	Departamento de Matemática da Universidade de Coimbra		
2006/07	**Métodos de Programação II**	**TPC 2**	**Entrega: 27/10/2006**

Números Primos de Mersenne

Marin Mersenne (1588-1648) foi um monge com interesses matemáticos, que se correspondia com os maiores vultos da cena científica do seu tempo. Cerca de 1640, numa das suas missivas, descreve números da forma $M_p = 2^p - 1$, onde p é um número primo, isto em ligação com um seu estudo sobre números perfeitos[1]. Desde então que sabemos que alguns desses números, ditos de *Mersenne*, são primos, outros não. Por exemplo, $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ e $M_7 = 127$ são primos, enquanto que o próximo número de Mersenne é composto: $M_{11} = 2047 = 23 \times 89$. O crescimento destes números é da ordem exponencial[2], o que explica que, até ao momento, apenas sejam conhecidos 44 (o último foi descoberto dia 6 de Setembro de 2006, através de um projecto de computação distribuída chamado GIMPS[3]), e que possui mais de 9.8 milhões de digitos:

$$2^{32582657} - 1$$

No entanto, e já em 1640, Mersenne tinha identificado como primos os acima apresentados e ainda aqueles com $q = 13, 17, 19, 31, 127$. Para além disso, todos os primos de Mersenne que existem com $q \leq 127$ foram descobertos antes da era do computador. Em 1951, Alan Turing fez a primeira tentativa (frustada) para encontrar novos primos de Mersenne usando um computador. No ínicio do ano seguinte, Robinson, Lucas e Lehmer, descobrem, usando um programa de computador, os primos M_{521} e M_{607}. Ainda no final desse ano de 1952, conseguem descobrir os primos M_{1279}, M_{2203} e M_{2281}.

Na procura de números primos de Mersenne, um teste de primalidade muito usado é baseado no Lucas-Lehmer e consiste no seguinte resultado:

se p é primo então $M_p = 2^p - 1$ é primo se e só se M_p divide S_{p-2}

onde

$$S_k = \begin{cases} 4 & \text{se} \quad k = 0 \\ S_{k-1}^2 - 2 & \text{se} \quad k \geq 1 \end{cases}$$

Mais ainda, se M_p é um número primo então p é primo, o que significa que basta testar números de Mersenne com índices primos pois qualquer outro representa um número composto.

Neste trabalho pretende-se implementar um programa em Pascal para encontrar *Números primos de Mersenne*, os maiores possíveis usando apenas os computadores do Departamento (um para cada trabalho). Para isso, será, pelo menos, necessário:

- implementar um método de gerar números primos (pode usar um dos métodos estudados nas aulas de Métodos de Programação)
- implementar um teste de primalidade (o acima indicado ou outro que ache mais adequado) para números de Mersenne construídos com índice primo

[1] Números perfeitos são aqueles cuja soma dos seus divisores próprios iguala o próprio número.
[2] Crescem muito rapidamente, tal qual uma função exponencial.
[3] Great Internet Mersenne Prime Search. Ver mais informações em http://www.mersenne.org/

Tal como no trabalho anterior, o programa deve ser enviado, em "attachment" por mail para o endereço da professora e o relatório deve ser individual e manuscrito (de modo legível), explicando os algoritmos, os tipos de dados e o funcionamento geral do programa (sem recurso a qualquer linha de código nem a transcrição literal de tais linhas em Português).

Poderá consultar bibliografia/webgrafia variada, entre as possíveis destacamos:

1. *Prime Numbers: A Computational perspective*, R. Crandall, C. Pomerance, Springer, 2005
2. *The little book of big primes*, P. Ribenboim, Springer, 1991
3. *The book of prime number records*, P. Ribenboim, Springer-Verlag, 1988
4. *O Livro dos números*, J. Conway, R. Guy, Universidade de Aveiro/Gradiva, 1999

1. *GIMPS*, http://www.mersenne.org/
2. http://mathworld.wolfram.com/MersenneNumber.html
3. *The Prime Pages*, http://primes.utm.edu/ e http://primes.utm.edu/primes/

Não esqueça que, no relatório, deve ser indicada toda a bibliografia/webgrafia consultada.