Purezza e semplicità nel XXIV problema di Hilbert

Filosofia della matematica del 900
Accademia dei Lincei, 4-5 aprile 2024

Gabriele Pulcini, Dipartimento di Studi letterari, filosofici e di Storia dll'arte
Università di Roma Tor Vergata
gabriele.pulcini@uniroma2.it

Argomenti trattati

- Descrizione del XXIV problema
- Purezza come precondizione per valutare la semplicità
- Euclide IX-20 come caso studio
- Lo strumento della matematica formalizzata
- Conclusioni

Il XXIV problema di Hilbert

Ma non erano 23?

- Il matematico tedesco David Hilbert presenta 23 problemi al *Secondo congresso internazionale dei matematici* tenutosi a Parigi nell'agosto del 1900.

- Tra questi problemi, il problema di Cantor della potenza del continuo (1), la non contraddittorietà degli assiomi aritmetici (2), trattazione matematica degli assiomi della fisica (6), decisione della risolubilità di un'equazione diofantea (10).

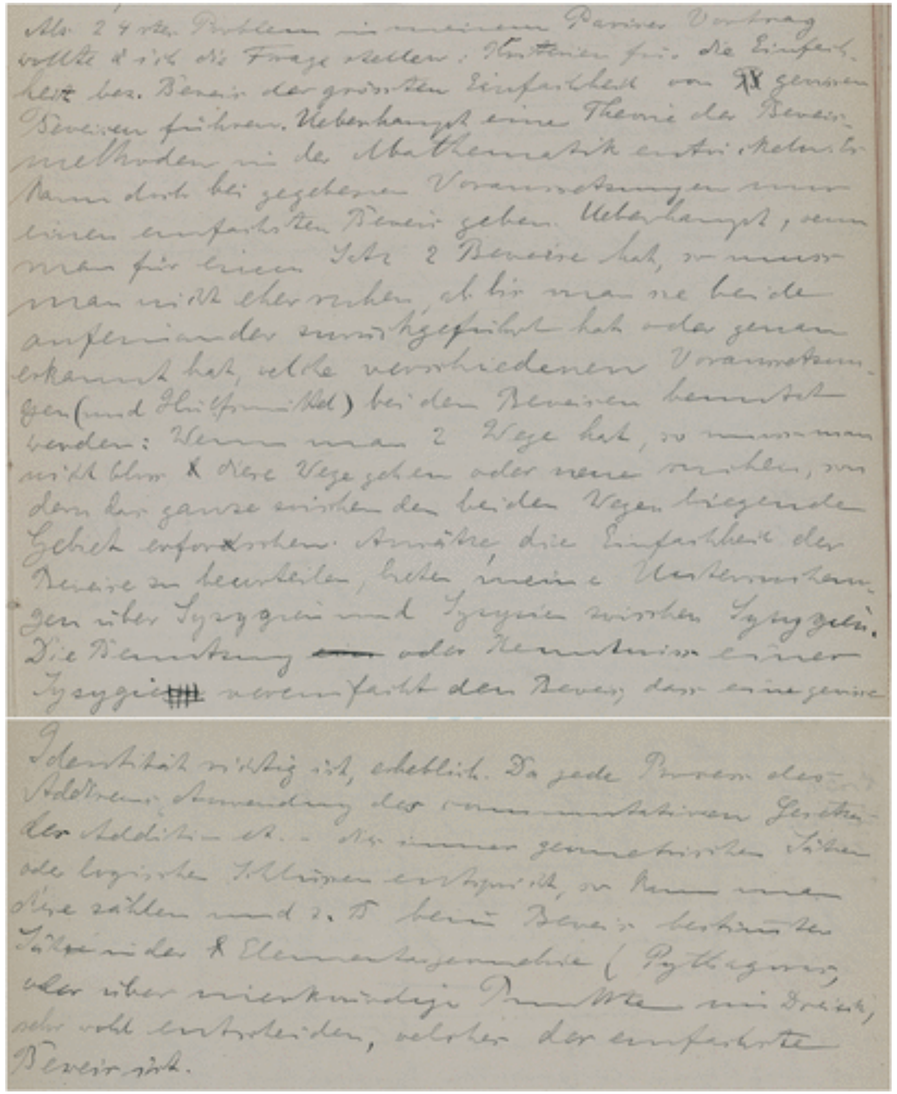
- **Assenti illustri**: l'ultimo teorema di Fermat ("*abbastanza particolare e apparentemente insignificante*") (10), il problema dei tre corpi (6).

David Hilbert, 1862-1943

“A Sleeping Beauty”

Rüdiger Thiele, **Hilbert’s Twenty-Fourth Problem**
American Math. Monthly 2003

Criteri di semplicità o dimostrazioni del fatto che certe dimostrazioni sono le più semplici. Sviluppare una teoria generale del metodo dimostrativo in matematica. Sotto determinate condizioni, non può esserci che una dimostrazione più semplice di tutte le altre. Più in generale, date due dimostrazioni di uno stesso teorema, bisognerebbe andare avanti fino a che non si riesce a derivare una dimostrazione dell’altra o finché non risulti del tutto evidente quali condizioni (e aiuti) sono stati utilizzati nelle due dimostrazioni. Date due vie, non è corretto scegliere una di queste o cercarne una terza; è necessario indagare l’area sottostante compresa tra i due percorsi […]



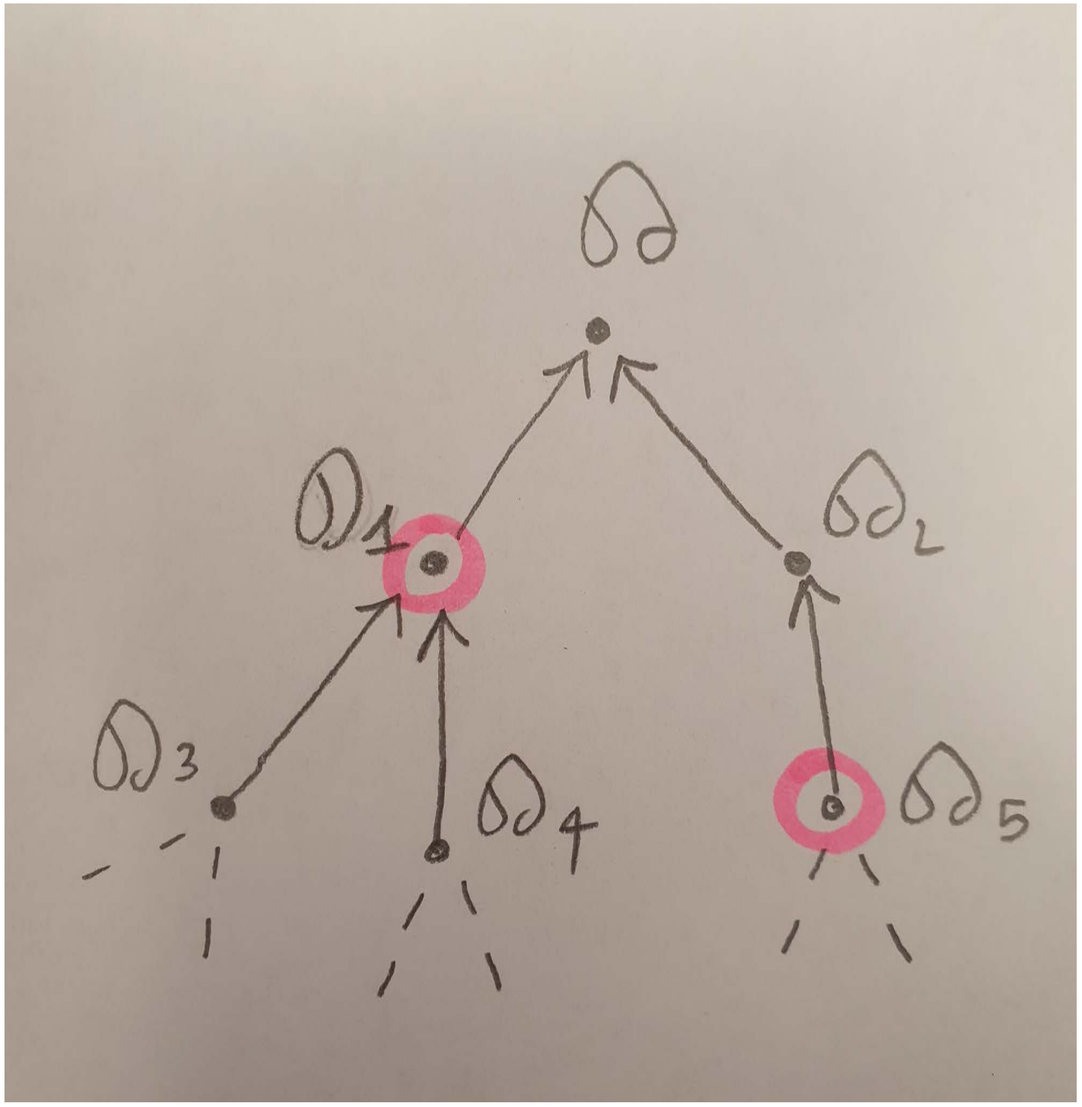
Dal *Nachlass* di Hilbert a Göttingen

Un problema di confine

- Filosofia (semplicità / purezza dei metodi / capacità esplicativa)
- Matematica (metamatematica, analisi della morfologia dell'oggetto-dimostrazione)
- Informatica teorica (isomorfismo di Curry-Howard, identità delle dimostrazioni-algoritmi)

