TREINAMENTO EGMO 2021

Profª Ana Paula Chaves
apchaves@ufg.br
https://apchaves.ime.ufg.br/

• Ordem de Elementos de $\mathbb{Z}_m$ •

Resumo: *Dentre os conceitos advindos da Álgebra Abstrata mais utilizados na resolução de problemas, seguramente está o de* ordem. *Nesse texto, vamos exibir alguns dos resultados mais clássicos sobre o tema, restringindo nosso universo aos inteiros módulo m, e aplicá-los na resolução de alguns problemas de olimpíada. Também são propostos alguns problemas ao final, para deleite do(a) leitor(a).*

1. INTRODUÇÃO

Dados dois inteiros $a \in \mathbb{Z}$ e $m \in \mathbb{N}$, tais que $(a,m) = 1$, sabemos, pelo *Teorema de Euler*, que $a^{\phi(m)} \equiv 1 \pmod{m}$. Uma questão natural que podemos levantar é: pode existir uma potência menor de a que é congruente a 1 módulo m? Se pensamos um pouco, rapidamente produzimos um exemplo onde isso ocorre. Considere $a = 4$ e $m = 5$. Temos que $\phi(5) = 4$, mas $4^2 \equiv 1 \pmod{5}$, e 4^2 é a menor potência de 4 congruente a 1 módulo 5. Essa *menor potência*, ou como veremos a posteriori a *ordem*, é nosso interesse principal.

Já vimos que o conjunto $A = \{d \in \mathbb{N};\ a^d \equiv 1 \pmod{m}\}$ é não vazio, pois $\phi(m) \in A$. Assim, pelo *Princípio da Boa Ordem*[*], A possui um elemento minimal. Este elemento minimal, ou seja, o menor $n \in \mathbb{N}$ tal que $a^n \equiv 1 \pmod{m}$, é dito a *ordem de a módulo m*, cuja notação é dada comumente por $ord_m(a)$ ou $o_m(a)$[†].

Exemplo 1.1. A ordem de 2 módulo 9 é 6, já que $2^1 \equiv 2 \pmod{9}$, $2^2 \equiv 4 \pmod{9}$, $2^3 \equiv 8 \pmod{9}$, $2^4 \equiv 7 \pmod{9}$, $2^5 \equiv 5 \pmod{9}$ e $2^6 \equiv 1 \pmod{9}$.

Nosso objetivo neste texto é fornecer os resultados mais utilizados na resolução de problemas de olimpíada, que envolvem a ordem de um elemento em $\mathbb{Z}_m$, colocando-os em prática com alguns problemas resolvidos no *Warm-up*, e deixando alguns problemas interessantes na subseção de *Problemas Propostos*.

[*] Todo subconjunto não vazio de $\mathbb{N}$, possui um elemento minimal.

[†] Vale a pena ressaltar que o conceito de *ordem* é bem mais geral. Dado um grupo $(G,\times)$, escrito multiplicativamente, com identidade e, denominamos a *ordem de* $a \in G$, pelo menor $d \in \mathbb{N}$ tal que $a^d = e$.

Na próxima seção, *Fatos que Ajudam*, vamos exibir e demonstrar alguns dos resultados mencionados anteriormente.

2. Fatos que Ajudam

O primeiro resultado que vamos enunciar, é extremamente importante e será usado diversas vezes durante o texto.

Teorema 2.1. Sejam a e m inteiros positivos, tais que $(a,m) = 1$. Então,

$$a^n \equiv 1 \pmod{m} \Leftrightarrow ord_m(a)|n.$$

Demonstração. Note que a volta é imediata, donde vamos nos ocupar apenas da ida. Suponha que $a^n \equiv 1 \pmod{m}$. Efetuando a divisão euclideana de n por $ord_m(a)$, obtemos $n = q \cdot ord_m(a) + r$, onde $0 \leq r < ord_m(a)$. Assim, obtemos,

$$a^r \equiv (a^{ord_m(a)})^q a^r \equiv a^n \equiv 1 \pmod{m},$$

ou seja, $a^r \equiv 1 \pmod{m}$ e, caso $r \neq 0$, teríamos uma contradição com o fato de $ord_m(a)$ ser minimal, já que $r < ord_m(a)$. Portanto, $r = 0$ e finalizamos a prova. □

