $n \geq 3$ tali che: $[A(x)]^n+[B(x)]^n = [C(x)]^n$.

Dimostrazione. Ammettiamo per assurdo che in $Z^*[x]$ esistano una terna di polinomi $(A(x); B(x); C(x))$, ciascuno dei quali non identicamente nullo, e un naturale $n \geq 3$ tali che $[A(x)]^n+[B(x)]^n = [C(x)]^n$.

Se tutti i polinomi considerati sono costanti, è contraddetto l'Ultimo Teorema di Fermat (che, com'è noto, è stato dimostrato da Andrew Wiles nel 1993-1994). Considerando polinomi non costanti, è possibile sostituire un naturale alla x in modo che $A(x)$, $B(x)$, $C(x)$ siano contemporaneamente positivi (per la positività dei coefficienti direttivi $\lim_{x\to+\infty} A(x) = \lim_{x\to+\infty} B(x) = \lim_{x\to+\infty} C(x) = +\infty$) e otteniamo ancora un'uguaglianza tale da contraddire l'Ultimo Teorema di Fermat. ν

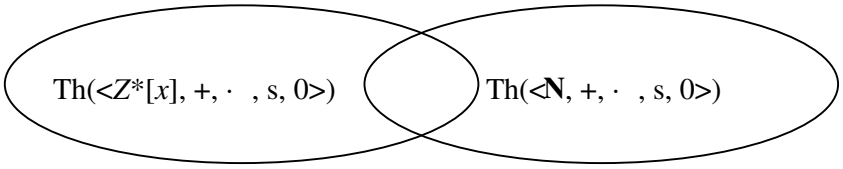
Abbiamo dunque constatato che l'Ultimo Teorema di Fermat mantiene la propria validità passando dall'ambiente numerico a quello polinomiale [3]; esaminando altre proprietà vedremo però che ci sono alcune differenze tra quanto accade in ambiente numerico e quanto accade nell'insieme $Z^*[x]$.

Il confronto tra $\mathbf{N}$ e $Z^*[x]$ non si basa solo sulla considerazione di esempi e controesempi. Sottolineiamo innanzitutto che $\langle Z^*[x], +, \cdot, s, 0\rangle$ non è un modello di *PA*; ad esempio:

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

che può essere dimostrato per induzione, non è in $Z^*[x]$ (ogni polinomio non costante di $Z^*[x]$, $B(x) = a_n x^n+a_{n-1}x^{n-1}+...+a_1 x+a_0$ I cui coefficienti a_n, a_{n-1}, $...a_1$ non siano tutti pari può essere considerato come controesempio). Troveremo proposizioni vere in $\langle Z^*[x], +, \cdot, s, 0\rangle$ che saranno false se riferite a $\langle \mathbf{N}, +, \cdot, s, 0\rangle$ (Chang & Keisler, 1973, p. 32). Nella figura seguente Th(M) indica l'insieme degli enunciati veri in M:

[3] Si noti che l'ultimo teorema di Fermat può essere dimostrato per i polinomi non costanti anche senza ricorrere alla dimostrazione di Wiles-Taylor per i numeri naturali (Nathanson, 1996).



Si dimostra che Th(<**N**, +, · , s, 0>)∩Th(<$Z^*[x]$, +, · , s, 0>) ≠ ∅ (tale intersezione include *la chiusura deduttiva* di Q, l'insieme di tutti gli enunciati deducibili da Q).

Abbiamo sopra osservato che un elemento di Th(<**N**, +, · , s, 0>)–Th(<$Z^*[x]$, +, · , s, 0>) è: $(\forall y)(\exists z)(z+z = y \vee z+z = y+1)$. Cercheremo ora anche un elemento di Th(<$Z^*[x]$, +, · , s, 0>)–Th(<**N**, +, · , s, 0>): a tale proposito, potremmo ad esempio occuparci dell'ordine in $Z^*[x]$.

