I. S. T. — Cálculo Automático — Exame Final — 2.ª Epoca — 16 de Outubro de 1971

I

5795 — *a*) Escreva um subprograma em FORTRAN para, dependendo de um parâmetro que será um valor inteiro, adicionar ou subtrair duas matrizes quaisquer, ambas de M linhas e N colunas. Considere no subprograma que as matrizes são dadas por linhas e colunas.

b) O subprograma que escreveu na alínea *a*) de que tipo é? Poderá ser de outro tipo? Justifique.

c) Quais as limitações de generalidade impostas pelo facto de se considerarem as matrizes por linhas e colunas, em vez de as tomar como vectores de $M*N$ componentes?

d) Indique quais as alterações que seriam necessário introduzir no seu subprograma para considerar as matrizes no caso da alínea *c*).

II

Uma estrutura vectorial possui, no máximo, 100 componentes. Cada uma das primeiras K componentes, excepto a primeira e a K-ésima, devem ser substituídas por

$$A_i = (A_{i-1} + A_i + A_{i+1}) \div 3$$

e posteriormente pretende calcular-se a norma do vector das K componentes transformadas, de acordo com a definição

$$N = \sqrt{\sum_{i=1}^{K} A_i^2}$$

Escreva um programa em FORTRAN para, a partir dos valores originários das componentes de A em memória, imprimir o valor de N numa impressora de linhas.

III

a) Defina valores e vectores próprios de uma matriz quadrada.

b) Demonstre ou dê um contra exemplo para a afirmação seguinte: «para matriz real os valores próprios definem univocamente a matriz».

c) Demonstre qualquer facto que considere importante acerca dos valores ou vectores próprios de matrizes reais e simétricas.

Enunciados dos n.os 5793 a 5795 de J. Marques Henriques

BOLETIM BIBLIOGRÁFICO

Nesta secção, além de extractos de críticas aparecidas em revistas estrangeiras, serão publicadas críticas de livros e outras publicações de Matemática de que os Autores ou Editores enviarem dois exemplares à Redacção.

OS COMPUTADORES E AS MATEMÁTICAS PURAS

188 — Leech, John (editor) — **Computational Problems in Abstract Algebra** — Proceedings of a Conference held at Oxford under the auspices of the Science Research Council — Pergamon Press, Oxford, 1970.

189 — Atkin, A. O. L. and Birch, B. J. (editors) — **Computers in Number Theory** — Proceedings of the Science Research Council Atlas Symposium No. 2 — Academic Press, London and New York, 1971.

Os dois livros aqui em crítica, embora versem tópicos bem distintos, o primeiro dedicado à Álgebra e o segundo à Teoria dos Números, têm contudo muito mais em comum para além de se tratarem de actas de dois Simpósios organizados pelo Atlas Computer Laboratory da Universidade de Oxford: ambos têm uma linha de rumo comum e visam tópicos de investigação fortemente condicionados ou impulsionados pelo uso de computadores. Por isso mesmo faremos a sua crítica conjuntamente e por se tratar de domínios quase desconhecidos entre nós alongar-nos-emos na exposição mais do que é normal numa simples crítica bibliográfica.

Já há longos anos que vários investigadores têm procurado utilizar computadores com maior ou menor sucesso no campo das Matemáticas Puras. Um dos mais lídimos precursores desta utilização foi, sem dúvida, J. von Neumann, mas devem aqui ser também

mencionados, em especial M. Kac, G. B. Danzig, H. Kuhn, A. W. Tucker, M. Hall, T. S. Motzkin, R. Belman, D. H. Lehmer e tantos outros.

Uma resenha relativamente moderna de alguns resultados obtidos até cerca de 1967 encontra-se no livro editado por R. F. Churchhouse e J. C. Herz, *Computers in Mathematical Research*, North-Holland Publishing Co., Amsterdam, 1968, prefaciado por J. Dieudonné, obra esta infelizmente muito pouco divulgada entre nós e da qual nem sequer se nos consta que tenha havido qualquer apreciação crítica escrita em português.

