Ordem! Ordem!

Diego Eloi

8 de janeiro de 2017

Tudo na vida precisa de ordem. Seria estranho na matemática não haver um ente sequer com este nome...Dado $n > 1$ um inteiro fixado e a um inteiro tal que $mdc(a, n) = 1$. Dizemos que m é a *ordem de a módulo n*, quando m for o menor natural tal que $a^m \equiv 1(mod\ n)$. Perceba que não faz sentido considerar $mdc(a, n)$ diferente de 1, pois, caso isso acontecesse, teríamos $a^m \equiv 1(mod\ n) \Rightarrow a^m - n.k = 1$, para algum $k \in \mathbb{Z}$ e daí como a e n são divisíveis por um $d = mdc(a, n)$, então $d|1 \Rightarrow d = 1, -1$. Denotaremos por $m = ord_n^a$ a ordem de a módulo n.

Proposição Seja $m = ord_n^a$. Se existe um t natural tal que $a^t \equiv 1(mod\ n)$, então $m|t$.

Prova: Suponha que m não divide t. Por definição, m é a menor potência, então $m \leq t$. Pelo algoritmo de Euclides, existem q,$r \in \mathbb{Z}$ tais que $t = q.m + r$ com $r < m$. Daí, $a^t \equiv 1(mod\ n) \Leftrightarrow a^{qm+r} \equiv 1(mod\ n) \Leftrightarrow (a^m)^q a^r \equiv a^r \equiv 1(mod\ n)$. Logo, existe um $r < m$ tal que $a^r \equiv 1(mod\ n)$, o que é um absurdo, pois m é o menor possível.

Observações: 1. Lembrando que, para a e n com $mdc(a, n) = 1$ vale o Teorema de Euler, ou seja, $a^{\varphi(n)} \equiv 1(mod\ n)$, pela proposição anterior, temos que $ord_n^a|\varphi(n)$.

2. Se $a^m \equiv a^k \equiv 1(mod\ n) \Rightarrow m \equiv k(mod\ ord_n^a)$.

Exercício: Encontre o menor n tal que $2^{2005}|17^n - 1$.

Solução: Queremos encontrar $ord_{2^{2005}}^{17}$ e sabemos que $ord_{2^{2005}}^{17}|\varphi(2^{2005}) = 2^{2004}$. Logo, $ord_{2^{2005}}^{17} = 2^k$ para algum $k \in \{1, 2, 3, ..., 2004\}$. Daí, $17^{2^k} \equiv 1(mod\ 2^{2005})$ e também temos

$$17^{2^k} - 1 = (17 - 1)(17 + 1)(17^2 + 1)...(17^{2^{k-1}} + 1)$$

Perceba agora que, se $i \geq 0$, o número $17^{2^i} + 1$ é múltiplo de 2, mas não de 4. Daí, temos que o menor k que satisfaz isso é 2001, então $ord_{2^{2005}}^{17} = 2^{2001}$.

Exercício: Mostre que $n|\varphi(a^n - 1)$ para todo inteiro positivo $a > 1$.

Exercício: Mostre que não existe um inteiro $n > 1$ tal que $n|2^n - 1$.

Os números a tais que $ord_n^a = \varphi(n)$ recebem um nome específico. Quando isso acontece, dizemos que a é *raiz primitiva* módulo n. Procure sempre lembrar do teorema abaixo:

Teorema Existe uma raiz primitiva módulo n se, e somente se $n \in \{2, 4, p^k, p^k\}$, onde p é um primo ímpar.

Problema 1 Encontre todos os primos p e q tais que $p^2 + 1|2003^q + 1$ e $q^2 + 1|2003^p + 1$.

Problema 2 Encontre todos as triplas de primos (p, q, r) tais que

$$p|q^r + 1, q|r^p + 1, r|p^q + 1$$

Problema 3 Encontre todos os primos p e q tais que $pq|2^p + 2^q$.

Problema 4 Encontre a ordem de 2 módulo 101.

Problema 5 (PUTNAM/94) Para todo inteiro a, considere o número

$$n_a = 102a - 100.2^a$$

Mostre que para $0 \leq a, b, c, d \leq 99$ temos $n_a + n_b = n_c + n_d (mod\ 10100)$.

Problema 6 Mostre que não existe nenhum n tal que $3^n - 2^n$ seja divisível por n.

Problema 7 Prove que $p^p - 1$ tem um fator primo da forma $kp + 1$.

Problema 8 (IMO/90) Encontre todos os inteiros positivos n tais que $n^2|2^n + 1$.

Problema 9 Seja $p = 2^n + 1$ um número primo. Prove que 3 é raiz primitiva módulo p.

Problema 10 Seja p um primo ímpar e sejam q e r primos tais que $p|q^r + 1$. Prove que ou $2r|p - 1$ ou $p|q^2 - 1$.

Problema 11 Sejam $a > 1$ e n inteiros positivos. Se p é um divisor primo de $a^{2^n} + 1$, prove que $2^{n+1}|p - 1$.