Secondo un assioma di Q, l'ordine è definito in $Z^*[x]$ nel modo seguente:

$$f(x) \le g(x) \iff \text{(def.)} \quad g(x)-f(x) \in Z^*[x]$$
$$f(x) < g(x) \iff \text{(def.)} \quad 0 \ne g(x)-f(x) \in Z^*[x]$$

Evidentemente se $f(x)$, $g(x)$, $h(x)$ sono elementi di $Z^*[x]$:

$$f(x) \le g(x) \Rightarrow f(x)+h(x) \le g(x)+h(x)$$
$$f(x) < g(x) \Rightarrow f(x)\cdot h(x) < g(x)\cdot h(x)$$
$$f(x) \le g(x) \Rightarrow f(x)+h(x) \le g(x)+h(x)$$
$$f(x) < g(x) \Rightarrow f(x)\cdot h(x) < g(x)\cdot h(x) \quad (\text{con } h(x) \ne 0)$$

Se $f(x)$, $g(x)$, $h(x)$, $h(x)-f(x)$, $h(x)-g(x)$ sono elementi di $Z^*[x]$:

$$f(x) \le g(x) \Rightarrow h(x)-g(x) \le h(x)-f(x)$$
$$f(x) < g(x) \Rightarrow h(x)-g(x) < h(x)-f(x)$$

Per quanto riguarda il minimo elemento di $Z^*[x]$, per ogni $f(x) \in Z^*[x]$ risulta: $0 \le f(x)$ (le proprietà ora ricordate valgono in $Z^*[x]$ essendo dimostrabili in Q: la loro verifica diretta in $Z^*[x]$, partendo dalle definizioni date, può essere didatticamente interessante).

Dimostriamo ancora alcuni semplici risultati:

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

Dimostrazione. Se $f(x) \leq g(x)$ è falso, allora $g(x)-f(x) \notin Z^*[x]$, quindi il coefficiente direttore di $g(x)-f(x)$ è negativo. Da ciò segue che il coefficiente direttore di $f(x)-g(x)$ è positivo, dunque $f(x)-g(x) \in Z^*[x]$ e $g(x) \leq f(x)$. ν

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

Dimostrazione. Dall'ipotesi si ha che: $f(x)+1-g(x) < f(x)+1-f(x) = 1$. Quindi: $f(x)+1-g(x) = 0$ e $g(x) = f(x)+1$. ν

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

Dimostrazione. Se $f(x) < g(x)$ allora $0 \neq g(x)-f(x) \in Z^*[x]$; quindi: $0 \neq g(x)-f(x)-k-n \in Z^*[x]$ e da $0 \neq g(x)-k-[f(x)+n] \in Z^*[x]$ si conclude: $f(x)+n < g(x)-k$. ν

Questa proprietà è interessante: abbiamo infinite coppie di elementi f, g di $Z^*[x]$ tali che $f<g$ e infinite coppie di elementi n, $k \in Z^*[x]$ tali che $f+n<g-k$. Tale proprietà vale in $Z^*[x]$, ma non vale in **N**. Abbiamo quindi trovato un elemento di $\mathrm{Th}(\langle Z^*[x], +, \cdot, s, 0\rangle)-\mathrm{Th}(\langle \mathbf{N}, +, \cdot, s, 0\rangle)$? Il problema è l'espressione formale della proprietà in questione: I quantificatori logici sono infatti *finitari*, cioè non possiamo utilizzare un infinito numero di quantificatori esistenziali nello stesso enunciato[4].

Per proporre l'interpretazione di congetture aritmetiche in $Z^*[x]$ è utile operare una distinzione. Notiamo che **N** è un sottomodello di $Z^*[x]$: dunque ogni enunciato con un solo quantificatore esistenziale vero in **N** è vero anche in $Z^*[x]$ ed ogni enunciato con un solo quantificatore universale vero in $Z^*[x]$ è vero anche in **N**.

Ci occuperemo di alcune congetture riguardanti i primi. Un elemento non nullo p di $Z^*[x]$ sarà detto *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 è primo se e solo se è irriducibile ed è primitivo (cioè il massimo comune divisore dei suoi coefficienti è 1).