Na medida em que procuramos embora sem reparar a falta chamar pelo menos a atenção para ela, cumpre-nos mesmo sumàriamente indicar alguns resultados interessantissimos obtidos no âmbito das ciências matemáticas com o auxílio dos computadores.

Não nos referimos, evidentemente, à contribuição essencial que os computadores têm fornecido no campo dos vários ramos da Análise Numérica, e das suas múltiplas aplicações no âmbito das ciências físicas e da engenharia, e de outros domínios da Matemática Aplicada, nomeadamente na Estatística, Investigação Operacional e Simulação. Aqui vamo-nos reportar exclusivamente a vários resultados do âmbito da Matemática Pura (sem pretender, como é óbvio, dividir a Matemática em duas...).

Ora muitas vezes as Matemáticas Puras têm feito uma figura de parentes pobres no âmbito das aplicações dos computadores. Por seu lado os computadores desempenham frequentemente o papel de intrusos para muitos matemáticos puros. Consoante o seu temperamento (e, vamos lá, também a sua formação) estes dividem-se entre os incrédulos, os hostis e os indiferentes. Por esta razão não teria sido possível impedir que em vários centros matemáticos de universidades ou de outros organismos ligados a projectos científicos os computadores tenham desempenhado papel importante na investigação no domínio das Matemáticas Puras. Ao mesmo tempo estes resultados têm levado a novas aplicações; por seu lado as modernas teorias das linguagens e dos sistemas de exploração, ligados ao funcionamento e operacionalidade dos computadores, têm levantado complexos e profundos problemas de natureza matemática.

A actividade do matemático puro pode em geral dividir-se entre a investigação de novos teoremas e a sua demonstração. Enquanto uma proposição não é demonstrada continua a ser uma conjectura. Pelo lado do matemático, quando este é levado a formular uma nova conjectura, esta formulação é de tal modo difícil de definir que mesmo para um enunciado não pode haver qualquer possibilidade de o matemático se fazer substituir por uma máquina. Em compensação o computador pode guiar a intuição do matemático, pelo menos em alguns ramos tais como, por exemplo, a Teoria dos Números e a Análise, trazendo-lhe ou analisando por ele um volume enorme de dados numéricos. Por vezes numa investigação paciente pode encontrar-se um contra-exemplo, destruindo uma conjectura.

Assim, Euler conjecturou em 1769 que a equação

$$x^5 + y^5 + z^5 + t^5 = u^5$$

não deveria ter solução no conjunto dos números inteiros. Em 1966 um computador encontrou o quintuplo $x = 27$, $y = 84$, $z = 110$, $t = 133$, $u = 144$, que constitui uma solução da equação dada.

É claro que não há verdadeiras vantagens que se psssam esperar dum computador quando ele se encarrega de uma demonstração, e se bem que toda a Matemática seja redutível a um jogo de escritas formais não existem métodos mecânicos gerais que permitam a construção de uma demonstração de um enunciado a partir desse mesmo enunciado. Mesmo se esse método existisse numa parte restrita da teoria a sua aplicação prática seria limitada pela extensão dos cálculos.

Mas ainda aí a experiência e a intuição do matemático permitirão muitas vezes encontrar sem grandes dificuldades as malhas essenciais da cadeia lógica. O computador não pode intervir senão em pequenos detalhes, como o faria qualquer escravo fiel. Foi assim que, com a ajuda de uma técnica já antiga, mas impossível de aplicar até ao aparecimento dos computadores em vista do grande volume de operações a efectuar, se pôde fazer avançar os limites conhecidos da validade da conjectura de Fermat, segundo a qual a equação

$$x^n + y^n = z^n$$

não possui solução no conjunto dos números naturais para $n > 2$. Esta propriedade foi demonstrada em 1964 para todos os valores de n inferiores a 25000. É claro que aqui não se trata de uma simples verificação, uma vez que os valores das incógnitas não são limitados. Sobre a veracidade ou falsidade da conjectura de Fermat talvez que ainda a palavra final venha a ser dada por um computador...