Semplicità e identità

- Spesso il XXIV problema viene identificato con quello dell'identità delle dimostrazioni
- Problema di determinare quando due programmi/dimostrazioni determinano, di fatto, lo stesso algoritmo.
- Questo dipende dall'assunzione non del tutto banale che $\mathscr{D}_1 \rhd \mathscr{D}_2$ e $\mathscr{D}_2 \rhd \mathscr{D}_1$ implica $\mathscr{D}_1 = \mathscr{D}_2$



Mathematische Probleme, 1900

[…] *è un errore credere che il rigore nella conduzione della dimostrazione sia nemico della semplicità. Al contrario, numerosi esempi ci confermano che i metodi rigorosi sono anche i più semplici e i più facili da cogliere. Lo sforzo verso il rigore ci costringe appunto a trovare metodi più semplici di argomentazione: spesso ci apre la via anche a metodi che sono più passibili di sviluppo rispetto a quelli vecchi e meno rigorosi.*

In Hilbert's approach to mathematics, simplicity and rigor go hand in hand.

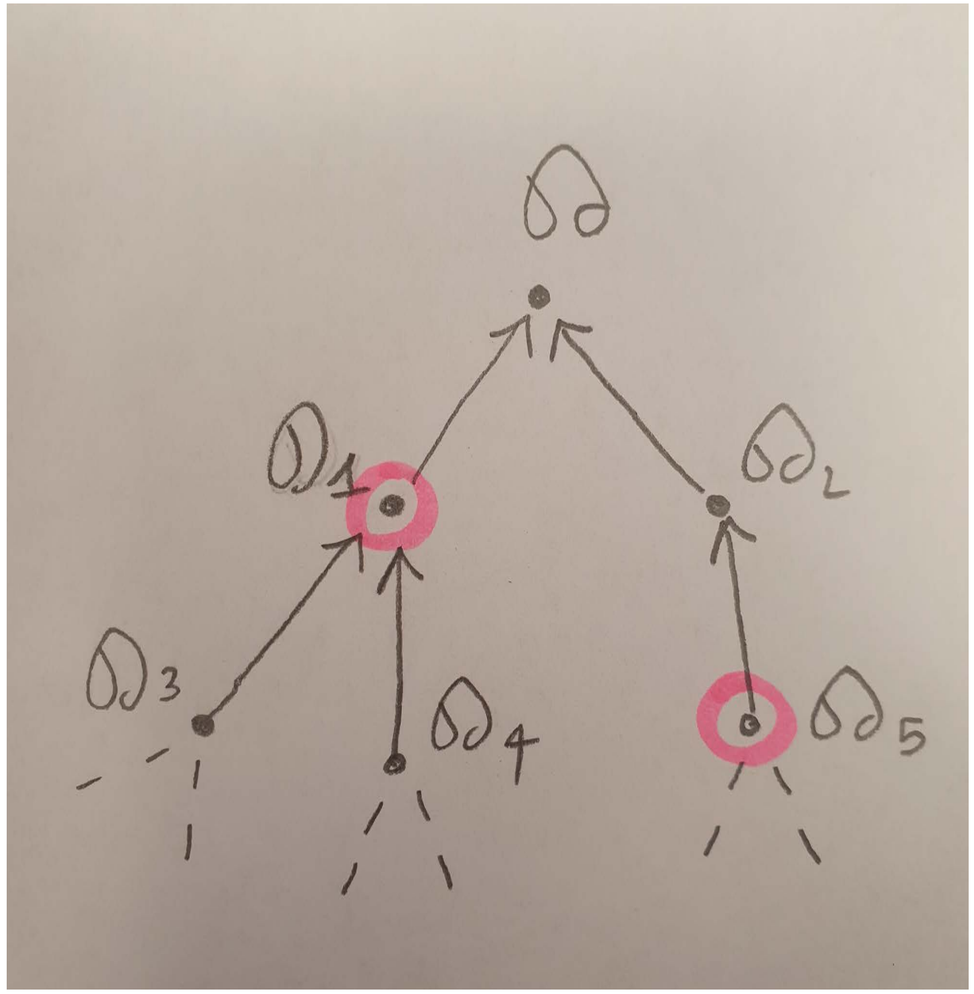
H. Weyl, *David Hilbert and his Mathematical Work* (Hilbert's Obituary)

Axiomatisches Denken, 1918

[…] *Ad una più approfondita riflessione, ci accorgiamo presto che la questione della non-contraddittorietà per i numeri naturali e per gli insiemi non è una questione isolata, ma appartiene a un grande ambito di questioni gnoseologiche fra le più difficili aventi tonalità specificamente matematiche: al fine di caratterizzare brevemente questo ambito di questioni, cito la questione della risolubilità in linea di principio di ogni problema matematico, la questione della controllabilità a posteriori del risultato di una ricerca matematica, e inoltre la questione relativa ad un criterio di semplicità per le dimostrazioni matematiche, la questione del rapporto tra contenutisticità e formalismo in matematica e in logica, e infine la questione della decidibilità di un problema matematico mediante un numero finito di operazioni.*

Axiomatisches Denken, 1918

Ma osservando criticamente queste “dimostrazioni” ci si può rendere conto che esse in se stesse non sono dimostrazioni bensì, in sostanza, esse rendono possibile soltanto la riconduzione a teoremi più profondi che, a loro volta, possono essere riguardati come nuovi assiomi al posto dei teoremi da dimostrare. In questo modo sono sorti quelli che oggi vengono detti propriamente assiomi della geometria, dell’aritmetica, della statica, della meccanica, della teoria dell’irraggiamento e della termodinamica.



Alcune osservazioni generali

- Dal 1900 al 1918 i **criteri** (plurale) di semplicità sono diventati un unico **criterio** (singolare)
- La ricerca della semplicità viene intesa come **fattore unificante** tra le varie discipline matematiche
- Il **rigore matematico** non ostacola, piuttosto spinge verso la semplificazione delle dimostrazioni
- Forte spinta verso la messa a punto di una **teoria della dimostrazione**, cioè una teoria matematica (**metamatematica**) i cui oggetti d'indagine sono le dimostrazioni stesse
- La teoria della dimostrazione trasforma una nozione **estetica** e **soggettiva** come quella di semplicità in una nozione **matematica** e **intersoggettiva**

Purezza e semplicità

Purezza come “determinata condizione”

Criteri si semplicità o dimostrazioni del fatto che certe dimostrazioni sono le più semplici. Sviluppare una teoria generale del metodo dimostrativo in matematica. Sotto determinate condizioni, non può esserci che una dimostrazione più semplice di tutte le altre. Più in generale, date due dimostrazioni di uno stesso teorema, bisognerebbe andare avanti fino a che non si riesce a derivare una dimostrazione dell’altra o finché non risulti del tutto evidente quali condizioni (e aiuti) sono stati utilizzati nelle due dimostrazioni. Date due vie, non è corretto scegliere una di queste o cercarne una terza; è necessario indagare l’area sottostante compresa tra i due percorsi […]

Una dimostrazione $\mathscr{D}$ si dice pura rispetto al teorema dimostrato $\mathscr{T}$ quando gli strumenti matematici utilizzati in $\mathscr{D}$ non trascendono l’ambito matematico a cui $\mathscr{T}$ si riferisce.

