Ordem de um número módulo um inteiro

1. Calcula a ordem de

   (a) 5 módulo 19; (b) 4 módulo 21; (c) 3 módulo 200.

2. Mostra que se a tem ordem $2k$ módulo um primo ímpar p então $a^k \equiv -1 \pmod{p}$.

3. Supõe que a ordem de a módulo n é h e que a ordem de b módulo n é k. Mostra que a ordem de ab módulo n divide hk. Conclui que se $\mathrm{m.d.c.}(h,k) = 1$ então a ordem de ab é hk.

4. Mostra que se p é um primo, então $p^p - 1$ tem algum factor primo congruente com um módulo p. Generaliza este resultado.

5. Mostra que $\phi(2^n - 1)$ é um múltiplo de n, para qualquer $n > 1$. Generaliza este resultado.

6. Dizemos que a é uma *raíz primitiva* de n se a tem ordem $\phi(n)$ módulo n. Mostra que 2 não é uma raíz primitiva de 17, e que 3 é uma raíz primitiva de 17.

Desafios

1. Um *número de Fermat* é um inteiro da forma $F_n = 2^{2^n} + 1$, onde $n \geq 0$. Se F_n é primo, então dizemos que F_n é um *primo de Fermat*. Os inteiros $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$ são primos de Fermat. Não se sabe se há mais algum primo de Fermat.

   (a) Prova que se $m > n \geq 0$ então $F_n | (F_m - 2)$. Deduz que $(F_m, F_n) = 1$ se $m \neq n$.

   (b) Mostra que 2 não é uma raíz primitiva de F_n.

2. Determina todos os inteiros n tais que existem sistemas completos de restos módulo n da forma $(a_1, \ldots, a_n)$ e $(b_1, \ldots, b_n)$ para os quais $(a_1 + b_1, \ldots, a_n + b_n)$ ainda é um sistema completo de restos módulo m.

3. Considera a sucessão de Fibonacci

   $$f_1 = f_0 = 1, \quad f_n = f_{n-1} + f_{n-2}, \quad n \geq 2,$$

   Mostra que existe $n \leq 10^8 + 1$ tal que f_n termina com quatro zeros.

No que se segue, p_n denota o n-ésimo número primo.

Distribuição dos números primos

1. Um par de primos *gémeos* é um par de primos da forma p, $p+2$. Por exemplo, 11 e 13 são primos gémeos, 17 e 19 são primos gémeos, e 23 é um primo que não é gémeo. Prova as seguintes propriedades:
   (a) O produto de um par de primos gémeos somado de uma unidade é um quadrado perfeito.
   (b) Com uma única excepção, a soma de um par de primos gémeos é um múltiplo de 12.
2. Mostra que se $n \geq 5$ então $p_n > 2n - 1$.
3. Mostra que nenhum dos inteiros $P_n = p_1 p_2 \cdots p_n + 1$ é um quadrado perfeito.
4. Mostra que a soma $\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$ nunca é um inteiro.
5. (a) A função $f(n) = n^2 + n + 41$ tem a seguinte propriedade: se n é um inteiro tal que $0 \leq n \leq 39$ então $f(n)$ é primo. Mostra que $f(40)$ e $f(41)$ não são primos.
   (b) Mostra que se $f(n)$ é um polinómio de grau k de coeficientes inteiros, isto é, se
   $$f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_2 n^2 + a_1 n + a_0$$
   onde os coeficientes $a_0, a_1, \ldots, a_k$ são inteiros e $a_k \neq 0$, então existem inteiros m tais que $f(m)$ é um número composto.
6. (a) Mostra que se $n > 3$ então n, $n+2$ e $n+4$ não são todos primos.
   (b) Encontra exemplos em que p, $p+2$ e $p+6$ são todos primos.
   (c) Aplica o Teorema de Dirichlet para provar que existe uma infinidade de números primos que não pertencem a pares de números gémeos.
7. Mostra que $p_n < p_1 + p_2 + \cdots + p_{n-1}$ se $n > 3$.
8. Prova que entre n e $2n$ existem aproximadamente tantos primos como entre 1 e n.

Desafios

1. Mostra que a progressão aritmética $73n + 2011$ tem uma infinidade de termos que são o produto de $14^{5^{2011}}$ primos distintos.
2. Mostra que se n é um inteiro maior do que 1 então $n^5 + n^4 + 1$ não é primo.