Um domínio de eleição da aplicação dos computadores na Matemática Pura tem sido a Teoria dos Números. Assim, por exemplo, é bem conhecida a afirmação enunciada por Mersenne em 1644 de que $M_p = 2^p - 1$ seria primo se e só se p fosse um dos primos 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 e composto para os restantes 44 primos $p \leq 257$. Ainda hoje se desconhecem as razões que levaram Mersenne a este

enunciado; contudo, o primeiro erro na sucessão de MERSENNE foi descoberto em 1886 por PERVUSIN e SEELHOF. Outros erros foram descobertos posteriormente, mas em 1876 LUCAS descobriu um teste de primalidade (mais tarde aperfeiçoado por LEHMER, tendo já em vista os modernos computadores), que aplicou a M_{127}, verificando que se tratava, efectivamente, de um número primo. Este terá sido, muito provàvelmente, o maior primo descoberto sem o auxílio de máquinas de cálcular ou de computadores.

Só em 1951 se vieram a descobrir números primos maiores: M_{521} foi ainda descoberto com o auxílio de máquinas de calcular; todos os outros conhecidos até este momento foram-no com o auxílio de computadores.

Em 1964 GILLIES descobriu que M_{9689}, M_{9941} e M_{11213} são também primos (os maiores conhecidos até essa altura) e graças aos esforços de vários investigadores entre os quais é de salientar também FERRIER, MILLER, WHEELER, LEHMER, ROBINSON, RIESEL, HURWITZ e SELFRIDGE, os 23 primos de MERSENNE conhecidos até então eram os correspondentes a $p=2$, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941 e 11213. De acordo com o teorema de EUCLIDES e de EULER, segundo o qual um número par n é perfeito se e só se $n=(2^p-1)\cdot 2^{p-1}$ com p primo e tal que 2^p-1 seja ele também primo eram portanto conhecidos em 1964 23 números perfeitos. Note-se que o maior primo conhecido no tempo de EULER era $2^{31}-1$.

Em 4 de Março de 1971 B. TUCKERMAN aplicou com êxito o teste de LUCAS-LEHMER para descobrir que o 24.º primo de MERSENNE é M_{19937} e que, associado a ele, o número $(2^{19937}-1)\cdot 2^{19936}$ é o 24.º número perfeito conhecido. Cada um destes números possui, respectivamente 6002 e 12003 dígitos e é impensável que esses resultados tivessem podido ser obtidos por outra via, atendendo a que em computadores com a potência de vários milhões de instruções por segundo o tempo de cálculo oscila por uma hora!

Virá a ser, sem dúvida, interessante verificar por quanto tempo manterá M_{19937} o título do «maior primo conhecido». Efectivamente, M_{11213} resistiu durante 7 anos; a sua primalidade, que em 1964 demorou várias horas de cálculo a ser estabelecida, é verificada actualmente em escassos minutos usando os mesmos computadores e programas utilizados por TUCKERMAN. Esta evolução veio permitir, por outro lado, que fossem efectuados testes exaustivos para todos os primos $p<20000$. Estes cálculos foram confirmados durante o Verão de 1971 por M. SPECINER e R. C. SCHROEPPEL, usando outros métodos introduzidos no teste de LUCAS-LEHMER por D. E. KNUTH. Quer isto dizer portanto que só máquinas extremamente potentes, comparadas com os maiores supercomputadores existentes actualmente, poderão vir a ser usadas de futuro.

Esta busca está longe de ter interesse estritamente académico. Por um lado tem permitido aperfeiçoamentos sucessivos de algoritmos de cálculo, por outro exige refinamentos adequados das linguagens e dos programas utilizados. É de mencionar ainda o interesse destes métodos associados, por exemplo, a problemas tão diversos como a geração de números pseudo-aleatórios em computador.

Não menos frutuosa tem sido a utilização dos computadores nos domínios da Teoria Combinatória e da Programação Matemática, Linear e Não-Linear.