Dimostrazioni pure *vs* impure

- *Ogni numero primo della forma* $4n + 1$ *può essere scritto come la somma di due quadrati, cioè* $4n + 1 = a^2 + b^2$

  Dimostrazione di Eulero (1752) - Dimostrazioni che includono elementi immaginari

- *Ultimo teorema di Fermat: non esistono soluzioni intere positive per l'equazione* $a^z + b^z = c^z$*, con* $z \geqslant 3$

  Pierre de Fermat, Nota a margine sulle *Osservazioni su Diofanto* (?) -
  Dimostrazione di Wiles (curve ellittiche, rappresentazioni di Galois, etc)

- *Teorema di Desargues* che parla di una proprietà dei triangoli sul piano (2D), ma la sua dimostrazione ha bisogno di costruzioni che si articolano nello spazio (3D)

- Dimostrazione topologica del fatto che i numeri primi sono infiniti (Fürstenberg, 1955)

Contro la *metabasis*

Aristotele, *Secondi Analitici*

Non è dunque possibile condurre la dimostrazione, passando da un genere a un altro: ad esempio, non si può dimostrare una proposizione geometrica mediante l'aritmetica. **75a**, 35-40

[…] *d'altro lato, quando le scienze sono differenti per il genere, come avviene all'aritmetica e alla geometria, non è possibile adattare per esempio la dimostrazione aritmetica alle determinazioni delle grandezze spaziali, a meno che tali grandezze non siano numeri.* **75b**, 1-5

Due aspetti della purezza

Dimostrazioni ontologicamente impure

Teoremi di teoria elementare dei numeri dimostrati facendo ricorso a enti matematici estranei all'ambito di $\mathbb{Q}$: numeri immaginari, reali, transfiniti, curve ellittiche, etc.

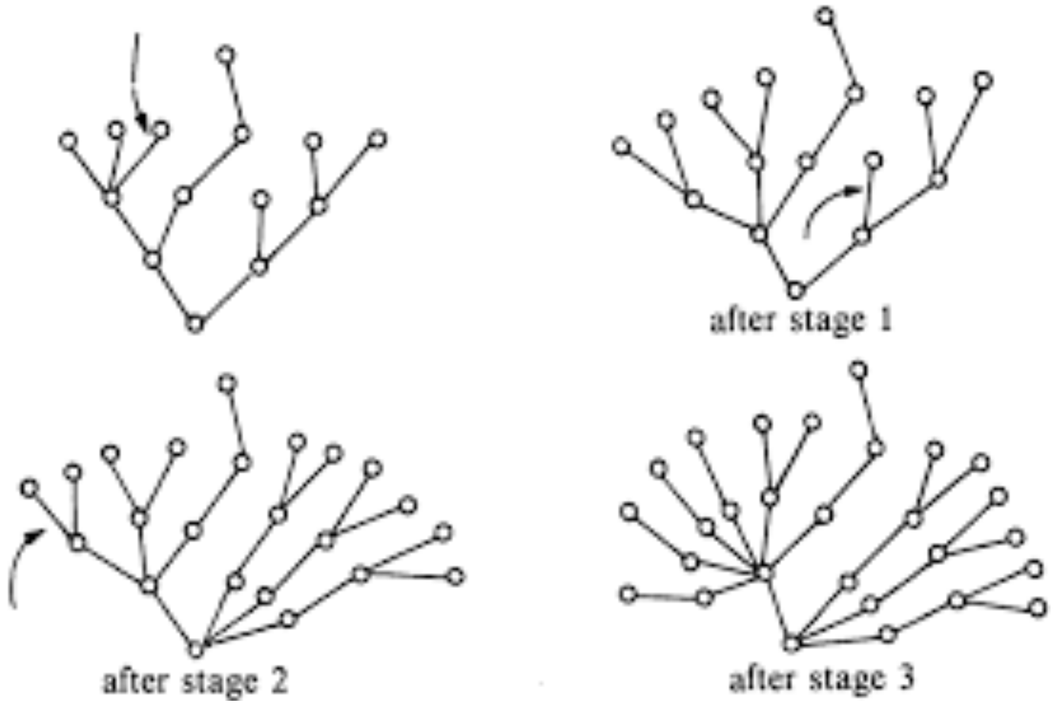
Dimostrazioni epistemicamente impure

- Teoremi di geometria piana dimostrati attraverso costruzioni spaziali
- Uso dell'infinito attuale per giustificare proprietà strettamente finitarie, ad esempio l'impiego di principi infinitari per dimostrare proprietà di combinatoria finita (es. gioco dell'idra)

Il gioco dell'Idra

J. Paris e L. Kirby, *Accessible Independence Results for Peano Arithmetic*, 1982

- Impurità ontologica: dimostrazione che fa uso della **notazione ordinale** e, conseguentemente, dell'induzione transfinita.
- Impurità epistemica: dimostrazione che combina l'induzione standard con il **Lemma di König**



Hilbert sulla purezza

Mathematische Probleme, 1900

Ci soffermiamo ancora, brevemente, sui requisiti generali che legittimamente vanno posti alla soluzione di un problema matematico. Penso innanzi tutto a questo: si deve riuscire a far vedere la correttezza della risposta mediante un numero finito di inferenze e precisamente in base a un numero finito di ipotesi che si trovano nella presentazione del problema [in der Problemstellung liegen] *e che ogni volta vanno formulate con esattezza.*

Matematica reale e matematica ideale

Matematica reale (ragionamento strettamente finalistico)

Tutta quella parte di matematica che può essere ricondotta a all'utilizzo procedure effettive e, più in generale, a situazioni riguardanti la combinatoria finita

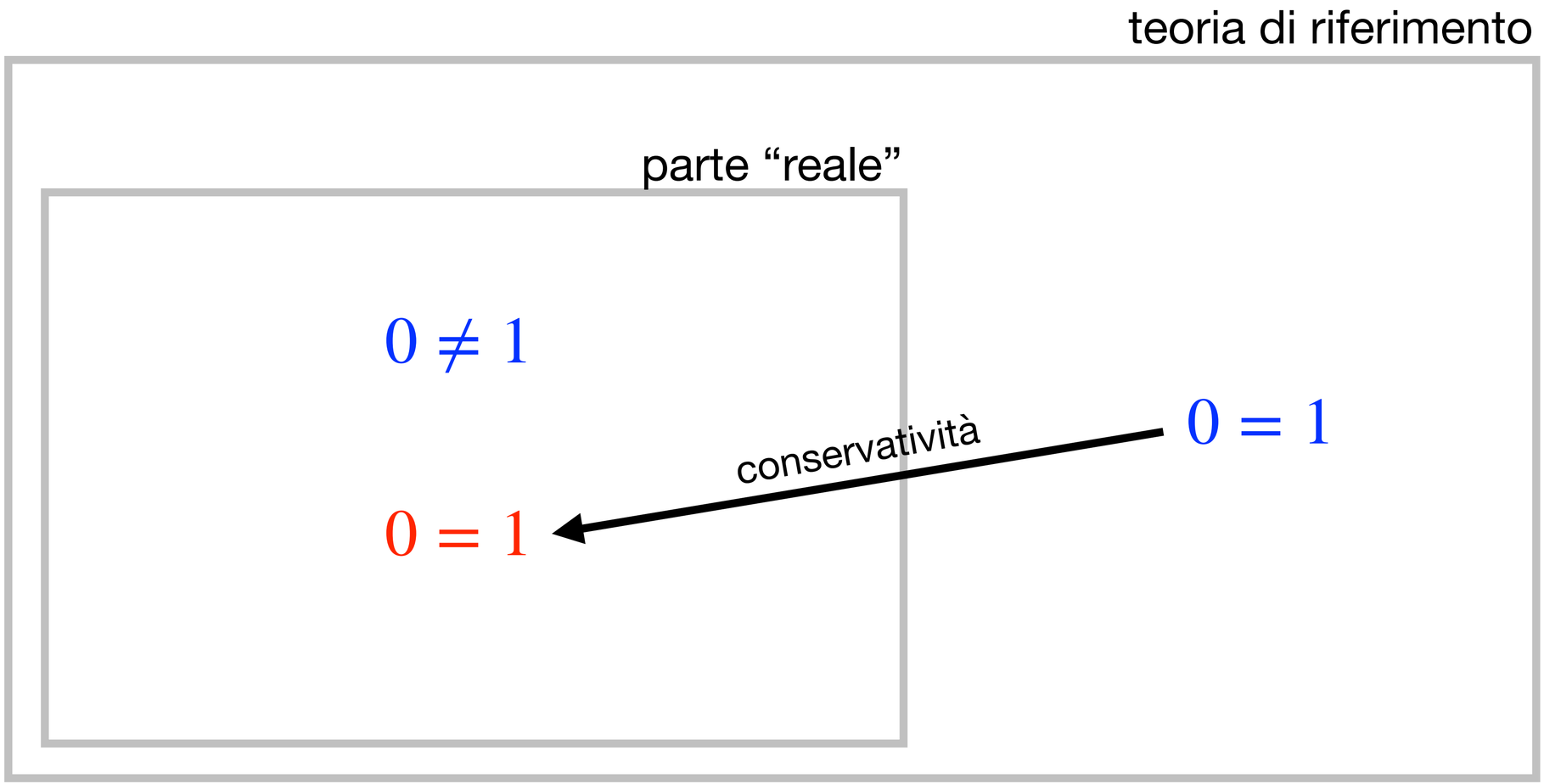
Matematica ideale (ragionamento astratto)

La parte rimanente della matematica, quella che non può essere ricondotta a situazioni strettamente algoritmiche o di combinatoria finita (ad esempio le dimostrazioni che fanno uso dell'infinito attuale) e che viene manipolata attraverso procedure astratte

Coerenza

L'enunciato di coerenza "non esiste alcuna dimostrazione che termini per $0 = 1$" ha una natura finitistica, perché le dimostrazioni (in un sistema formalizzato sono oggetti finiti)

conservatività ⇒ coerenza



Euclide IX-20 come caso di studio

Elementi, IX-20

Esistono* [*sempre*] *numeri primi in numero maggiore di quanti primi si voglia proporre.

