

# DA CORTE SUPREMA, A MATEMÁTICA, À MATEMÁTICA NOS TRIBUNAIS

**Isabel Cafezeiro**

UFF

isabel@dcc.ic.uff.br

**Ivan da Costa Marques**

Professor do HCTE/UFRJ

imarques@ufrj.br

## **O supremo tribunal: a matemática**

Em 1900, o matemático David Hilbert lançou, no Segundo Congresso Internacional de Matemáticos, em Paris, um desafio aos matemáticos da época. Ele reuniu uma lista de 23 problemas em aberto, e convocou uma união de esforços para que se buscasse a solução daqueles problemas. Este episódio revela a têmpera dos movimentos de fundamentação da matemática que se desenrolaram em meados do século XIX, e se caracterizaram pelo esforço na busca da verdade matemática e da precisão e coerência dos métodos matemáticos:

“Basta pensar, as definições e os métodos dedutivos que todos aprendem, ensinam e usam em matemática, o paradigma da verdade e da certeza, levam a absurdos! Se o pensamento matemático é defeituoso, onde vamos encontrar a verdade e certeza? Há, no entanto, uma maneira completamente satisfatória de evitar os paradoxos sem trair nossa ciência. Os desejos e atitudes que nos ajudam a encontrar esse caminho e nos mostram que direção tomar são as seguintes: 1. Onde quer que haja alguma esperança de salvação, iremos investigar cuidadosamente definições fecundas e métodos dedutivos. Vamos nutri-los, fortalecê-los e torná-los úteis. Ninguém pode nos expulsar do paraíso que Cantor criou para nós. 2. Devemos estabelecer na matemática a mesma certeza para nossas deduções como há na teoria elementar dos números, da qual ninguém duvida e onde contradições e paradoxos surgem apenas pelo nosso próprio descuido.” (HILBERT, 1925)

Três anos depois, em Bolonha, 1928, no Congresso Internacional de Matemáticos, ele divulga o *Programa de Hilbert*, que propunha a formalização da matemática para garantir rigidez e solidez. A ideia geral era reduzir toda matemática a manipulações finitárias, ou seja, que pudessem ser completadas em tempo finito, envolvendo um número finito de passos, e responder afirmativamente as questões: 1) A matemática é completa, ou seja, a todo enunciado verdadeiro expresso no próprio sistema cabe uma prova formalizada no sistema? 2) É consistente, isto é, impossibilita a derivação do absurdo? 3) É decidível? A esta questão denominou-se "O Problema de Decisão de Hilbert" (*Hilbert's Entscheidungsproblem*): encontrar um mecanismo genérico e finitário que, ao considerar

um enunciado qualquer do sistema formal, no caso, a Lógica de Primeira Ordem, fosse capaz de verificar sua validade ou não. O Programa de Hilbert (abordagem formalista) estabelecia-se como uma forte opção, dentre outras abordagens de fundamentação da matemática.

Mas “[e]ntão veio a catástrofe: assumindo a consistência, K. Gödel mostrou como construir proposições aritméticas que eram evidentemente verdadeiras, embora não dedutíveis no formalismo”. Estas palavras de Weyl, publicadas em 1944 sob a comoção do falecimento de Hilbert (1943), nos dão a sensação de que desmantelava-se o sonho da matemática completamente segura e controlada. Porém, mesmo dentre os seguidores de Hilbert, havia opiniões menos pessimistas com relação ao futuro da matemática:

“Com a sua permissão, vou agora conduzi-lo ao assunto da presente situação da pesquisa sobre os fundamentos da matemática. Uma vez que persistem questões abertas neste campo, não estou em posição de pintar um retrato definitivo. Mas é necessário destacar que a situação não é tão crítica como se poderia pensar ao ouvir aqueles que falam de uma crise dos fundamentos. De alguns pontos de vista, esta expressão pode ser justificada; mas poderia gerar a opinião de que a ciência matemática está abalada até as raízes. A verdade é que as ciências matemáticas estão crescendo em completa segurança e harmonia.” (BERNAYS, 1935)

Ao introduzir a densa exposição matemática de *Über formal unentscheidbare sätze der Principia Mathematica und verwandter systeme*, Gödel situa o alcance de seus resultados:

“No que se vai seguir mostrar-se-á que (...) em ambos os sistemas citados [Principia Mathematica e Zermelo-Fraenkel], existem problemas relativamente simples da teoria dos números inteiros que não podem ser decididos com base nos axiomas. Esta situação não depende da natureza especial dos sistemas construídos mas aplica-se a uma *vasta classe de sistemas formais* (...)” (GÖDEL, 1931) (ênfase adicionada).

