FMC1, 2016.1
(Turma do Thanos)

Prova 3
12.0 pts, max: 10.0

Nome:

Consulta

(Considere p primo onde aparece; o resto, inteiros.)

$$d \mid a \;\&\; d \mid b \implies d \mid ax + by \tag{3.1}$$
$$a \mid b \;\&\; b \mid c \implies a \mid c \tag{3.2}$$
$$a \mid b \;\&\; b \mid a \implies a = \pm b \tag{3.3}$$

$$p \mid ab \implies p \mid a \text{ ou } p \mid b \tag{3.4}$$
$$(c, a) = 1 \;\&\; c \mid ab \implies c \mid b \tag{3.5}$$

$$(a, b) = d \implies \text{existem } s, t \in \mathbb{Z} \text{ tais que } d = sa + tb \tag{3.6}$$
$$(a, m) = 1 \implies \text{existe } a^{-1} \pmod{m} \tag{3.7}$$

$$(m, n) = 1 \implies \phi(mn) = \phi(m)\phi(n) \tag{3.8}$$
$$(a, m) = 1 \implies a^{\phi(m)} \equiv 1 \pmod{m} \qquad \text{(Euler)}$$
$$(a, p) = 1 \implies a^{p-1} \equiv 1 \pmod{p} \qquad \text{(pequeno Fermat)}$$
$$(a, p) = d \implies a^{p} \equiv a \pmod{p} \qquad \text{(Fermat)}$$

Boas provas!

A (3 pts)

Sejam $a, b \in \mathbb{Z}$, com $b > 0$. O algoritmo da divisão nos dá $q, r \in \mathbb{Z}$, tais que:

$$a = bq + r, \qquad 0 \leq r < b.$$

(1.5) **A1.** Prove que $(a, b) = (b, r)$.

(1.5) **A2.** Explique porque o algoritmo sempre termina.

B (3 pts)

(0.7) **B1.** Ache o $(101, 174)$.

(0.8) **B2.** Escreva o $(101, 174)$ como *combinação linear* de 101 e 174, ou seja, ache $s, t \in \mathbb{Z}$ tais que:

$$(101, 174) = 101s + 174t.$$

(1.5) **B3.** Ache $x, y \in \mathbb{Z}$ tais que

(0.7 + 0.8) (i) $174x \equiv 1 \pmod{101}$; (ii) $101y \equiv -2 \pmod{174}$

C (3 pts)

(3.0) Ache um x tal que o sistêma de equações seguinte é satisfeito:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ 3x &\equiv 1 \pmod 4 \\ 4x &\equiv 1 \pmod 5 \\ 5x &\equiv 2 \pmod 7 \end{aligned}$$

D (3 pts)

Pela definição, a função "totient" de Euler conta os números coprimos com sua entrada:

$$\phi(n) = |\,\{c \in \mathbb{N} \mid 1 \leq c \leq n \;\;\&\;\; (c, n) = 1\}\,|.$$

(0.7) **D1.** Seja p primo. Calcule o somatório $\sum_{i=1}^{k} \phi(p^i)$.

(0.7) **D2.** Calcule o $\phi(75)$.

(1.6) **D3.** Ache $x, y \in \mathbb{Z}$ tais que:

(0.8 + 0.8) (i) $2^{42} \equiv x \pmod{75}$; (ii) $2^{2^{11}} \equiv y \pmod{75}$.

Nada mais.