- Siano i numeri primi ‘limitati’, diciamo $\{p_1, \ldots, p_n\}$
- Consideriamo poi $k = p_1 p_2 \cdots p_n + 1$
- Il numero k sarà allora o **primo** o **composto** [Elementi, VII-31]
- Se è primo, la dimostrazione è terminata perché $k \notin \{p_1, \ldots, p_n\}$
- Se è composto, esisterà un primo $p \mid k$
- Se $p \mid p_1 p_2 \cdots p_n$ allora $p \nmid p_1 p_2 \cdots p_n + 1$ (infatti, $k \equiv 1 \pmod{p}$)
- Da questo possiamo concludere che $p \notin \{p_1, \ldots, p_n\}$

Dimostrazione per induzione

Se $\mathbb{P}$ ha un sottoinsieme $\mathbb{P}_n$ di cardinalità n, allora ha anche un sottoinsieme $\mathbb{P}_{n+1}$ di cardinalità $n+1$

- *Base* $\mathbb{P}_1 = \{2\}$ e $\mathbb{P}_1 \subseteq \mathbb{P}$
- *Passo induttivo* Sia $\mathbb{P}_n = \{p_1, \ldots, p_n\} \subseteq \mathbb{P}$

  Si consideri $k = p_1 p_2 \cdots p_n + 1$, chiaramente $k \notin \mathbb{P}_n$

  Seguendo il ragionamento di Euclide si arriva a concludere che $k \in \mathbb{P}$ e

  allora possiamo porre $\mathbb{P}_{n+1} = \mathbb{P}_n \cup \{k\}$ oppure esiste un $p \in \mathbb{P} \backslash \mathbb{P}_n$ e allora

  sarà sufficiente porre $\mathbb{P}_{n+1} = \mathbb{P}_n \cup \{p\}$

Elementi, VII-31

Ogni numero composto ha per divisore un numero primo

- Sia k composto, ma non divisibile per un primo
- Ci sarà allora un k_1 tale che $k_1 \mid k$ con $k_1 < k$
- k_1 sarà a sua volta composto ma non divisibile per un primo (altrimenti k sarebbe divisibile per un primo), diciamo $k_2 \mid k_1$ con $k_2 < k_1$
- k_2 sarà ancora composto, ma non divisibile per un primo: $k_3 \mid k_2$ con $k_3 < k_2$
- Avremo allora la seguente **catena discendente arbitrariamente estendibile**:

$$0 < \cdots < k_3 < k_2 < k_1 < k$$

Dimostrazione per discesa

Se $\mathbb{P}$ fosse finito, allora nel segmento $[0, n]$ di $\mathbb{N}$ giacerebbero più di n numeri naturali

- Si assuma per assurdo che $\mathbb{P} = \{p_1, \ldots, p_n\}$
- Si consideri ancora $k = p_1 p_2 \cdots p_n + 1$ e si osservi che, per ogni $p_i \in \mathbb{P}$, abbiamo che $p_i \nmid k$ (infatti $k \equiv 1 \pmod{p}$)
- Per ipotesi, $k \notin \mathbb{P}$ quindi k sarà un numero composto, diciamo $k = k_1 q_1$ con $0 < k_1 < k$
- Ancora, k_1 sarà un numero composto (se fosse primo, dividerebbe anche k), diciamo $k_1 = k_2 q_2$ con $0 < k_2 < k_1$
- Reiterando: $0 < \cdots < k_n < k_{n-1} < \cdots < k_2 < k_1 < k$

Altre applicazioni della procedura di Euclide

Esistono infiniti numeri primi della forma $4n-1$

- Supponiamo per assurdo che siano finiti $\mathbb{P}' = \{4k_1 - 1, 4k_2 - 1, \ldots, 4k_n - 1\}$
- Sia $k = 4(4k_1 - 1)(4k_2 - 1)\cdots(4k_n - 1) - 1$, chiaramente $k \notin \mathbb{P}'$
- Se k è primo, allora abbiamo finito. Altrimenti k sarà composto e tutti i suoi fattori saranno dispari.
- Ogni dispari può essere della forma $4n+1$ oppure $4n-1$
- Siccome il prodotto di due numeri della forma $4n+1$ dà ancora un numero della forma $4n+1$, sarà necessario che k abbia almeno un fattore primo k' della forma $4n-1$
- Chiaramente k' è primo, ma $k' \notin \mathbb{P}'$

Dimostrazione topologica

H. Fürstenberg, *On the infinitude of primes*. Amer. Math Mon. 1955

- Dati $a, b \in \mathbb{N}$ con $a \leqslant b \leqslant 0$, sia $S(a,b) = \{ax + b \,|\, x \in \mathbb{N}\}$
- Si può anche scrivere $S(a,b) = \{x \equiv b \,[\mathrm{mod}\, a]\}$
  - Esempio: $S(3,2) = \{2,5,8,\ldots\}$
- Sia adesso $\mathscr{B}$ il più piccolo insieme di sottoinsiemi di $\mathbb{N}$ tale che:
  - $\emptyset \in \mathscr{B}$
  - $A \in \mathscr{B}$ esattamente quando la seguente condizione è soddisfatta:
    se $a \in A \Rightarrow \exists b$ tale che $S(a,b) \subseteq A$
- Osservazione: preso un qualsiasi elemento di $\mathscr{B}$ questo è o l'insieme **vuoto** o è **infinito**.

Dimostrazione topologica

H. Fürstenberg, *On the infinitude of primes*. Amer. Math Mon. 1955

Teorema. $\mathscr{B}$ costituisce una topologia su $\mathbb{N}$

In particolare, abbiamo che:

1. Per qualsiasi coppia $a, b \in \mathbb{N}$: $S(a,b) \in \mathscr{B}$ e $S(a,b)$ è un **aperto**
2. $S(a,b) = \mathbb{N} - \big((S(a,0) \cup \cdots \cup S(a,a-1)) - S(a,b)\big)$

   aperto
3. L'unione di aperti è ancora un **aperto**
4. Essendo il complemento di un aperto, ogni $S(a,b)$ sarà anche **chiuso**

Dimostrazione topologica

H. Fürstenberg, *On the infinitude of primes*. Amer. Math Mon. 1955

- Assumiamo che i primi siano finiti $\{p_1, p_2, \ldots, p_n\}$
- Si consideri poi $S = S(p_1,0) \cup S(p_2,0) \cup \cdots \cup S(p_n,0)$
- Abbiamo quindi $\mathbb{N} - S = \{1\}$
- L'unione finita di chiusi è un chiuso, quindi S è **chiuso**
- Il singoletto $\{1\}$ è il complemento di un chiuso, quindi un **aperto**
- Il singoletto $\{1\}$ dovrebbe essere allo stesso tempo **finito** e **infinito**!

Alcuni risultati preliminari

I. D. Mercer. *On Fürstenberg's proof of the infinitude of primes*. Amer. Math Mon. 2009

Lemma 1. Ogni intersezione finita $S(a_1, b_1) \cap \cdots \cap S(a_n, b_n)$ è o vuota o infinita.

Dim. Semplice proprietà di aritmetica modulare. Si consideri mcm$(a_1, \ldots, a_n)$ …

Lemma 2. Ogni intersezione finita di unioni finite può essere espressa come unione finita di intersezioni finite.

Dim. $(A \cup B) \cap (C \cup D) = (A \cap C) \cup (A \cap D) \cup (A \cap D) \cup (B \cap D)$

Dimostrazione topologica senza topologia

I. D. Mercer. *On Fürstenberg's proof of the infinitude of primes*. Amer. Math Mon. 2009

- Sia $NM(m) = S(m,1) \cup S(m,2) \cup \cdots \cup S(m, m-1)$
- Assumiamo poi che ci sia un numero finito di primi $\{p_1, \ldots, p_n\}$
- Avremo $NMP = NM(p_1) \cap NM(p_2) \cap \cdots \cap NM(p_k) = \{1\}$
  (intersezione finita di unioni finite)
- Si applichi il Lemma 2, per riscrivere NMP come l'unione finita di intersezioni finite ciascuna delle quali sarà **vuota** oppure **infinita** (Lemma 1).
- Il singoletto $\{1\}$ dovrebbe essere allo stesso tempo **vuoto** e **infinito**!