Assim, há vários estudos que relacionam as propriedades dum grafo com o espectro da matriz adjacente do grafo. Estes estudos incluem entre outros: limites superiores e inferiores do número de cores e funções relacionadas, caracterização dos grafos em que o primeiro ou o segundo ou o mais pequeno dos valores próprios são limitados e caracterização de famílias de grafos fortemente regulares.

Também vários estudos têm relacionado a Teoria dos Grafos com todos ou alguns dos vértices de poliedros, tendo-se chegado, muitas vezes por vias enumerativas a extensões de trabalhos anteriores de TUTTE e de EDMONDS.

Algumas questões da Teoria Combinatória têm surgido na Teoria dos Grafos noutros contextos, por exemplo argumentos grafoteóricos que têm sido usados para provar que são necessárias pelo menos $2n-1$ operações binárias para calcular o produto interno de dois vectores no espaço n-dimensional, quaisquer que sejam as funções auxiliares contínuas que são calculadas em primeiro lugar. Esta teoria deu lugar a toda uma reformulação de certos algoritmos de cálculo, em particular no que diz respeito ao vulgar produto de matrizes, destacando-se nestes trabalhos em especial S. WINOGRAD.

Uma vez que em computador o tempo necessário para efectuar uma soma (ou subtracção) é, em geral, mais reduzido do que o necessário para uma multiplicação, estas descobertas são de importância excepcional em processos envolvendo muitos milhões de operações aritméticas. Assim, verificou-se que em geral o menor número de multiplicações exigido para o cálculo do valor de um polinómio inteiro de grau n é o que se obtém pela aplicação da regra de HORNER e que é precisamente n; o mesmo sucede quando se trata do produto interno de dois vectores de n componentes e ainda a regra do produto de uma matriz $m\times n$ por um vector exige, no mínimo $n\cdot m$ multiplicações (S. WINOGRAD, On the number of multipli-

cations required to compute certain functions, *Proc. of the Nat. Academy of Sciences* 58 pgs. 1840-2, November 1967). Porém, o vulgar produto de matrizes, a que acima nos referimos não é optimal, no sentido de que não minimiza o número de multiplicações; assim, como é bem conhecido, o produto ordinário de uma matriz $m \times p$ por outra $p \times q$ exige $m \cdot p \cdot q$ multiplicações. Se as duas matrizes forem quadradas, de ordem n (*i.e.* $m = p = q = n$), o número de multiplicações é pois de n^3. Ora, os trabalhos de WINOGRAD e outros, entre os quais devemos ainda mencionar V. STRASSEN, permitiram estabelecer que $n^3/2 + n^2$ multiplicações são suficientes se as matrizes forem quadradas. Para valores suficientemente grandes de n as reduções nos tempos de cálculo são substanciais, mesmo atendendo a que são necessárias mais somas e subtracções do que para o algoritmo vulgarmente usado.

Aquele número é apenas um limite superior geral: assim, para o produto de duas matrizes 2×2 basta o cálculo de 7 multiplicações, o que corresponde a $n^3/2 + n^2 - n/2$, expressão válida para matrizes de ordem $n = m \cdot 2^{k+1}$ com m e k naturais, aperfeiçoamento este devido a A. WAKSMAN (On WINOGRAD's algorithm for inner products, *IEEE Transactions on Computers* C-19 pgs. 360-1, April 1970).

Também com base na utilização de computadores foram iniciados estudos bastante gerais de problemas da programação inteira, baseados numa análise exaustiva do ambiente convexo dos pontos inteiros contidos no cone determinado pelos hiperplanos que intersectam o vértice de um poliedro. Esta análise tem-se baseado num novo ponto de vista que relaciona a Teoria dos Poliedros com a Teoria dos Grupos Abelianos.