Como consequência imediata, temos o seguinte corolário:

Corolário 2.1. Se a e m inteiros positivos, são tais que $(a,m) = 1$, então

$$ord_m(a)|\phi(m).$$

Exemplo 2.1. Dado $a \in \mathbb{N}$, encontrar $ord_{a^n-1}(a)$, para todo $n \in \mathbb{N}$.

Solução: Primeiro, observe que $a^n \equiv 1 \pmod{a^n-1}$, donde $ord_{a^n-1}(a) \leq n$. Por outro lado, temos que, se $0 < x < n$, então $a^x - 1 < a^n - 1$, não podendo haver x em tal intervalo tal que $a^x - 1$ é múltiplo de $a^n - 1$, i. e., de modo que $a^x \equiv 1 \pmod{a^n-1}$. Portanto, $ord_{a^n-1}(a) = n$.

Também como consequência do Teorema 2.1, temos:

Corolário 2.2. Temos que $a^l \equiv a^n \pmod{m}$, se, e somente se, $l \equiv n \pmod{ord_m(a)}$.

Demonstração. Novamente, observe que a volta é imediata, e vamos nos ocupar apenas da ida. De fato, suponha SPG que $l \geq n$. Então, como $(a,m) = 1$, "dividimos"ambos os lados da congruência $a^l \equiv a^n \pmod{m}$, para obter $a^{l-n} \equiv 1 \pmod{m}$, donde, pelo Teorema 2.1, isso implica em $ord_m(a)|l-n$, ou seja, $l \equiv n \pmod{m}$, como desejamos. □

3. PROBLEMAS

3.1. **Warm-up.**

Problema 3.1: (AIME 2001) *Quantos inteiros positivos múltiplos de* 1001 *podem ser escritos da forma* $10^j - 10^i$*, onde* i *e* j *são inteiros e* $0 \leq i < j \leq 99$*?*

Solução: Note que, se $1001|10^j - 10^i$, então $10^j \equiv 10^i \pmod{1001}$, e, como $(1001, 10) = 1$, temos pelo Corolário 2.2 que $j \equiv i \pmod{ord_{1001}(10)}$. Assim, precisamos encontrar $ord_{1001}(10)$ para continuar. Essa tarefa não é muito árdua, pois como $10^3 \equiv -1 \pmod{1001}$, temos $10^6 \equiv 1 \pmod{1001}$, e já que $10, 10^2, \ldots, 10^5$ não são congruentes a 1 módulo 1001, concluímos que $ord_{1001}(10) = 6$. Com isso, traduzimos o nosso problema em contar os pares (i, j) de inteiros positivos distintos, com $0 \leq i < j \leq 99$, tais que $i \equiv j \pmod 6$. Perceba que, se $i \equiv j \equiv 0 \pmod 6$, como temos precisamente 17 múltiplos de 6 no intervalo $[0, 99]$, a quantidade de pares desejados é $\binom{17}{2} = 136$. O mesmo também vale para $i \equiv j \equiv 1, 2$ ou $3 \pmod 6$, nos dando uma parcial de $4 \cdot 136 = 544$ pares. Nos casos em que $i \equiv j \equiv 4$ ou $5 \pmod 6$, temos 16 números no intervalo $[0, 99]$ satisfazendo tais congruências, nos dando $\binom{16}{2} = 120$ pares em cada caso, somando 240. Contando todos os pares encontrados, obtemos 784 no total.

