12. Classes de congruência

Dado um número natural n e um inteiro a, a classe de congruência de a módulo n é o conjunto

$$[a]_n = \{x \in \mathbb{Z} : x = a \mod n\}.$$

Quando n está fixado e não há risco de confusão, podemos escrever apenas $\overline{a}$ em vez de $[a]_n$. Definimos o conjunto de todas as classes de congruência módulo n por

$$\mathbb{Z}_n = \{\overline{a} : a \in \mathbb{Z}\} = \left\{\overline{0}, \overline{1}, \dots, \overline{n-1}\right\}.$$

Definimos em $\mathbb{Z}_n$ uma operação de adição por

$$\overline{a} + \overline{b} = \overline{a+b}$$

e um produto por

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Chamamos inverso de um elemento $\overline{a}$ em $\mathbb{Z}_n$ a um elemento $\overline{a'}$ tal que

$$\overline{a} \cdot \overline{a'} = \overline{1}.$$

Se $\overline{a}$ admite inverso, dizemos que $\overline{a}$ é invertível. Dizemos que um elemento não nulo $\overline{a} \in \mathbb{Z}_n$ é um divisor de zero se existe um elemento não nulo $\overline{b} \in \mathbb{Z}_n$ tal que

$$\overline{a} \cdot \overline{b} = \overline{0}.$$

Algoritmo RSA

O algoritmo RSA é um algoritmo utilizado em criptografia de chave pública. Funciona da seguinte maneira:

Geração da chave. São escolhidos dois números primos distintos, p e q. Seja $n = pq$ e seja $\phi(n) = (p-1)(q-1)$. Seja e um natural tal que $1 < e < \phi(n)$ e $\operatorname{mdc}(e, \phi(n)) = 1$. Seja d um natural tal que $\overline{d}$ é o inverso de $\overline{e}$ em $\mathbb{Z}_{\phi(n)}$, isto é

$$ed = 1 \mod \phi(n).$$

O par (n, e) será a chave pública e o natural d será a chave privada.

Encriptar. Para encriptar uma mensagem que esteja codificada num número m tal que $0 < m < n$, encontramos um natural c, com $c < n$, tal que

$$c = m^e \mod n,$$

isto é, calculamos em $\mathbb{Z}_n$ a classe $[m^e]_n$

Desencriptar. Para recuperar a mensagem inicial, calculamos a classe

$$\left[c^d\right]_n$$

e obtemos $[m]_n$

1. Construa as tabelas de adição e multiplicação de $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_6$, $\mathbb{Z}_7$ e $\mathbb{Z}_{12}$. Em cada caso, identifique os elementos invertíveis e os divisores de zero.

2. (a) Mostre que se p é primo e $0 < k < p$, então $\binom{p}{k}$ é múltiplo de p.
   (b) Dê exemplo de um par de naturais n e k, com $0 < k < n$ tal que $\binom{n}{k}$ não é múltiplo de n.
   (c) Utilizando o binómio de Newton e a alínea (2a), mostre que em $\mathbb{Z}_p$,
   $$\left(\overline{a} + \overline{b}\right)^p = \overline{a}^p + \overline{b}^p.$$

3. Considere a chave pública $(33, 7)$ para o algoritmo RSA.
   (a) Faça a encriptação do número 30.
   (b) Calcule a chave privada d para o algoritmo RSA (é necessário descobrir os primos p e q).
   (c) Faça a desencriptação do número obtido na alínea (3a).

4. Com a ajuda de um computador, e considerando os primos $p = 47$ e $q = 43$ e a chave pública $(1932, 335)$, calcule a chave privada d para o algoritmo RSA. Faça a encriptação e a desencriptação do número 999.