Assim, considerando o Programa Formalista em suas questões puramente matemáticas, vemos que o conflito com os resultados de Gödel se dá na medida em que Hilbert restringe a um único sistema formal (pertencente à tal vasta classe) a resolução de qualquer problema matemático. Podemos ver que, se tomarmos o Programa Formalista em sua dimensão sociotécnica, da qual fazem parte, em igual importância, a empolgação com que Hilbert o conduziu, o esforço de alistamento de matemáticos para aderirem às iniciativas do programa, a segurança que depositava nos métodos puramente dedutivos e o desconforto de perder o enquadramento tão bem arrumado que restringia a busca pela solução de todos os problemas enunciáveis no sistema formal ao próprio sistema formal, o termo “catástrofe” de Weyl se justifica: os Teoremas de Gödel abalaram a certeza do matemático de dominar toda a matemática. Desmantelou-se a convicção de Hilbert, que já chegava a considerar a matemática como um tribunal supremo: “A matemática tornou-se uma corte de arbitragem, um

tribunal supremo para decidir questões fundamentais – em uma base concreta sobre a qual todos podem concordar e onde cada instrução pode ser controlada.” (Hilbert, 1925)

### **A matemática nos tribunais**

No entanto, há evidências de que a matemática, se busca chegar aos tribunais como árbitro isolado, sem aliados, pouco ou quase nada decide. Theodore Porter aborda o prestígio e o poder dos métodos matemáticos, e argumenta que objetividade buscada nos números, nas técnicas, etc, justifica a desconsideração de questões locais. Ele argumenta que o discurso objetivo é globalizado, inquestionável e distante, e, embora se diga apoiado apenas sobre o que é científico, é comprometido com as condições de quem o enunciou.

(...) A quantificação é uma tecnologia da distância. Talvez, o mais crucial, a confiança nos números e a manipulação quantitativa minimiza a necessidade de conhecimento íntimo e confiança pessoal. Quantificação é bem adequada para comunicação que vai além dos limites da localidade e da comunidade. Um discurso altamente disciplinado ajuda a produzir conhecimento independente das pessoas particulares que a fazem.” (PORTER, 1995:ix)

Análises matemáticas, estatísticas, medidas, números, em geral, resultam de um processo de purificação especialmente orientado para produzir o conhecimento chamado “científico” que exige tipos especiais de investimentos para vencer sua resistência a ser desmantelado. O filósofo, imbricado nas disputas contemporâneas entre a epistemologia e a semiótica, problematiza a qualidade e a escala desses investimentos e como se constrói essa resistência (não esqueçamos de que o real é o que resiste) mas não o leigo. Para o senso comum, os números “despersonalizam”, tornam a análise (e a realidade) menos subjetiva, menos dependente de circunstâncias locais, livre de conhecimento tácito, e assim, quando matematizadas, as proposições e as argumentações parecem mais confiáveis. Uma seqüência lógica formal é geralmente considerada mais confiável do que qualquer argumento não formalizado. Uma prova matemática, mesmo que não compreendia, costuma ter o poder do convencimento: “Está provado que é assim!”. Porter comenta:

“'Objetividade' desperta as paixões como poucas palavras. Sua presença é evidentemente necessária para justiça básica, o governo honesto e conhecimento verdadeiro. Mas um excesso dela esmaga sujeitos individuais, humilha culturas minoritárias, desvaloriza a criatividade artística, e desacredita a participação política democrática genuína.” (PORTER, 1995:3)