Uma vez que começámos a abordar este tipo de problemas, parece-nos interessante recordar aqui o seguinte problema, enunciado e resolvido por D. H. LEHMER: pretende-se calcular todos os menores (de ordem 12) de uma matriz dada, de 12 linhas e 20 colunas. Na Análise Combinatória clássica, no sentido de LEIBNIZ, existem exactamente $\binom{20}{12} = 125970$ tais menores, número susceptível de ser convenientemente trabalhado em computador. Contudo pretende-se ainda distribuir este trabalho por dois computadores, um dos quais é cinco vezes mais rápido do que o outro, de tal modo que a ocupação em tempo seja igual nas duas máquinas. Assumindo ainda que a máquina mais lenta processa o trabalho começando pelo princípio (menor constituido pelas 12 primeiras colunas da matriz), com que menor deverá a máquina mais rápida iniciar o processamento?

A resposta é que deverá ser o menor determinado pelas colunas 1, 2, 3, 6, 7, 12, 13, 14, 16, 17, 18, 19. Este problema pode ser generalizado: se n é um inteiro e m é outro inteiro qualquer $(m \geq n)$, então

$$m = \binom{k_1}{1} + \binom{k_2}{2} + \cdots + \binom{k_n}{n}$$

onde $0 \leq k_1 < k_2 < \cdots < k_{n-1} < k_n$, e esta representação é única, podendo servir para determinar a ordem das combinações de m objectos tomados n a n. Esta representação é de interesse noutros ramos da Matemática, em particular na Teoria das Probabilidades, onde foi redescoberta por L. DUBINS e L. J. SAVAGE.

Outros dois aspectos que têm sido fortemente impulsionados pelos computadores são os da Programação Permutacional e o Problema do Caixeiro Viajante.

A Programação Permutacional pode enunciar-se simplesmente como uma programação inteira em que a solução deve consistir numa permutação dos números $1, 2, \cdots, n$ (n = número de incógnitas). Este problema tem sido estudado por JAESCHKE, sem contudo se conhecerem ainda soluções gerais satisfatórias.

Quanto ao Problema do Caixeiro Viajante, embora envolvendo grandes dificuldades computacionais, está hoje já razoàvelmente equacionado e resolvido, mesmo em casos de variantes mais complexas: o caixeiro viajante pretende passar por n pontos (designados por $1, 2, \cdots, n$ e vulgarmente conhecidos por «cidades» na terminologia do problema), e regressar à base (ponto 0), sem nunca passar duas vezes pelo mesmo ponto. O custo da deslocação do ponto i para o ponto j é c_{ij} (òbviamente $c_{ij} = c_{ji}$ e $c_{ij} > 0$ se $i \neq j$, sendo $c_{ii} = 0$). O problem consiste em obter uma permutação cíclica Φ dos números $1, 2, \cdots, n$ tal que para cada ponto i seja possível encontrar um sucessor $\Phi(i)$, de tal modo que $\sum_{i=1}^{n} c_{i,\Phi(i)}$ seja mínimo.

Como o número das permutações de n números é $n!$, com $n = 10$, virão neste caso $10! = 3628800$ hipóteses (repare-se que 10 é ainda um caso simplificado, pois todas as formulações com interesse prático conduzem a valores de n da ordem de 25 ou superiores). De acordo com D. E. KNUTH (*The Art of Computer Programming* 1, Addison-Wesley Publishing Co., Reading, Mass., 1968) este valor constitui, para efeitos práticos, o limite ao número aceitável de interacções que é actualmente possível de efectuar em computador, o que de modo algum virá a ser uma limitação de futuro, dado que as velocidades máximas dos computadores têm duplicado em média de 2 em 2 anos.

Contudo, frizamos uma vez mais, tal limitação veio simplesmente implicar que os matemáticos descobrissem novos métodos de ataque a estes problemas. Foi aliás o caso com o Problema do Caixeiro Viajante, em que existem algoritmos bastante gerais devidos a R. E. Gomory.

Cremos ser suficiente o que acima se disse para avaliar do interesse dos livros que agora passamos a criticar. Qualquer deles possui excelentes artigos, cujo grau de acessibilidade ao Leitor varia do «razoàvelmente simples» ao «extremamente complexo», como aliás seria de esperar em publicações deste tipo; contudo tanto numa como na outra destas obras encontram-se imensos resultados de profundo interesse e novas formulações de outros já conhecidos.