Problema 3.2: *Mostre que, se* p *é primo, então todo fator primo de* $2^p - 1$ *é maior que* p*.*

Solução: Tome q um primo, tal que $q|2^p - 1$. Com isso, $q \neq 2$, e como $2^p \equiv 1 \pmod q$, temos pelo Teorema 2.1 que $ord_q(2)|p$, donde, como p também é primo, conseguimos $ord_q(2) \in \{1, p\}$. Como, é imediato que $ord_q(2) \neq 1$, então $ord_q(2) = p$. Por outro lado, como $(2, q) = 1$, sabemos, pelo Corolário 2.1, que $ord_q(2)|\phi(q) = q - 1 \Rightarrow p|q - 1$. Assim, $q - 1 \geq p$, donde $q \geq p + 1 > p$, como queríamos.

Problema 3.3: *Sejam* $a > 1$ *e* n *inteiros positivos. Se* p *é um primo ímpar, divisor de* $a^{2^n} + 1$*, mostre que* p *é congruente a* 1 *módulo* 2^{n+1}*.*[‡]

Solução: Como p é um primo ímpar, tal que $p|a^{2^n} + 1$, então $p \nmid a^{2^n} - 1$ o que nos dá $p|(a^{2^n} + 1)(a^{2^n} - 1) = a^{2^{n+1}} - 1$. Assim, $a^{2^{n+1}} \equiv 1 \pmod p \quad \Rightarrow \quad ord_p(a)|2^{n+1}$. Agora, vamos mostrar que $ord_p(a)$ é exatamente 2^{n+1}. De fato, se tivéssemos $ord_p(a)|2^{n+1}$, então pelo Teorema 2.1, $a^{2^n} \equiv 1 \pmod p \quad \Rightarrow p|a^{2^n} - 1$, mas vimos que isso não pode acontecer. Portanto, $ord_p(a) = 2^{n+1}$. Por outro lado, como $(a, p) = 1$, temos pelo Corolário 2.1,

$$2^{n+1} = ord_p(a)|\phi(p) = p - 1 \quad \Rightarrow \quad p \equiv 1 \pmod{2^{n+1}},$$

como queríamos.

[‡]Observe que esse resultado implica que todo divisor primo do *n-ésimo número de Fermat*, $2^{2^n} + 1$, é congruente a 1 módulo 2^{n+1}.

Problema 3.4: (Coreia IMO TST 2003) *Dado um primo p, seja $f_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.*

a) Se $p|m$, mostre que existe um fator primo de $f_p(m)$ que é relativamente primo com $m(m-1)$.

b) Mostre que existem infinitos n tais que $pn+1$ é primo.

Solução:

a) Na verdade, qualquer fator primo de $f_p(m)$, quandp $p|m$, é coprimo com $m(m-1)$. Com efeito, tome um fator primo qualquer $q|f_p(m)$. É imediato que $q \not| m$, já que, caso contrário $q|m^{p-1} + m^{p-2} + \cdots + m + 1$ e $q|m$, nos dá $q|1$, um absurdo. Agora, vamos mostrar que $(q, m-1) = 1$. De fato, se $q|m-1$, então $m \equiv 1 \pmod{p}$. Daí,

$$p \equiv m^{p-1} + m^{p-2} + \cdots + m + 1 = f_p(m) \equiv 0 \pmod{q} \quad \Rightarrow \quad q|p.$$

Por outro lado, também temos por hipótese que $p|m$, donde $q|m$, um absurdo. Portanto, $(q, m(m-1)) = 1$.

b) Primeiro, vamos mostrar, usando o item **a)**, que os fatores primos de $f_p(m)$, quando $p|m$, são todos da forma $pn+1$. Seja q um desses fatores primos. Então,

$$\begin{aligned} q|f_p(m) = m^{p-1} + m^{p-2} + \cdots + m + 1 \quad &\Leftrightarrow \quad q|(m-1)(m^{p-1} + m^{p-2} + \cdots + m + 1) \\ &\Leftrightarrow \quad q|m^p - 1 \\ &\Leftrightarrow \quad m^p \equiv 1 \pmod{q} \\ &\Leftrightarrow \quad ord_q(m)|p, \end{aligned}$$