Muitos exemplos cotidianos se sustentam sobre esta confiança no conhecimento distanciado, abstrato, baseado no mito da universalidade. Em particular, na computação, onde o conhecimento abstrato, formal, se materializa nos programas de computadores, e assim toma contato

aparentemente direto, sem intermediação, com o “mundo da vida” (Husserl (1954/1970:48-49) (o mundo onde se ergue e esmaga, se enaltece e humilha, se dá valor e despreza, se tem convicção e se desacredita), surgem diversos exemplos onde a autoridade da matemática se mostra impotente diante de certas questões de ordem “prática”. “Em 1987, E. Peláez, J. Fleck e [D. MacKensie] previram que a demanda por provas da correção de sistemas de computadores levaria inevitavelmente a um tribunal governar sobre a natureza da prova matemática.” (MacKensie, 1996:166) Um caso prático surgiu já na década de 1970 em controvérsias em torno da definição de uma aritmética computacional decorrentes do confronto da expansão infinita de certos números reais e o tamanho finito da representação computacional, o que certamente impõe alguma forma de truncamento do número. Uma comparação entre os diversos algoritmos usados por diferentes empresas fabricantes de computadores na época evidencia que há muitas decisões a serem tomadas quanto à representação e tratamento dos números fracionários. E os diversos algoritmos usados por diferentes empresas (IBM, Digital, HP, Intel, Texas) apresentavam resultados diferentes.

“Um especialista cit[ou] um problema de cálculo de juros compostos que teve quatro resultados diferentes quando feito em computadores de quatro diferentes tipos: \$331,667.00, \$293,539.16, \$334,858.18 e \$331,559.38. Ele indentific[ou] máquinas nas quais  $a/1$  não é igual a  $a$  (como, na aritmética humana, deveria sempre ser) e  $e\pi - \pi e$  não é zero.” (MacKensie, 1966:168)

Negociar a aritmética se provou ser um processo longo. Um comitê começou a trabalhar em setembro de 1977 e o padrão IEEE 754, Aritmética Binária de Números Fracionários, só foi adotado em 1985. O ponto crucial, destacado por (MACKENZIE, 1996:182) é que

“havia uma aritmética humana consensual e estável perante a qual a aritmética computacional poderia ser julgada. A aritmética humana foi, contudo, insuficiente para *determinar* a melhor forma da aritmética computacional. ... a aritmética humana proveu um recurso, ao qual os diferentes participantes recorreram diferentemente, e não um conjunto de regras que poderia simplesmente ser aplicado na aritmética dos computadores.”

Tornou-se necessário que entrassem em cena fatores extra-matemáticos, e a negociação de um *acordo* sobrepôs a autoridade matemática. Por outro lado, nos processos de certificação de sistemas de computadores de alto risco não são evidentes as convenções, os fatores extra-matemáticos, as negociações e os acordos que sustentam a autoridade dos métodos matemáticos como árbitros de correção. Esta situação tem suas origens ao fim dos anos 1960, quando os programas de computadores já se tornavam demasiado grandes, e serviam a aplicações envolvendo situações críticas de segurança. O Departamento de Defesa Norte Americano (DoD) iniciou uma série de debates que apontavam para a matematização dos sistemas como indicador de correção. Buscava-se

criar metodologias para matematizar a atividade de programar, questionava-se a eficácia dos testes empíricos e apostava-se nas especificações formais como meio viabilizador da programação segura em dois sentidos: sendo as linguagens de especificação mais abstratas do que as linguagens de programação, as primeiras estariam mais próximas do domínio do problema do que as últimas, facilitando o correto entendimento e a fácil expressão da solução, e, por serem formais, possibilitariam provas de propriedades de programas, assegurando a correção (qualidade do correto):

"A única maneira eficaz de elevar o nível de confiança de um programa de forma significativa é dar uma prova convincente de sua correção. Mas não se deve primeiro fazer o programa e depois provar sua correção, porque assim, a exigência de fornecer a prova, só iria aumentar o fardo do pobre programador. Pelo contrário: o programador deve deixar a prova correção e programa crescerem de mãos dadas." (DIJKSTRA, 1972).

Mas a confiança em métodos formais para assegurar a ausência de erros já não era, naquela época, um consenso. DeMillo, Lipton e Perlis questionavam a abrangência das provas e indicavam a presença de fatores sociais interferindo nos processos de verificação.

"[S]uponhamos que o programador recebe a mensagem 'VERIFICADO'. E suponhamos ainda que a mensagem não resulta de uma falha por parte do sistema de verificação. O que é que o programador sabe? Sabe que seu programa é formalmente, logicamente, provadamente, certificadamente correto. Ele não sabe, no entanto, até que ponto é confiável, seguro, ele não sabe os limites em que vai trabalhar, ele não sabe o que acontece quando se ultrapassa esses limites. E ainda tem esse selo místico de aprovação: 'VERIFICADO'. Quase podemos ver o iceberg que aparece em segundo plano sobre o navio inafundável." (DEMILLO, LIPTON e PERLIS, 1979).