Dimostrazione topologica senza topologia

I. D. Mercer. *On Fürstenberg's proof of the infinitude of primes*. Amer. Math Mon. 2009

> *There is a particularly striking proof, due to Fürstenberg in 1955, that uses, of all things, topological language! In this note, we give a variant of Fürstenberg's proof that avoids topological language and thus, in the opinion of the current author, better exhibits the "real reason" that Furstenberg's approach works.*

- In che senso è possibile dire che nella dimostrazione di Fürstenberg è possibile **fare a meno dell'apparato topologico**?
- In che senso è possibile dire che la riduzione di Mercer è **più semplice** della dimostrazione originaria di Fürstenberg?

Dimostrazioni formalizzate

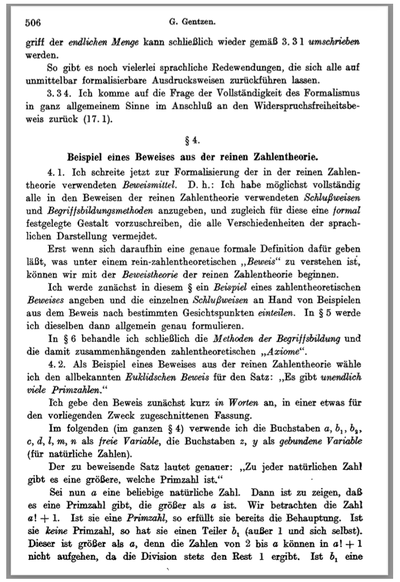
Euclide riletto da Gentzen

***Die Widerspruchsfreiheit der reinen Zahlentheorie* (1936)**

Esiste un numero primo più grande di qualsiasi numero naturale assegnato.

Il testo fornisce le istruzioni per formalizzare la dimostrazione, non è una dimostrazione formalizzata vera e propria.

Si tratta piuttosto di una “dimostrazione” del fatto che esiste una dimostrazione formalizzata per Euclide IX-20



506 G. Gentzen.

griff der *endlichen Menge* kann schließlich wieder gemäß 3. 3 1 *umschrieben* werden.

So gibt es noch vielerlei sprachliche Redewendungen, die sich alle auf unmittelbar formalisierbare Ausdrucksweisen zurückführen lassen.

3. 3 4. Ich komme auf die Frage der Vollständigkeit des Formalismus in ganz allgemeinem Sinne im Anschluß an den Widerspruchsfreiheitsbeweis zurück (17. 1).

§ 4.

Beispiel eines Beweises aus der reinen Zahlentheorie.

4. 1. Ich schreite jetzt zur Formalisierung der in der reinen Zahlentheorie verwendeten *Beweismittel*. D. h.: Ich habe möglichst vollständig alle in den Beweisen der reinen Zahlentheorie verwendeten *Schlußweisen* und *Begriffsbildungsmethoden* anzugeben, und zugleich für diese eine *formal* festgelegte Gestalt vorzuschreiben, die alle Verschiedenheiten der sprachlichen Darstellung vermeidet.

Erst wenn sich daraufhin eine genaue formale Definition dafür geben läßt, was unter einem rein-zahlentheoretischen „*Beweis*“ zu verstehen ist, können wir mit der *Beweistheorie* der reinen Zahlentheorie beginnen.

Ich werde zunächst in diesem § ein *Beispiel* eines zahlentheoretischen *Beweises* angeben und die einzelnen *Schlußweisen* an Hand von Beispielen aus dem Beweis nach bestimmten Gesichtspunkten *einteilen*. In § 5 werde ich dieselben dann allgemein genau formulieren.

In § 6 behandle ich schließlich die *Methoden der Begriffsbildung* und die damit zusammenhängenden zahlentheoretischen „*Axiome*“.

4. 2. Als Beispiel eines Beweises aus der reinen Zahlentheorie wähle ich den allbekannten *Euklidschen Beweis* für den Satz: „Es gibt *unendlich viele Primzahlen*.“

Ich gebe den Beweis zunächst kurz *in Worten* an, in einer etwas für den vorliegenden Zweck zugeschnittenen Fassung.

Im folgenden (im ganzen § 4) verwende ich die Buchstaben $a, b_1, b_2, c, d, l, m, n$ als *freie Variable*, die Buchstaben z, y als *gebundene Variable* (für natürliche Zahlen).

Der zu beweisende Satz lautet genauer: „Zu jeder natürlichen Zahl gibt es eine größere, welche Primzahl ist.“

Sei nun a eine beliebige natürliche Zahl. Dann ist zu zeigen, daß es eine Primzahl gibt, die größer als a ist. Wir betrachten die Zahl $a!+1$. Ist sie eine *Primzahl*, so erfüllt sie bereits die Behauptung. Ist sie *keine* Primzahl, so hat sie einen Teiler b_1 (außer 1 und sich selbst). Dieser ist größer als a, denn die Zahlen von 2 bis a können in $a!+1$ nicht aufgehen, da die Division stets den Rest 1 ergibt. Ist b_1 eine

Widerspruchsfreiheit der Zahlentheorie. 507

Primzahl, so erfüllt sie die Behauptung. Ist sie keine Primzahl, so hat sie ebenfalls einen Teiler b_2 außer 1 und sich selbst. Dieser geht auch in $a!+1$ auf, da b_1 darin aufgeht. Also ist b_2 ebenfalls größer als a. Durch dauernde Wiederholung dieses Gedankengangs erhalten wir eine Reihe von Zahlen: $a!+1, b_1, b_2, \ldots$, die immer kleiner werden. Die Reihe muß also irgendwann ein Ende nehmen, d. h. die letzte Zahl ist dann eine *Primzahl*, die Teiler von $a!+1$ und größer als a ist. Damit ist die Existenz einer Primzahl, die größer als a ist, nachgewiesen. Da a eine ganz *beliebige* natürliche Zahl war, so folgt: Zu *jeder* natürlichen Zahl gibt es eine größere, welche Primzahl ist. Das war zu zeigen.

4. 3. Ich habe bei dem Beweis verschiedene einfache Sätze als bereits *bekannt* vorausgesetzt. Diese könnte man durch weitere Beweise auf noch einfachere Tatsachen *zurückführen*, doch kommt es mir darauf jetzt nicht an, sondern vor allem auf *die Schlüsse*, die in dem gezeigten Beweisgang selbst auftreten.

Dabei ist zu berücksichtigen, daß wir durch Übung gewohnt sind, *ganze Schlußreihen auf einmal* durchzuführen, ohne daß wir uns noch jedes *einzelnen* darin enthaltenen Schlusses bewußt sind. Um also die eigentlichen *Elementarschlüsse* herauszufinden, will ich den Euklidschen Beweis jetzt noch einmal durchgehen und bei einigen Teilen des Beweises *alle darin enthaltenen Einzelschlüsse* ans Licht bringen. Zugleich werde ich die einzelnen nacheinander vorkommenden *Aussagen* gemäß § 3 *formalisieren*.

4. 4. *Ausführliche Zergliederung des Euklidschen Beweises.*

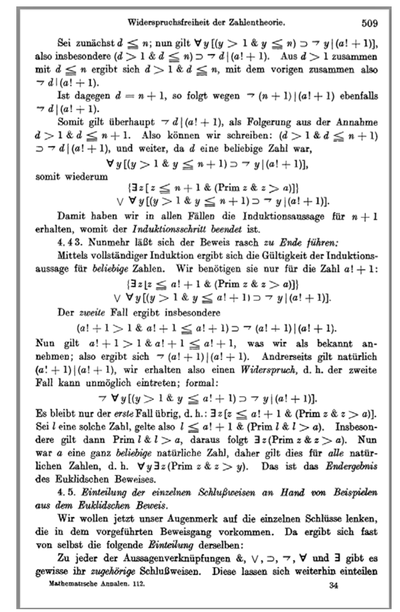
Der Beweis enthält, etwas versteckt, eine „vollständige Induktion“ (siehe die Stelle: „durch dauernde Wiederholung dieses Gedankengangs . . .“). Die übliche *Normalform* der Schlußweise durch vollständige Induktion ist diese: Man beweist die Gültigkeit einer Aussage für die Zahl 1; man zeigt ferner, daß die Aussage, wenn sie für eine beliebige natürliche Zahl n gilt, auch für $n+1$ gültig ist; alsdann gilt diese Aussage für jede beliebige natürliche Zahl.