assim, $ord_q(m) \in \{1, p\}$. Se tivéssemos $ord_q(m) = 1$, então $m \equiv 1 \pmod{q} \Rightarrow q|m-1$, o que contradiz o que mostramos no item **a)**. Portanto, $ord_q(m) = p$, donde, como $(q, m) = 1$,

$$p = ord_q(m)|\phi(q) = q-1 \Rightarrow p|q-1,$$

o que nos dá $q \equiv 1 \pmod{p}$, como queríamos. Perceba que mostrar esse fato não nos garante a existência de infinitos primos da forma desejada, pois temos que garantir que existe uma sequência $(m_k)_k$, de inteiros, de modo que o conjunto dos divisores primos de $(f_p(m_k))_k$ seja infinito. Observe que, se garantimos a existência de $(m_k)_k$, tais que os valores $f_p(m_k)$ são dois a dois coprimos, resolvemos nosso problema. Lembrando que, para usar o que foi feito até aqui, precisamos que $p|m_k$, para todo k, se tomamos $m_1 = p$ e $m_2 = pf_p(m_1)$, então $(f_p(m_1), f_p(m_2)) = 1$, pois caso exista um fator primo q, em comum entre eles, teremos

$$q|f_p(m_1) \quad \text{e} \quad q|f_p(m_2) = (pf_p(m_1))^{p-1} + (pf_p(m_1))^{p-2} + \cdots + ((pf_p(m_1))) + 1 \Rightarrow \quad q|1,$$

um absurdo. Note que, se tomarmos $m_3 = pf_p(m_1)f_p(m_2)$, usando o mesmo argumento teremos $(f_p(m_3), f_p(m_1)) = (f_p(m_3), f_p(m_2)) = 1$. Generalizando tal construção, tomamos

$$m_k = pf_p(m_1)f_p(m_2)\cdots f_p(m_{k-1}),$$

e com isso $(f_p(m_k), f_p(m_i)) = 1$, para todo $1 \leq i < k$, o que finaliza o problema.

Problema 3.5: (Turquia EGMO TST 2017) *Encontre todos os pares* (p,q) *de números primos, tais que*

$$\frac{(2p^2-1)^q+1}{p+q} \quad e \quad \frac{(2q^2-1)^p+1}{p+q}$$

são ambos inteiros.

Solução: Pelo que foi dado, queremos

$$(2p^2-1)^q \equiv -1 \pmod{p+q} \text{ e } (2q^2-1)^p \equiv -1 \pmod{p+q}.$$

Como $q \equiv -p \pmod{p+q}$, a segunda congruência acima se torna $(2p^2-1)^p \equiv -1 \pmod{p+q}$. Elevando ao quadrado as duas congruências, obtemos

$$(2p^2-1)^{2q} \equiv 1 \pmod{p+q} \text{ e } (2p^2-1)^{2p} \equiv 1 \pmod{p+q},$$

donde, $ord_{p+q}(2p^2-1)|2q$ e $ord_{p+q}(2p^2-1)|2p$, nos dando

$$ord_{p+q}(2p^2-1)|(2p,2q) = 2(p,q). \tag{1}$$

Aqui, dividimos o problema em alguns casos:

- Caso $p \neq q$ sejam primos ímpares: Então $(p,q) = 1$, e por (1) temos $ord_{p+q}(2p^2-1) = 1$ ou 2. Como não podemos ter $ord_{p+q}(2p^2-1) = 1$, pois caso contrário, teríamos $(2p^2-1) \equiv 1 \pmod{p+q}$, o que combinado com $(2p^2-1)^q \equiv -1 \pmod{p+q}$ implica em $p+q|2$, um absurdo. Assim, $ord_{p+q}(2p^2-1) = 2$ e como $q \equiv 1 \pmod 2$, pelo Corolário 2.2