A matematização, entretanto, ganhou força dentre os cientistas da computação, influenciando currículos e tornando-se um “ponto de passagem obrigatório” em aplicações de risco. Atualmente, empresas de certificação em informática criam padrões para garantir a confiabilidade de sistemas em um amplo espectro de aplicações. A grande maioria dos profissionais de informática não é capaz de entender as complicadas provas de correção adotadas nestes padrões. Possivelmente compreenderiam melhor os próprios programas. Mas considera-se que se o sistema é "certificado", então ele tem a garantia de que pode ser utilizado mesmo em situações de alto risco. Dando continuidade aos padrões promovidos pelo DoD na década de 70 a associação de empresas Common Criteria (CC), criada em 1999, define sete níveis de confiabilidade, onde o grau de confiança é diretamente proporcional à aderência a métodos formais. Para avaliar um sistema, os CC designam um grupo de especialistas, cujo nome, “*evaluation authority*”, deixa transparecer o forte senso da autoridade matemática. O papel dos métodos formais é como se segue: (i) O desenvolvedor *escolhe* e formaliza as propriedades que *ele* considera fundamentais para a

segurança. (ii) O desenvolvedor apresenta a especificação formal das partes *que ele considera* que são pontos críticos. (iii) O desenvolvedor fornece a prova de que a especificação formal (de partes) do sistema satisfaz as propriedades *escolhidas*. (iv) O desenvolvedor fornece a prova de que o sistema é realmente um refinamento (uma implementação) da especificação dada, e portanto, também satisfaz as mesmas propriedades que foram provadas no nível formal.

Grifamos as palavras “escolher” e “considerar” por serem indicadores de muita subjetividade no estágio inicial deste processo. Incapaz de eliminá-la, o método formal acaba por, subrepticiamente, propagar a subjetividade das escolhas e considerações por todo o processo. Então, o que fala mais alto aqui não é a objetividade, o raciocínio puramente dedutivo, mas a força da confiança e da autoridade que robustecem (tornam verdades aceitas) afirmações como "produtos de TI que ganham um certificado Common Criteria podem ser adquiridos ou utilizados sem a necessidade de uma avaliação posterior" (<http://www.commoncriteriaportal.org/ccra/>).

Não obstante o exemplo da Common Criteria, as críticas nos anos 70 em relação aos processos de matematização foram além da constatação da impotência métodos formais. DeMillo, Lipton e Perlis, de certa forma, anteciparam o movimento que hoje presenciamos de envolvimento com processos sociais como meio de adquirir maior credibilidade e correção:

"Que elementos podem contribuir para tornar a programação mais como engenharia e matemática? Um mecanismo que pode ser explorado é a criação de estruturas gerais cujas instâncias tornam-se mais confiáveis a medida em que aumenta a confiabilidade da estrutura geral. Essa noção já apareceu de várias formas, das quais a insistência de Knuth sobre a criação e entendimento de algoritmos gerais é um dos mais importantes e encorajadores. A metodologia de equipe de programação de Baker é uma tentativa explícita de expor o software a processos sociais. Se o reuso tornar-se um critério efetivo de projeto, uma comunidade cada vez mais ampla examinará as ferramentas mais comuns de programação." (DEMILLO, LIPTON e PERLIS, 1979).

Os citados "algoritmos gerais" tomaram a forma de *design patterns*: algoritmos inacabados que descrevem soluções gerais e devem ser adaptados a muitas situações reais. As "metodologias em equipe" foram ampliadas através das capacidades de colaboração introduzidas pela Internet, de forma que um código possa ser construído e examinado por muitos, tendendo à estabilidade. O reuso é amplamente disseminado porque permite a utilização de códigos já estáveis para a construção de novos módulos evitando a introdução de erros em tarefas pela re-programação. Além disso, cada usuário é também um fiscal, já que, no momento da ocorrência de um erro lhe é oferecida a oportunidade de notificar o desenvolvedor. Atualmente há uma proliferação de metodologias de desenvolvimento de software que apostam em processos colaborativos e aprendizagem participativa, como *Test Driven Development*, *Problem Based Learning*, *Social*

*Coding, Pair Programming*. Tais iniciativas partem do pressuposto de que a criação coletiva, negociação, discussão, revisão por múltiplos agentes, entre outros mecanismos de participação, tendem a maximizar as chances de sucesso minimizando os erros na construção do código. Assim configura-se atualmente, no mundo da computação, o seguinte confronto: de um lado, a autoridade da matemática, a universalidade, o conhecimento livre de subjetividades, e de outro, os processos localizados, subjetivos, participativos, que pressupõem interação social e se conformam cara a cara.