Ich will auch die hier auftretende verkappte vollständige Induktion auf diese Normalform bringen; dazu wähle ich folgende Aussage als „Induktionsaussage“, für eine Zahl m ausgesprochen: „Entweder gibt es unter den Zahlen von 1 bis m eine Primzahl, die größer als a ist, oder alle diese Zahlen, außer 1, gehen nicht in $a!+1$ auf.“ Formal:

$$\{\exists z[z \leqq m \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]\} \vee \forall y[(y > 1 \,\&\, y \leqq m) \supset \neg\, y \mid (a!+1)].$$

Der Beweis verläuft nun so:

4. 4 1. Zunächst ist die Induktionsaussage für $m = 1$ zu beweisen. Hier ist ihr zweiter Teil ganz von selbst erfüllt, da es überhaupt keine Zahlen, die größer als 1 und kleiner oder gleich 1 sind, gibt. Ausführlich: Für beliebiges c gilt $\neg\,(c > 1 \,\&\, c \leqq 1)$; dies setzen wir als bekannt voraus.



Widerspruchsfreiheit der Zahlentheorie. 509

Sei zunächst $d \leqq n$; nun gilt $\forall y[(y > 1 \,\&\, y \leqq n) \supset \neg\, y \mid (a!+1)]$, also insbesondere $(d > 1 \,\&\, d \leqq n) \supset \neg\, d \mid (a!+1)$. Aus $d > 1$ zusammen mit $d \leqq n$ ergibt sich $d > 1 \,\&\, d \leqq n$, mit dem vorigen zusammen also $\neg\, d \mid (a!+1)$.

Ist dagegen $d = n+1$, so folgt wegen $\neg\,(n+1) \mid (a!+1)$ ebenfalls $\neg\, d \mid (a!+1)$.

Somit gilt überhaupt $\neg\, d \mid (a!+1)$, als Folgerung aus der Annahme $d > 1 \,\&\, d \leqq n+1$. Also können wir schreiben: $(d > 1 \,\&\, d \leqq n+1) \supset \neg\, d \mid (a!+1)$, und weiter, da d eine beliebige Zahl war,

$$\forall y[(y > 1 \,\&\, y \leqq n+1) \supset \neg\, y \mid (a!+1)],$$

somit wiederum

$$\{\exists z[z \leqq n+1 \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]\} \vee \forall y[(y > 1 \,\&\, y \leqq n+1) \supset \neg\, y \mid (a!+1)].$$

Damit haben wir in allen Fällen die Induktionsaussage für $n+1$ erhalten, womit der *Induktionsschritt beendet* ist.

4. 4 3. Nunmehr läßt sich der Beweis rasch *zu Ende führen:*

Mittels vollständiger Induktion ergibt sich die Gültigkeit der Induktionsaussage für *beliebige* Zahlen. Wir benötigen sie nur für die Zahl $a!+1$:

$$\{\exists z[z \leqq a!+1 \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]\} \vee \forall y[(y > 1 \,\&\, y \leqq a!+1) \supset \neg\, y \mid (a!+1)].$$

Der *zweite* Fall ergibt insbesondere

$$(a!+1 > 1 \,\&\, a!+1 \leqq a!+1) \supset \neg\,(a!+1) \mid (a!+1).$$

Nun gilt $a!+1 > 1 \,\&\, a!+1 \leqq a!+1$, was wir als bekannt annehmen; also ergibt sich $\neg\,(a!+1) \mid (a!+1)$. Andrerseits gilt natürlich $(a!+1) \mid (a!+1)$, wir erhalten also einen *Widerspruch*, d. h. der zweite Fall kann unmöglich eintreten; formal:

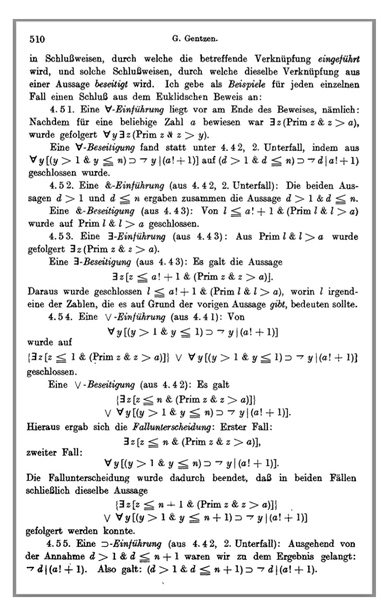
$$\neg\, \forall y[(y > 1 \,\&\, y \leqq a!+1) \supset \neg\, y \mid (a!+1)].$$

Es bleibt nur der *erste* Fall übrig, d. h.: $\exists z[z \leqq a!+1 \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]$. Sei l eine solche Zahl, gelte also $l \leqq a!+1 \,\&\, (\mathrm{Prim}\, l \,\&\, l > a)$. Insbesondere gilt dann $\mathrm{Prim}\, l \,\&\, l > a$, daraus folgt $\exists z(\mathrm{Prim}\, z \,\&\, z > a)$. Nun war a eine ganz *beliebige* natürliche Zahl, daher gilt dies für *alle* natürlichen Zahlen, d. h. $\forall y \exists z(\mathrm{Prim}\, z \,\&\, z > y)$. Das ist das *Endergebnis* des Euklidschen Beweises.

4. 5. *Einteilung der einzelnen Schlußweisen an Hand von Beispielen aus dem Euklidschen Beweis.*

Wir wollen jetzt unser Augenmerk auf die einzelnen Schlüsse lenken, die in dem vorgeführten Beweisgang vorkommen. Da ergibt sich fast von selbst die folgende *Einteilung* derselben:

Zu jeder der Aussagenverknüpfungen $\&, \vee, \supset, \neg, \forall$ und $\exists$ gibt es gewisse ihr *zugehörige* Schlußweisen. Diese lassen sich weiterhin einteilen



510 G. Gentzen.

in Schlußweisen, durch welche die betreffende Verknüpfung *eingeführt* wird, und solche Schlußweisen, durch welche dieselbe Verknüpfung aus einer Aussage *beseitigt* wird. Ich gebe als *Beispiele* für jeden einzelnen Fall einen Schluß aus dem Euklidschen Beweis an:

4. 5 1. Eine $\forall$-*Einführung* liegt vor am Ende des Beweises, nämlich: Nachdem für eine beliebige Zahl a bewiesen war $\exists z(\mathrm{Prim}\, z \,\&\, z > a)$, wurde gefolgert $\forall y \exists z(\mathrm{Prim}\, z \,\&\, z > y)$.

Eine $\forall$-*Beseitigung* fand statt unter 4. 4 2, 2. Unterfall, indem aus $\forall y[(y > 1 \,\&\, y \leqq n) \supset \neg\, y \mid (a!+1)]$ auf $(d > 1 \,\&\, d \leqq n) \supset \neg\, d \mid (a!+1)$ geschlossen wurde.

4. 5 2. Eine &-*Einführung* (aus 4. 4 2, 2. Unterfall): Die beiden Aussagen $d > 1$ und $d \leqq n$ ergaben zusammen die Aussage $d > 1 \,\&\, d \leqq n$.

Eine &-*Beseitigung* (aus 4. 4 3): Von $l \leqq a!+1 \,\&\, (\mathrm{Prim}\, l \,\&\, l > a)$ wurde auf $\mathrm{Prim}\, l \,\&\, l > a$ geschlossen.

4. 5 3. Eine $\exists$-*Einführung* (aus 4. 4 3): Aus $\mathrm{Prim}\, l \,\&\, l > a$ wurde gefolgert $\exists z(\mathrm{Prim}\, z \,\&\, z > a)$.

Eine $\exists$-*Beseitigung* (aus 4. 4 3): Es galt die Aussage

$$\exists z[z \leqq a!+1 \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)].$$

Daraus wurde geschlossen $l \leqq a!+1 \,\&\, (\mathrm{Prim}\, l \,\&\, l > a)$, worin l irgendeine der Zahlen, die es auf Grund der vorigen Aussage *gibt*, bedeuten sollte.

4. 5 4. Eine $\vee$-*Einführung* (aus 4. 4 1): Von

$$\forall y[(y > 1 \,\&\, y \leqq 1) \supset \neg\, y \mid (a!+1)]$$

wurde auf

$$\{\exists z[z \leqq 1 \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]\} \vee \forall y[(y > 1 \,\&\, y \leqq 1) \supset \neg\, y \mid (a!+1)]$$

geschlossen.

