Secção de Matemática Aplicada e Análise Numérica
Departamento de Matemática/Instituto Superior Técnico

Matemática Experimental (LMAC) – 1º Semestre de 2011/2012

1º **Miniteste – Resolução**

1. Tendo em conta que $a \bmod m$ é o resto da divisão de a por m temos

$$a \bmod m = b \bmod m \qquad \Leftrightarrow \qquad a - m\,q_1 = b - m\,q_2\,,$$

onde $q_1, q_2 \in \mathbb{N}$. Segue-se que

$$a \bmod m = b \bmod m \qquad \Leftrightarrow \qquad a - b = (q_1 - q_2)\,m \qquad \Leftrightarrow \qquad a \equiv b \pmod{m}\,.$$

2. **a)** O código `seula` é o crivo de Eratóstenes (ver os apontamentos). O programa recebe um inteiro $n \geq 2$ e começa por criar uma lista `data` de inteiros de 2 a n. Depois retira dessa lista todos os múltiplos de `pdiv`$= 2$ excepto o próprio. A seguir, considera o próximo elemento da lista `data`, um primo, actualiza `pdiv=data[[i]]` e retira da lista `data` os múltiplos de `pdiv` excepto o próprio. O ciclo `While` termina quando o primo divisor `pdiv` for maior que a raiz quadrada de n. O programa devolve a lista dos primos entre 2 e n.

b) O comando `seula[15]` cria a lista `data` $= \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$. De seguida retira da lista os múltiplos de `pdiv` $= 2$, i.e. `data` $\to$ `data` $= \{2, 3, 5, 7, 9, 11, 13, 15\}$, e os múltiplos de `pdiv` $= 3$, i.e. `data` $\to$ `data` $= \{2, 3, 5, 7, 11, 13\}$. Visto que `pdiv` $= 5 > \sqrt{15}$ o programa termina e devolve a lista $\{2, 3, 5, 7, 11, 13\}$.

3.

a)
```
teste[n_Integer/;n>= 4]:=(Mod[n-1,6]==0||Mod[n+1,6]==0)
```

b)
```
tabela=Table[Prime[n],{n,3,PrimePi[100]}]
Map[teste,tabela]
```

c) Os números inteiros da forma $6k, 6k+2, 6k+4, k \geq 1$, são divisíveis por 2, logo não são primos. De ígual modo os inteiros da forma $6k+3, k \geq 1$, são divisíveis por 3 e não são primos. Assim, todos os primos $p \geq 5$ podem ser escritos na forma $6k+1$ ou $6k-1$. Note-se no entanto que nem todos os inteiros da forma $6k+1$ ou $6k-1$ são primos.

4. Se $p = kq$ fosse composto então

$$a^p - 1 = a^{kq} - 1 = (a^k - 1)\,(1 + a + a^2 + \cdots + a^{(q-1)k})\,,$$

onde $k, q \geq 2$ são inteiros. Portanto $a^p - 1$ não seria primo. Por outro lado, temos

$$a^p - 1 = (a - 1)\,(1 + a + a^2 + \cdots + a^{p-1})\,,$$

ou seja se $a^p - 1$ é primo então $a - 1 = 1$ ou $1 + a + a^2 + \cdots + a^{p-1} = 1$. Segundo caso é impossível visto que $a, p > 1$. Do primeiro caso vem $a = 2$.