### **Localizando a matemática: contribuições para a sociologia do conhecimento**

No processo de construção do conhecimento, questões usualmente ditas “técnicas” são de tal forma indissociáveis daquelas usualmente ditas “sociais” que não há como estabelecer fronteiras precisas entre elas. Ao argumentarmos que o conhecimento, em particular, o conhecimento matemático, é localmente produzido e comprometido com as conjunturas onde foi concebido, evidenciamos duas questões que, por se situarem no encontro do “técnico” com o “social”, se perdem na dicotomia técnico-social: (1<sup>o</sup>) relações assimétricas de poder se fortalecem no que é dito “técnico” na medida em que a técnica, sob um caráter universal e neutro, só admite questionamentos em seus próprios termos; (2<sup>o</sup>) situações conjunturais, ou seja, de certo local, de certa data, influenciam diretamente na conformação do técnico. Bloor (2009:131) pergunta: “Questão mais controversa é se a sociologia pode atingir o âmago do conhecimento matemático. Ela seria capaz de explicar a necessidade lógica de um passo em um argumento, ou porque uma prova é de fato uma prova?” e propõe uma sociologia da matemática que, ao resgatar vínculos da matemática com condições locais, permita, senão confirmar a aparência que a matemática assume no senso comum, ao menos explicá-la.

A corte suprema de Hilbert ilustra um momento na história em que a matemática procurava desprender-se de todos os seus vínculos com materialidades para ser abstrata, neutra, universal. Em algum momento, entretanto, ao tornar-se aplicada a alguma questão do mundo da vida, a matemática localiza-se, ou seja, re-estabelece vínculos com (outras) materialidades. Como no caso de sistemas computacionais, a matemática neutra e universal não mais dá conta de apontar um “caminho correto”, e as controvérsias são resolvidas por acordos que transbordam o mundo matemático. Neste momento, abala-se o eixo da autoridade da matemática, abrem-se espaço a novas possibilidades de construção de conhecimento, possivelmente permitindo uma matemática que as pessoas fazem, que as pessoas vivem, no local onde fazem, onde vivem, mesmo que seja fora dos grandes centros de autoridade.

## REFERÊNCIAS BIBLIOGRÁFICAS

- BERNAYS, P. Platonism in mathematics. Bernays Project, texto 13. Disponível em <<http://www.phil.cmu.edu/projects/bernays/Pdf/platonism.pdf>>. Acesso em 29/09/2011.
- BLOOR, D. Conhecimento e Imaginário Social. São Paulo, Editora UNESP 2009
- DIJKSTRA, E. W. The Humble Programmer. *Commun. ACM* 15, 10 (Out 1972), 859-866
- GÖDEL, K. On Formally Undecidable Propositions of Principia Mathematica and Related Systems I, In: DAVIS, M. (Org) *The Undecidable*, Raven Press, Hewlett, New York, 1965.
- HILBERT, D. On the infinite. In: BENCERRAF, P. (ed.) *Philosophy of Mathematics*, <http://www.math.dartmouth.edu/~matc/Readers/HowManyAngels/Philosophy>
- HUSSERL, E. *The crisis of European sciences and transcendental phenomenology*. Evanston: Northwestern University Press. (1954/1970). xliii, 405 p. p.
- MACKENZIE, D. A. *Mechanizing proof: computing, risk, and trust*. Cambridge, Mass.: MIT Press. 2001. xi, 427 p. p. (Inside technology)
- MACKENSIE, D. Negotiating Arithmetic, Constructing Proof. In: D. Mackensie (Ed.). *Knowing Machines - Essays on Technical Change*. Cambridge, MA: The MIT Press, 1996 p.165-184
- DEMILLO, LIPTON e PERLIS, Social Process and Proofs of Theorems and Programs. *Commun. ACM* 22, 5 (1979), 271-280
- PORTER, T. M. *Trust in numbers: the pursuit of objectivity in science and public life*. Princeton University Press, 1995
- WEYL, H. David Hilbert and his Mathematical work. *Bull. Amer. Math. Soc.* v.50, p.612-654.