Elementos de Matemática Finita

Trabalho para casa

Esta ficha de trabalho tem duas partes, I e II. A resolução **da parte I** deve ser entregue até às 14.00 do dia 28/10 (início da aula da próxima quarta-feira). Se for necessário, o trabalho pode ser entregue por correio electrónico.
Os problemas da segunda parte são uma preparação para as próximas aulas e não é necessário entregar a sua resolução .

I 1. Resolver, usando o Teorema Chinês dos Restos, a equação modular

$$1368x \equiv 81 \mod 2079.$$

2. a) Mostrar que se p é um primo ímpar, a equação $x^2 \equiv 1 \mod p^t$, tem exactamente duas soluções módulo p.

   b) Sejam $p_1, p_2, \cdots, p_m$ primos ímpares, e $t_1, t_2, \cdots, t_m$ inteiros positivos. Se $M = \prod_{i=1}^{m} p_i^{t_i}$, quantas soluções distintas módulo M tem a equação $x^2 \equiv 1 \mod M$?

3. Escolher três primos p_1, p_2, p_3, e determinar três inteiros consecutivos tais que o menor deles é divisível por p_1^3, o seguinte por p_2^3 e o maior por p_3^3.

4. Mostrar, usando uma ideia semelhante à do problema anterior, que existem sequências arbitrariamente longas de inteiros consecutivos que não sãprimos (ou seja, os intervalos entre primos consecutivos podem ser arbitrariamente grandes).

II 1. Determinar, para cada classe de congruência $a \mod 7$, e em função do expoente $k > 0$, a classe de congruência de a^k. Repetir o problema para o módulo 9.

2. Seja p primo e $0 < a < p$. Mostrar que a função

$$f : \mathbb{Z}_{/p} \to \mathbb{Z}_{/p}, \qquad f(x) = ax \mod p$$

é uma bijecção. Concluir que

$$\prod_{k=1}^{p-1} k \equiv \prod_{k=1}^{p-1} (ak) \mod p.$$

3. Deduzir o chamado pequeno Teorema de Fermat: Se p é primo e a não é divisível por p, $a^{p-1} \equiv 1 \mod p$.

4. Qual o resto na divisão de 3^{748} por 31?