MAT0164 - Trabalho 3 (28/06/2023)

Nomes:
Números USP:
Assinaturas:

1) **(3 pontos)** Sejam a, b, n inteiros e k um inteiro positivo.

(a) Prove que, se $n \mid a-b$, então $n \mid a^k - b^k$.

(b) Prove que, se $n \mid a-b$ e k é ímpar, então $n \mid a^k + b^k$.

(c) Prove que não existe um polinômio P de coeficientes inteiros tal que $P(7) = 11$ e $P(11) = 13$.

Solução

(a) Se $n \mid a-b$, então existe um $q \in \mathbb{Z}$ tal que $a - b = nq$. Assim, observe que

$$a^k - b^k = (a-b)\left(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}\right) =$$

$$(a-b)\left(\sum_{i=0}^{k-1} a^i b^{k-1-i}\right) = nq\left(\sum_{i=0}^{k-1} a^i b^{k-1-i}\right)$$

Logo, $n \mid a^k - b^k$.

(b) Se $n \mid a-b$, então existe um $q \in \mathbb{Z}$ tal que $a - b = nq$. Assim, observe que

$$a^k + b^k = (a-b)\left(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}\right) =$$

$$(a-b)\left(\sum_{i=0}^{k-1} a^i b^{k-1-i}\right) = nq\left(\sum_{i=0}^{k-1} a^i b^{k-1-i}\right)$$

Logo, $n \mid a^k + b^k$ se k for ímpar.

(c) Vamos provar que se P é um polinômio com coeficientes inteiros, então $a-b \mid P(a)-P(b)$. Suponha sem perda de generalidadde que P possui grau n. Então ele deve ser da forma

$$P(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_1 x + \alpha_0 = \sum_{i=0}^{n} \alpha_i x^i,$$

Assim, note que

$$\begin{aligned} P(a) - P(b) &= \alpha_n(a^n - b^n) + \alpha_{n-1}(a^{n-1} - b^{n-1}) + \ldots + \alpha_1(a-b) \\ &= (a-b)(\alpha_n \left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right) \\ &+ \alpha_{n-1}\left(a^{n-2} + a^{n-3}b + \cdots + ab^{n-3} + b^{n-2}\right) + \ldots + \alpha_1) \end{aligned}$$

Ou sucintamente,

$$\begin{aligned} P(a) - P(b) &= \sum_{i=1}^{n} \alpha_i (a-b)^i \\ &= \sum_{i=1}^{n} \alpha_i (a-b) \sum_{k=0}^{i-1} a^k b^{i-1-k} \\ &= (a-b)\left(\sum_{i=1}^{n} \alpha_i \sum_{k=0}^{i-1} a^k b^{i-1-k}\right) \end{aligned}$$

Portanto, concluímos que $a-b \mid P(a)-P(b)$.
Suponha por contradição que existe P como no enunciado. Então teríamos que $11-7 \mid P(11)-P(7)$, ou seja, que $4 \mid 2$, uma contradição.

2) (3 pontos)

(a) Seja a um inteiro e m um inteiro positivo. Prove que $a^m - 1 = (a-1)(a^{m-1} + a^{m-2} + \cdots + a + 1)$.

(b) Prove que, se $a \neq 1$ é um inteiro e m é um inteiro positivo, então $\text{mdc}\left(\frac{a^m - 1}{a-1}, a - 1\right) = \text{mdc}(a-1, m)$.

Solução

(a) Vamos mostrar o resultado por indução em m.
Caso Base: $m = 1$ Temos que

$$a^1 - 1 = a - 1 = (a-1) \cdot 1;$$

Hipótese: Suponha que $a^m - 1 = (a-1)(a^{m-1} + a^{m-2} + \cdots + a + 1)$ para certo $m = k \geq 2$, ou seja,

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1).$$

Passo Indutivo: Vamos provar que o resultado vale para $n = k + 1$, ou seja, que

$$a^{k+1} - 1 = (a-1)(a^k + a^{k-1} + \cdots + a + 1).$$

Observe que

$$\begin{aligned} a^{k+1} - 1 &= a \cdot a^k - 1 \\ &= (a-1)a^k + a^k - 1 \\ &\overset{Hip.}{=} (a-1)a^k + (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1) \\ &= (a-1)(a^k + a^{k-1} + a^{k-2} + \cdots + a + 1) \end{aligned}$$

Assim, provamos utilizando o princípio da indução finita que $a^m - 1 = (a-1)(a^{m-1} + a^{m-2} + \cdots + a + 1)$ para todo $m \geq 1$.

(a) Observe que

$$\frac{a^m - 1}{a-1} = a^{m-1} + a^{m-2} + \cdots + a + 1 = (a-1)(a^{m-2} + 2a^{m-3} + \ldots + (m-2)a + (m-1)) + m.$$

Logo, pelo Algoritmo de Euclides, temos que

$$\text{mdc}\left(\frac{a^m - 1}{a-1}, a - 1\right) = \text{mdc}(a-1, m).$$

3) (4 pontos) Seja n um inteiro positivo.

(a) Prove que, se $2^n - 1$ é primo, então n é primo.

(b) Prove que, se $2^n + 1$ é primo, então $n = 2^t$ para algum t natural.
Sugestão: em ambos os itens, prove a contrapositiva, ou seja, que a negação da conclusão implica a negação da hipótese.

Solução

(a) Suponha que n não é primo. Vamos provar que $n^n - 1$ também não é primo.
Se n não é primo, então existem x, y tais que $n = xy$. Logo,

$$2^n - 1 = 2^{xy} - 1 = (2^x)^y - 1 = (2^y - 1)(2^{y(x-1)} + 2^{y(x-2)} + \ldots + 2^y + 1)$$

Logo, concluímos que $2^y - 1$ divide $2^{xy} - 1$, e portanto não pode ser um número primo.

(b) Suponha que n não é da forma 2^t. Logo, n admite um primo ímpar p como divisor. Assim, $n = pk$ para algum k natural. Desse modo,

$$2^{pk} + 1 = (2^k + 1)(2^{k(p-1)} - 2^{k(p-2)} + \ldots - 2^k + 1)$$

assim, $2^n + 1$ é composto.