MAC 105 – Fundamentos de Matemática para Computação

3ª Lista de Exercícios 1.0 – 8/6/2017 – Não vale nota

A maior parte desses exercícios pedem, ou para argumentar/fazer contas $\pmod p$ ou para trabalhar em $\mathbb{Z}_p$. É mais questão de conveniência: algo que nos inteiros se expressa como $\equiv \pmod p$, em $\mathbb{Z}_p$ se expressa como igualdade.

1. Resolva, em inteiros, as seguintes equações, ou mostre, conforme o caso, que não tem solução:
   (a) $250x - 147y = 12$
   (b) $363x - 48y + 135z = 2017$
   (c) $26x \equiv 1 \pmod{31}$
2. Note que as noções de "divisor comum" e "máximo divisor comum" têm sentido para qualquer conjunto de inteiros, não só para conjuntos de tamanho 2. Com isso, mostre que *se* $a, b, c \in \mathbb{Z}$*, então*
$$\text{mdc}(a, b, c) = \text{mdc}(\text{mdc}(a, b), c).$$
3. Prove que se p é primo, e $a \in \mathbb{Z}_p$, a equação $x^2 = a$ tem no máximo duas raízes em $\mathbb{Z}_p$ (ou seja, cada elemento de $\mathbb{Z}_p$ tem no máximo duas raízes quadradas). Dê um exemplo, com p composto, de um elemento $a \in \mathbb{Z}_p$ que tem mais que duas raízes quadradas.
4. Se p é primo, e $0 \neq a \in \mathbb{Z}_p$, então sabemos que existe $x \in \mathbb{Z}_p$ tal que $ax = 1$. Dizemos que x é o *inverso* de a. Mostre que:
   (a) Cada elemento não nulo de $\mathbb{Z}_p$ tem um único inverso.
   (b) Os únicos elementos de $\mathbb{Z}_p$ que são iguais ao seu inverso são 1 e -1.
5. Prove o Teorema de Wilson: *Se* p *é um primo positivo, então* $(p-1)! \equiv -1 \pmod p$.
6. Prove que se p é primo, $x, y \in \mathbb{Z}$ e $xy \equiv 0 \pmod p$, então $x \equiv 0 \pmod p$ ou $y \equiv 0 \pmod p$. Mostre que essa implicação não é verdadeira se p for composto.
7. Mostre que se p é primo e $r, s \in \mathbb{N}$ são tais que $r \equiv s \pmod{p-1}$, então, para todo $x \in \mathbb{Z}_p$, $x^r = x^s$.
8. Calcule o resto da divisão de $(1234^{567} + 8)^{910}$ por 11.