Teoria de Números Computacional

1. Introduziram-se os seguintes comandos no *pari/gp*. Repita-os, compare os tempos e interprete os resultados.

```
? for (i=1,1000000,i++)
? ##
  ***   last result computed in 265 ms.
? for (i=1,1000000,i+=1)
? ##
  ***   last result computed in 340 ms.
? for (i=1,1000000,i=i+1)
? ##
  ***   last result computed in 413 ms.
```

2. A cifra *shift* tem como funções de encriptação e decifração, respectivamente,

$$e_k(x) = x + k \mod n;\ d_k(y) = y - k \mod n$$

onde n indica a cardinalidade do alfabeto usado. Para $k = 3$ obtemos a cifra de César.

Introduza a função seguinte e interprete-a.

```
\\ cifra shift
\\ argumentos: frase sequencia de letras do algabeto, incr o shift

cesar(frase,incr=3)=    /* incr=3 e' o valor tomado para incr por defeito*/

{       local(lista, i, tamanho);

        if(type(incr)!="t_INT",
                error("Opcao invalida")
        );
        lista=Vecsmall(frase);
        tamanho=length(lista);
        print("incremento "incr);
        for(i=1,tamanho,
                lista[i]=((lista[i]-32+incr)%91)+32
        );
        print(Strchr(lista));
        return(Strchr(lista));
}
```

Use um ciclo `while` em vez do ciclo `for`.

3. A cifra *afim* tem como funções de encriptação e decifração, respectivamente,

$$e(x) = ax + k \mod n;\ d_k(y) = a^{-1}(y - k) \mod n$$

onde n indica a cardinalidade do alfabeto usado e a é tal que $(a, n) = 1$. Sabendo que o máximo divisor comum de a e n pode ser calculado à custa de `gcd(a,n)` e que o inverso de a em $\mathbb{Z}_n$, caso exista, pode ser calculado via `lift(Mod(1/a,n))`, implemente uma função para a cifra *afim*.

4. A *cifra de Vigenère* é uma cifra polialfabética com funções de encriptação e decifração

$$e_K(x_1, x_2, \ldots x_m) = (x_1 + k_1, x_2 + k_2, \ldots x_m + k_m)$$

$$d_K(x_1, x_2, \ldots x_m) = (x_1 - k_1, x_2 - k_2, \ldots x_m - k_m)$$

onde $K = (k_1, k_2, \ldots, k_m) \in \mathbb{Z}_n^m$. Este vector K pode corresponder a uma palavra, Por exemplo, se $A \sim 0, B \sim 1, C \sim 2, \ldots$, então se a chave="BLAISE" obtemos $K = (1, 11, 0, 8, 18, 4)$, $m = 6$. Implemente a *cifra de Vigenère*.

5. A sucessão de Fibonacci está definida recursivamente por $f_1 = 1, f_2 = 1, f_n = f_{n-1} + f_{n-2}$, para $n \geq 3$. Construa uma função que calcule os primeiros n termos da sucessão de Fibonacci.

6. A sucessão de Lucas está definida recursivamente por $L_1 = 1, L_2 = 3, L_n = L_{n-1} + L_{n-2}$, para $n \geq 3$. Construa uma função que calcule os primeiros n termos da sucessão de Lucas.

7. A conjectura dos primos gémeos afirma que existe uma infinidade de pares de números primos p e $p + 2$. Escreva uma função que encontre os primos gémeos inferiores a um certo argumento.

8. Teste a Conjectura de Goldbach: todo o natural par pode-se escrever como a soma de dois números primos.