Possiamo quindi esprimere $\mathrm{Pr}(y)$ ("y è primo") con:

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

[4] Per quanto riguarda i soli numeri naturali, se vogliamo esprimere la validità della proprietà $\mathrm{P}(n)$ per infiniti n, possiamo ad esempio scrivere: $(\forall m)(\exists n)(m<n \wedge \mathrm{P}(n))$, ma una simile espressione non è in grado di esprimere in $Z^*[x]$ la proprietà in questione.

Alcune differenze rispetto a quanto accade per i numeri primi sono immediatamente evidenti: ad esempio, in $Z^*[x]$ esistono infiniti elementi primi $x+k$ con k intero qualsiasi, mentre se un numero naturale $n>2$ è primo, il suo successore è composto in quanto è divisibile per 2. Ciò è molto interessante; infatti se scriviamo:

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

abbiamo trovato un elemento di $\mathrm{Th}(<Z^*[x], +, \cdot\ , s, 0>) - \mathrm{Th}(<\mathbf{N}, +, \cdot\ , s, 0>)$.

L'interpretazione e la dimostrazione di alcuni enunciati aritmetici in $Z^*[x]$ è elementare (alcune congetture sono presentate in: Guy, 1994).

Consideriamo innanzitutto la questione della presenza di primi in una progressione aritmetica (un celebre risultato dimostrato da Dirichlet nel 1837 afferma che se $h>1$ e $a \neq 0$ sono interi coprimi allora la progressione: a, $a+h$, $a+2h$, $a+3h$, … contiene infiniti numeri primi: Ribenboim, 1989, p. 205). Nel caso dei polinomi è semplice trovare progressioni aritmetiche costituite interamente da primi; ad esempio, se h è un intero non nullo, la progressione x, $x+h$, $x+2h$, $x+3h$, … è completamente costituita da polinomi primi. Immediata conseguenza di tale considerazione è la versione polinomiale della Congettura dei Primi Gemelli[5] (in $Z^*[x]$ esistono infinite coppie $(P(x); Q(x))$ di elementi primi tali che $Q(x) = P(x)+2$: si considerino $P(x) = x+k$ e $Q(x) = x+k+2$, per ogni $k \in \mathbf{Z}$) o dell'infinità dei primi della forma n^2+1 (si consideri $P(x) = x+k$ per ogni $k \in \mathbf{Z}$. Risulta: $[P(x)]^2+1 = x^2+2kx+k^2+1$, primo in quanto il suo discriminante è: $\Delta(k) = -4<0$).

Alcuni problemi aperti della Teoria dei Numeri fanno riferimento ai Numeri di Fermat $F_n = 2^{(2^n)}+1$ e ai Numeri di Mersenne, $M_q = 2^q - 1$, con q primo (Ribenboim, 1989, pp. 71-81): non sappiamo se F_n è primo per infiniti valori di n, se F_n è composto per infiniti valori di n, se F_n è privo di fattori quadrati per ogni n; le stesse domande per M_q sono ancora (2002) senza risposta. Osserviamo che la considerazione in ambito polinomiale di questi problemi non sarebbe significativa in $Z^*[x]$; infatti l'insieme dei numeri naturali è chiuso rispetto all'esponenziazione, ma ciò non accade per $Z^*[x]$: in generale, elevando un polinomio ad un esponente polinomiale non si ottiene un polinomio (potrebbe essere interessante esaminare i problemi che si ottengono mantenendo solo gli esponenti numerici).

---

[5] A proposito della Congettura dei Primi Gemelli, notiamo che i quantificatori logici sono finitari e tale congettura si riferisce all'esistenza di infinite coppie di primi gemelli; dovrebbe essere quindi espressa nella forma: $(\forall n)(\exists p)[\Pr(p) \wedge \Pr(p+2) \wedge (p>n)]$ (dove $\Pr(m)$ significa "m è primo").