Eine $\vee$-*Beseitigung* (aus 4. 4 2): Es galt

$$\{\exists z[z \leqq n \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]\} \vee \forall y[(y > 1 \,\&\, y \leqq n) \supset \neg\, y \mid (a!+1)].$$

Hieraus ergab sich die *Fallunterscheidung*: Erster Fall:

$$\exists z[z \leqq n \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)],$$

zweiter Fall:

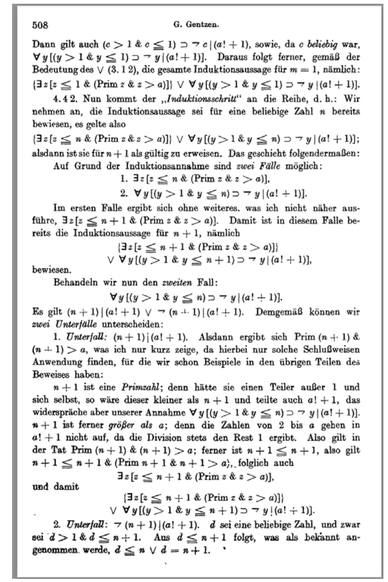
$$\forall y[(y > 1 \,\&\, y \leqq n) \supset \neg\, y \mid (a!+1)].$$

Die Fallunterscheidung wurde dadurch beendet, daß in beiden Fällen schließlich dieselbe Aussage

$$\{\exists z[z \leqq n+1 \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]\} \vee \forall y[(y > 1 \,\&\, y \leqq n+1) \supset \neg\, y \mid (a!+1)]$$

gefolgert werden konnte.

4. 5 5. Eine $\supset$-*Einführung* (aus 4. 4 2, 2. Unterfall): Ausgehend von der Annahme $d > 1 \,\&\, d \leqq n+1$ waren wir zu dem Ergebnis gelangt: $\neg\, d \mid (a!+1)$. Also galt: $(d > 1 \,\&\, d \leqq n+1) \supset \neg\, d \mid (a!+1)$.



508 G. Gentzen.

Dann gilt auch $(c > 1 \,\&\, c \leqq 1) \supset \neg\, c \mid (a!+1)$, sowie, da c *beliebig* war, $\forall y[(y > 1 \,\&\, y \leqq 1) \supset \neg\, y \mid (a!+1)]$. Daraus folgt ferner, gemäß der Bedeutung des $\vee$ (3. 1 2), die gesamte Induktionsaussage für $m = 1$, nämlich: $\{\exists z[z \leqq 1 \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]\} \vee \forall y[(y > 1 \,\&\, y \leqq 1) \supset \neg\, y \mid (a!+1)]$.

4. 4 2. Nun kommt der „*Induktionsschritt*“ an die Reihe, d. h.: Wir nehmen an, die Induktionsaussage sei für eine beliebige Zahl n bereits bewiesen, es gelte also

$$\{\exists z[z \leqq n \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]\} \vee \forall y[(y > 1 \,\&\, y \leqq n) \supset \neg\, y \mid (a!+1)];$$

alsdann ist sie für $n+1$ als gültig zu erweisen. Das geschieht folgendermaßen:

Auf Grund der Induktionsannahme sind *zwei Fälle* möglich:

1. $\exists z[z \leqq n \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]$,

2. $\forall y[(y > 1 \,\&\, y \leqq n) \supset \neg\, y \mid (a!+1)]$.

Im ersten Falle ergibt sich ohne weiteres, was ich nicht näher ausführe, $\exists z[z \leqq n+1 \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]$. Damit ist in diesem Falle bereits die Induktionsaussage für $n+1$, nämlich

$$\{\exists z[z \leqq n+1 \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]\} \vee \forall y[(y > 1 \,\&\, y \leqq n+1) \supset \neg\, y \mid (a!+1)],$$

bewiesen.

Behandeln wir nun den *zweiten* Fall:

$$\forall y[(y > 1 \,\&\, y \leqq n) \supset \neg\, y \mid (a!+1)].$$

Es gilt $(n+1) \mid (a!+1) \vee \neg\,(n+1) \mid (a!+1)$. Demgemäß können wir *zwei Unterfälle* unterscheiden:

1. *Unterfall:* $(n+1) \mid (a!+1)$. Alsdann ergibt sich $\mathrm{Prim}\,(n+1) \,\&\, (n+1) > a$, was ich nur kurz zeige, da hierbei nur solche Schlußweisen Anwendung finden, für die wir schon Beispiele in den übrigen Teilen des Beweises haben:

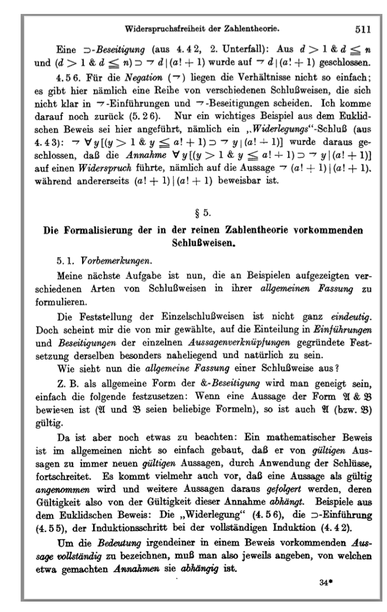
$n+1$ ist eine *Primzahl*; denn hätte sie einen Teiler außer 1 und sich selbst, so wäre dieser kleiner als $n+1$ und teilte auch $a!+1$, das widerspräche aber unserer Annahme $\forall y[(y > 1 \,\&\, y \leqq n) \supset \neg\, y \mid (a!+1)]$. $n+1$ ist ferner *größer als* a; denn die Zahlen von 2 bis a gehen in $a!+1$ nicht auf, da die Division stets den Rest 1 ergibt. Also gilt in der Tat $\mathrm{Prim}\,(n+1) \,\&\, (n+1) > a$; ferner ist $n+1 \leqq n+1$, also gilt $n+1 \leqq n+1 \,\&\, (\mathrm{Prim}\, n+1 \,\&\, n+1 > a)$, folglich auch

$$\exists z[z \leqq n+1 \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)],$$

und damit

$$\{\exists z[z \leqq n+1 \,\&\, (\mathrm{Prim}\, z \,\&\, z > a)]\} \vee \forall y[(y > 1 \,\&\, y \leqq n+1) \supset \neg\, y \mid (a!+1)].$$

2. *Unterfall:* $\neg\,(n+1) \mid (a!+1)$. d sei eine beliebige Zahl, und zwar sei $d > 1 \,\&\, d \leqq n+1$. Aus $d \leqq n+1$ folgt, was als bekannt angenommen werde, $d \leqq n \vee d = n+1$.



Widerspruchsfreiheit der Zahlentheorie. 511

Eine $\supset$-*Beseitigung* (aus 4. 4 2, 2. Unterfall): Aus $d > 1 \,\&\, d \leqq n$ und $(d > 1 \,\&\, d \leqq n) \supset \neg\, d \mid (a!+1)$ wurde auf $\neg\, d \mid (a!+1)$ geschlossen.

4. 5 6. Für die *Negation* ($\neg$) liegen die Verhältnisse nicht so einfach; es gibt hier nämlich eine Reihe von verschiedenen Schlußweisen, die sich nicht klar in $\neg$-Einführungen und $\neg$-Beseitigungen scheiden. Ich komme darauf noch zurück (5. 2 6). Nur ein wichtiges Beispiel aus dem Euklidschen Beweis sei hier angeführt, nämlich ein „*Widerlegungs*“-Schluß (aus 4. 4 3): $\neg\, \forall y[(y > 1 \,\&\, y \leqq a!+1) \supset \neg\, y \mid (a!+1)]$ wurde daraus geschlossen, daß die *Annahme* $\forall y[(y > 1 \,\&\, y \leqq a!+1) \supset \neg\, y \mid (a!+1)]$ auf einen *Widerspruch* führte, nämlich auf die Aussage $\neg\,(a!+1) \mid (a!+1)$, während andererseits $(a!+1) \mid (a!+1)$ beweisbar ist.

§ 5.

Die Formalisierung der in der reinen Zahlentheorie vorkommenden Schlußweisen.

5. 1. *Vorbemerkungen.*

Meine nächste Aufgabe ist nun, die an Beispielen aufgezeigten verschiedenen Arten von Schlußweisen in ihrer *allgemeinen Fassung* zu formulieren.

Die Feststellung der Einzelschlußweisen ist nicht ganz *eindeutig*. Doch scheint mir die von mir gewählte, auf die Einteilung in *Einführungen* und *Beseitigungen* der einzelnen *Aussagenverknüpfungen* gegründete Festsetzung derselben besonders naheliegend und natürlich zu sein.

Wie sieht nun die *allgemeine Fassung* einer Schlußweise aus?

