Introdução à Teoria dos Números
Ficha 4: primeiras noções de Aritmética Modular

Exercício 0.1 *Existe algum inteiro n tal que n^2+n+1 é divisível por 5? Encontrar um n tal que n^2+n+1 é divisível por 7; encontrar uma sucessão infinita de inteiros com essa propriedade.*

Exercício 0.2 *Qual o resto na divisão de* 20131400046512945769349674927 *por 4? Notar que*

$$20131400046512945769349674927 = 2013140004651294576934967 49\times 10^2+27.$$

Seja $n=4m+r$ com $0\leq r<4$; quais os possíveis restos na divisão de n^2 por 4?
Existe algum n inteiro tal que $n^2 =$ 20131400046512945769349674927?

Seja $m>1$. Dois inteiros a e b dizem-se **congruentes** módulo m

$$a\equiv b \mod m$$

se m divide $a-b$.
Portanto, qualquer inteiro é congruente módulo m a um único $0\leq a<m$.
O conjunto de todos os inteiros congruentes, módulo m, a um certo $0\leq a<m$ chama-se uma classe de congruência módulo m.

Exercício 0.3 *Verificar que se $a\equiv b \mod m$ e $c\equiv d \mod m$ então*

$$a+c\equiv b+d \mod m \qquad ac\equiv bd \mod m$$

As tabuadas de soma e multiplicação módulo 4 são

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Exercício 0.4 *Escrever as tabuadas da soma e multiplicação módulo* 7*.*

Exercício 0.5 *Notando que* $2^3 \equiv 1 \mod 7$*, calcular o resto na divisão de* 2^{74} *por* 7*.*

Exercício 0.6 *Quais as classes de congruência módulo* 12 *que estão contidas na classe de congruência de* 1 *módulo* 4*?*