Per considerare la Congettura di Goldbach in $Z^*[x]$ dobbiamo tenere presente che si tratta di una congettura in cui è presente un quantificatore universale[6]: ci occuperemo dunque del solo caso di polinomi non costanti.

Proposizione. Per ogni polinomio non costante e non primitivo $Q(x)$ di $Z^*[x]$ esistono due polinomi primi in $Z^*[x]$ tali che la loro somma sia $Q(x)$.

Dimostrazione. Consideriamo un polinomio non costante e non primitivo di $Z^*[x]$ (dove pq è il massimo comune divisore dei suoi coefficienti e p è primo):

$$Q(x) = pqa_n x^n + pqa_{n-1} x^{n-1} + ... + pqa_1 x + pqa_0$$

Sia $t \in \mathbf{Z}$; consideriamo i polinomi di $Z^*[x]$:

$$Q_1(x) = x^n + pqa_{n-1} x^{n-1} + ... + pqa_1 x - p(pt+1)$$
$$Q_2(x) = (pqa_n - 1)x^n + p(qa_0 + pt + 1)$$

la cui somma è $Q(x)$ per ogni valore di t. Proveremo che è possibile scegliere t in modo che entrambi i polinomi $Q_1(x)$ e $Q_2(x)$ siano primi.

Per ogni valore di t, $Q_1(x)$ è irriducibile per il criterio di Eisenstein in quanto il primo p ne divide tutti i coefficienti ad eccezione del coefficiente direttivo e p^2 non ne divide il termine noto (Piacentini Cattaneo, 1996, pp. 126-127); $Q_1(x)$ è monico, dunque primitivo ed è primo.

Se non è $qa_0 \equiv -1 \pmod{p}$ allora $qa_0 + pt + 1$ non è un multiplo di p e il criterio di Eisenstein può essere applicato anche a $Q_2(x)$ che è dunque irriducibile per ogni t. Verifichiamo la primitività di $Q_2(x)$ per opportuni valori di t: $(qa_0+1)+pt$ assume valori primi per infiniti valori di t in base al teorema di Dirichlet (qa_0+1 e p sono coprimi) e t può essere scelto in modo che $qa_0 + pt + 1$ sia primo e maggiore di $pqa_n - 1$.

Se invece $qa_0 \equiv -1 \pmod{p}$, dunque $qa_0 = kp - 1$ con k intero, risulta:

$$Q_2(x) = (pqa_n - 1)x^n + p^2(k+t)$$

Esistono infiniti valori di t in modo che $k+t$ sia primo e maggiore di $pqa_n - 1$: allora è possibile scegliere t in modo che $Q_2(x)$ sia irriducibile per il criterio di

[6] A rigore, la congettura di Goldbach non contiene solamente un quantificatore universale, in quanto afferma che per ogni naturale pari n, maggiore di 2, esiste una coppia di primi (p, q) tali che $p+q = n$ e dunque contiene anche due quantificatori esistenziali: tuttavia se n è un naturale anche p e q lo sono.

Eisenstein (il primo $k+t$ non divide pqa_n-1, divide $p^2(k+t)$ e $(k+t)^2$ non divide $p^2(k+t)$) e primitivo. ν

Dalla proposizione precedente per $p = 2$ segue che se la Congettura di Goldbach fosse verificata nell'insieme dei naturali, essa sarebbe anche verificata in $Z^*[x]$, ove si intenda per polinomio *pari* un polinomio il cui contenuto (il massimo comune divisore dei coefficienti) è pari; ribadiamo che la proposizione precedente *non* prova la Congettura di Goldbach in tutto l'insieme $Z^*[x]$[7].

[7] A proposito della teoria additiva dei numeri, segnaliamo che in $Z^*[x]$ è possibile provare il teorema di Shrinel'man (Nathanson, 1996, p. 177) nella forma seguente: ogni elemento di $Z^*[x]$ diverso da 0 e da 1 può essere espresso come la somma di una quantità limitata di primi di $Z^*[x]$.