Z. B. als allgemeine Form der &-*Beseitigung* wird man geneigt sein, einfach die folgende festzusetzen: Wenn eine Aussage der Form $\mathfrak{A} \,\&\, \mathfrak{B}$ bewiesen ist ($\mathfrak{A}$ und $\mathfrak{B}$ seien beliebige Formeln), so ist auch $\mathfrak{A}$ (bzw. $\mathfrak{B}$) gültig.

Da ist aber noch etwas zu beachten: Ein mathematischer Beweis ist im allgemeinen nicht so einfach gebaut, daß er von *gültigen* Aussagen zu immer neuen *gültigen* Aussagen, durch Anwendung der Schlüsse, fortschreitet. Es kommt vielmehr auch vor, daß eine Aussage als gültig *angenommen* wird und weitere Aussagen daraus *gefolgert* werden, deren Gültigkeit also von der Gültigkeit dieser Annahme *abhängt*. Beispiele aus dem Euklidschen Beweis: Die „Widerlegung“ (4. 5 6), die $\supset$-Einführung (4. 5 5), der Induktionsschritt bei der vollständigen Induktion (4. 4 2).

Um die *Bedeutung* irgendeiner in einem Beweis vorkommenden *Aussage vollständig* zu bezeichnen, muß man also jeweils angeben, von welchen etwa gemachten *Annahmen* sie *abhängig* ist.

Semplicità = Lunghezza delle dimostrazioni

$$\frac{[A]}{A \to A} \to \mathscr{E}$$

1. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ Ax
2. $A \to ((A \to A) \to A)$ Ax
3. $(A \to (A \to A)) \to (A \to A)$ MP 1, 2
4. $A \to (A \to A)$ Ax
4. $A \to A$ MP 3, 4

$$\dfrac{\dfrac{\dfrac{\dfrac{[A \to (B \to A)] \quad [A]}{B \to C} \qquad \dfrac{A \to B \quad A}{B}}{C}}{A \to C}}{(A \to B) \to (A \to C)}}{(A \to (B \to C)) \to ((A \to B) \to (A \to C))}$$

1. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$ Ax

Purezza come analiticità

G. Gentzen, 1936

$$\frac{A \Rightarrow \boxed{B} \qquad \boxed{B} \Rightarrow C}{A \Rightarrow C}\ \mathit{cut}$$

logica “pura” del prim’ordine

Cut-elimination. Tutte le dimostrazioni che presentano occorrenze della regola di cut possono essere riscritte in dimostrazioni in cui non ci sono applicazioni di cut (analitica).

Strong cut-elimination. Ogni dimostrazione con cut e assiomi matematici (non logici) può essere riscritta in una dimostrazione in cui le applicazioni di cut coinvolgono direttemente gli assiomi.

teorie matematiche formalizzate al prim’ordine

Subformula property. In una dimostrazione senza cut (analitica), tutte le formule sono sottoformule della formula finale.

Analiticità ⇒ coerenza

G. Gentzen, 1936

$$\frac{A \Rightarrow \boxed{B} \qquad \boxed{B} \Rightarrow C}{A \Rightarrow C}\ cut$$

La contraddizione può essere espressa tramite la seguente formula generale:

$$\emptyset \Rightarrow \emptyset$$

Non essendo un assioma, se fosse dimostrabile, tutte le formule che occorrono nella dimostrazione dovrebbero essere incluse anche in $\emptyset$ il che è chiaramente assurdo.

Don’t Eliminate Cut

George Boolos, 1984 (Journal of Philosophical Logic)

$$\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$$

$$\forall x (dx = x + x)$$

$$L1$$

$$\forall x (Lx \rightarrow Lx + 1)$$

There is a simple inference that can be shown valid by means of a deduction [with cuts/modus ponens] *whose every symbol can be written down in one or two pages of normally sized type or handwriting, but the smallest closed tree* [without cuts/modus ponens] *contains more symbols that there are nanoseconds between Big Bangs.*

Conclusioni

Dimostrazioni formalizzate *vs* dimostrazioni ordinarie

Sull'Atlantico gravava un'area di bassa pressione che, muovendosi verso oriente incontro a quella di alta pressione dislocata sulla Russia, non manifestava ancora alcuna tendenza a spostarsi verso nord per scansarla. Le isòtere e le isoterme facevano il loro dovere. La temperatura dell'aria era nella norma rispetto alla temperatura media annua, rispetto a quella del mese più fresco come a quella del mese più caldo e all'oscillazione mensile periodica della temperatura. Il sorgere e il tramontare del sole e della luna, le fasi lunari, quelle di Venere, dell'anello di Saturno e molti altri fenomeni rispettavano le previsioni degli annuari di astronomia. Nell'aria il vapore acqueo possedeva la massima elasticità e l'umidità era scarsa. Ovvero, con un'espressione che, quantunque un po' fuori moda, caratterizza benissimo quest'insieme di fatti: era una bella giornata d'agosto dell'anno 1913.

R. Musil, *L'uomo senza qualità* (1930-33)

Dimostrazioni formalizzate *vs* dimostrazioni ordinarie

Sull'Atlantico gravava un'area di bassa pressione che, muovendosi verso oriente incontro a quella di alta pressione dislocata sulla Russia, non manifestava ancora alcuna tendenza a spostarsi verso nord per scansarla. Le isòtere e le isoterme facevano il loro dovere. La temperatura dell'aria era nella norma rispetto alla temperatura media annua, rispetto a quella del mese più fresco come a quella del mese più caldo e all'oscillazione mensile periodica della temperatura. Il sorgere e il tramontare del sole e della luna, le fasi lunari, quelle di Venere, dell'anello di Saturno e molti altri fenomeni rispettavano le previsioni degli annuari di astronomia. Nell'aria il vapore acqueo possedeva la massima elasticità e l'umidità era scarsa. Ovvero, con un'espressione che, quantunque un po' fuori moda, caratterizza benissimo quest'insieme di fatti: era una bella giornata d'agosto dell'anno 1913.

R. Musil, *L'uomo senza qualità* (1930-33)

Dimostrazioni formalizzate *vs* dimostrazioni ordinarie

Sull'Atlantico gravava un'area di bassa pressione che, muovendosi verso oriente incontro a quella di alta pressione dislocata sulla Russia, non manifestava ancora alcuna tendenza a spostarsi verso nord per scansarla. Le isòtere e le isoterme facevano il loro dovere. La temperatura dell'aria era nella norma rispetto alla temperatura media annua, rispetto a quella del mese più fresco come a quella del mese più caldo e all'oscillazione mensile periodica della temperatura. Il sorgere e il tramontare del sole e della luna, le fasi lunari, quelle di Venere, dell'anello di Saturno e molti altri fenomeni rispettavano le previsioni degli annuari di astronomia. Nell'aria il vapore acqueo possedeva la massima elasticità e l'umidità era scarsa. Ovvero, con un'espressione che, quantunque un po' fuori moda, caratterizza benissimo quest'insieme di fatti: era una bella giornata d'agosto dell'anno 1913.

R. Musil, *L'uomo senza qualità* (1930-33)

Il XXIV è un buon problema?

Mathematische Probleme, 1900

La chiarezza e la facile esprimibilità, […] richieste così drasticamente per una teoria matematica, preferirei piuttosto esigerle da un problema matematico che voglia essere perfetto: infatti, ciò che è chiaro e facilmente esprimibile ci attrae, ciò che è intricato ci spaventa.

Inoltre, un problema matematico deve essere difficile perché possa eccitarci, e tuttavia non del tutto inaccessibile perché non irrida alle [sic] *nostre fatiche; deve essere per noi un segnale nei sentieri tortuosi verso le verità nascoste e ci deve ricompensare poi di gioia per la soluzione raggiunta.*

Le ragioni dell’esclusione

Carteggio con Hurwitz e Minkowski

- Hilbert non parla del XXIV problema durante la conferenza (presenta solo 10 problemi su 23) e non lo menziona esplicitamente neppure nel testo *Matematische Probleme*.

- Hilbert rimase incerto fino all’ultimo sull’opportunità di accettare l’invito alla conferenza e, dopo, sull’argomento da trattare (addirittura, il programma della conferenza apparve senza l’intervento di Hilbert).

- Nel 1900 Hilbert non aveva ancora un’idea precisa di come potesse configurarsi la sua ***Beweistheorie***. (NB I ***Principia Mathematica*** di Whitehead e Russell uscirono dal 1910 al 1913.)

I limiti imposti dallo strumentalismo

1. Il problema di Cantor della potenza del continuo
2. La non-contraddittorietà degli assiomi aritmetici

⋮

6. Trattazione matematica degli assiomi della fisica

⋮

10. Decisione della risulubilità di un’equazione diofantea

⋮

24. Criteri di semplicità per le dimostrazioni matematiche