No que toca à Algebra, o artigo de J. Neubüser (Investigations of groups on computers) resume em 20 páginas todo o desenvolvimento de um interessantíssimo campo de aplicação dos computadores em Matemática, envolvendo aspectos muito importantes da dualidade entre as aplicações numéricas e as não-numéricas; só é efectivamente pena que não tenha sido possível uma actualização bibliográfica neste volume: no artigo que acabamos de mencionar estaria bem uma referência a alguns outros resultados mais recentes, tal como foram sumarizados por J. J. Cannon (Computers in Group Theory; a survey, *Comm. of the ACM* 12 pgs. 3-12). Na nossa opinião estes dois artigos deveriam ser de leitura obrigatória para qualquer estudante de matemática das nossas universidades. Outro artigo de J. Neubüser e V. Felsch (On a programme for the determination of the automorphism group of a finite group) trata também de grupos finitos, e o mesmo sucede no trabalho extraordinário de M. Hall (A search for simple groups of order less than one million), este contudo de leitura muito menos acessível, até porque o Autor tem o cuidado de indicar as limitações do seu trabalho e as possíveis extensões.

Julgamos que seria interessante continuar a linha sugerida por Marshall Hall de construção de grupos simples de ordens bastante grandes. Tópicos para ulteriores trabalhos aparecem também frequentemente indicados no artigo de C. C. Sims (Computational methods in the study of permutation groups).

No total este volume contém 35 artigos, para todos os gostos e graus de dificuldade, quer do ponto de vista algébrico, quer computacional. Talvez fôsse de esperar uma certa ênfase, pela sua importância prática na Teoria das Equações, a que apenas são dedicados dois artigos, um de W. D. Maurer (The uses of computers in Galois theory), aliás bastante acessível e interessante, e o outro de H. Zassenhaus (A real root calculus).

O outro volume aqui em crítica, *Computers in Number Theory*, engloba 46 artigos, também para todos os paladares e graus de dificuldade, se bem que todos com o mesmo sentido de originalidade de resultados ou de métodos. Em geral todos eles são bastante interessantes, sendo porém de notar a ausência de artigos sobre a busca de números primos ou problemas relacionados.

Qualquer escolha no âmbito de uma crítica deste género terá forçosamente de reflectir as inclinações pessoais do crítico. Contudo notamos com agrado a inclusão de artigos como o de D. H. Lehmer (The economics of number theoretic computations) em que são incluidas discussões de vários tópicos do tipo das que mencionámos acima; o de H. M. Stark (An explanation of some exotic continued fractions); outro artigo de M. Hall (The Diophantine equation $x^3 - y^2 = k$), seguido de outro de F. B. Coghlan e N. M. Stephens, com o mesmo título mas com muito poucas relações com aquele (?).

Muito interessantes são, a nosso ver, os artigos que enunciam problemas de interesse geral e indicam também vários campos a explorar. Agrupamos aqui, além do de Lehmer, já mencionado, os artigos de P. Erdös (Some problems in number theory), que só poderemos classificar de excelente, o de R. K. Guy (Some unsolved problems) e finalmente outro artigo de P. Barrucand (Languages), que também classificaríamos como excelente se o encarássemos estritamente do ponto de vista do matemático, mas que a considerarmos também sob a óptica do informático, sinceramente não concordamos.

Efectivamente as críticas que Barrucand formula relativamente a certas linguagens de programação são válidas, mas o Autor aparentemente esqueceu o facto de haver muitas outras que poderão ser usadas com vantagem para a investigação de algoritmos e portanto para a pesquisa no campo da Teoria dos Números. Quanto aos problemas de certas imprecisões numéricas que dificultam o acesso ao computador relativamente a certos problemas, isso parece-nos ser uma barreira muito difícil ou mesmo impossível de ultrapassar...

Mas, em resumo: as aplicações dos computadores às Matemáticas Puras são uma feliz realidade e estes dois livros constituem um magnífico reportório de contribuições que nenhum matemático interessado em Álgebra, Teoria dos Números ou Ciência dos Computadores poderá ignorar.

J. Marques Henriques