  $$-1 \equiv (2p^2-1)^q \equiv 2p^2-1 \pmod{p+q} \Rightarrow p+q|2p^2$$

  e como $p+q$ é par, enquanto p é ímpar, teremos $(p+q)/2|p^2$, e assim $(p+q)/2 \in \{1, p, p^2\}$. É imediato que não podemos ter $(p+q)/2 = 1$ ou p. Para $(p+q)/2 = p^2$, teremos $q = 2p^2 - p = p(2p-1)$, contradizendo o fato de q ser primo. Portanto, esse caso não nos dá soluções.
- Caso $p = q$: Observe que, o caso $p = q = 2$ não satisfaz as condições do problema. Assim, vamos agora supor $p = q$ ímpares. Neste caso, observe que sempre temos solução, pois $p+q = 2p$ e

  $$(2p^2-1)^p \equiv (-1)^p \equiv -1 \pmod{2p},$$

  portanto $((2p^2-1)^p+1)/(p+q) \in \mathbb{Z}$.
- Caso $p \neq q$, com um deles igual a 2: Como as condições são simétricas, podemos supor SPG que $p = 2$ e q é um primo ímpar. Com isso, temos

  $$49 \equiv (2\cdot 2^2-1)^2 \equiv (2q^2-1)^2 \equiv -1 \pmod{q+2} \Rightarrow q+2|50 \Rightarrow q = 3 \text{ ou } 23.$$

Por outro lado, usando a segunda congruência

$$7^q \equiv -1 \pmod{q+2}.$$

Se $q = 3$, note que $7^3 \equiv 3 \pmod 5$, não nos dando solução. Caso tenhamos $q = 23$, não é difícil encontrar $7^{23} \equiv -7 \pmod{25}$, e concluímos que também não há solução nesse caso.

Portanto, as únicas soluções possíveis são (p, p), onde p é um número primo ímpar.

3.2. **Problemas Propostos.**

Ressaltamos aqui que, nem todos os problemas abaixo precisam que você invoque o poder da *ordem*, para serem resolvidos. :)

Problema 3.6: *Sejam a e b inteiros positivos, coprimos com m, tais que $a^x \equiv b^x \pmod m$ e $a^y \equiv b^y \pmod m$. Mostre que*

$$a^{(x,y)} \equiv b^{(x,y)} \pmod{m}.$$

Problema 3.7: *Encontre o menor n inteiro positivo que satisfaz*

$$2^{2005} | 17^n - 1.$$

Problema 3.8: *Encontre todos os pares (p, q) de números primos tais que $p^2+1 | 2003^q+1$ e $q^2+1 | 2003^p+1$.*

Problema 3.9: *Prove que, se p é primo, então $p^p - 1$ tem um fator primo da forma $kp+1$.*

Problema 3.10: (Bulgária 1996) *Encontre todos os pares (p, q) de números primos tais que $pq | (5^p - 2^p)(5^q - 2^q)$.*

Problema 3.11: *Sejam $a, n > 2$ inteiros positivos tais que $n | a^{n-1} - 1$ e n não divide $a^x - 1$, para todo $x < n-1$, onde x é divisor de $n-1$. Mostre que n é primo.*

Problema 3.12: (Romênia 1996) *Encontre todos os pares de primos (p, q) para os quais a congruência*

$$\alpha^{3pq} \equiv \alpha \pmod{3pq},$$

é válida para todo $\alpha \in \mathbb{Z}$.

Problema 3.13: (EUA TST 2003) *Encontre todos os trios de primos* (p,q,r) *tais que* $p|q^r+1$, $q|r^p+1$ *e* $r|p^q+1$.

Problema 3.14: (China 2009) *Encontre todos os pares de primos* p,q *tais que*

$$pq|5^p+5^q.$$

REFERÊNCIAS

[1] T. Andreescu, Z. Feng, *101 Problems in Algebra*, Vol. 18, Australian Mathematics Trust, (2001) 139pp.

[2] T. Andreescu, D. Andrica, *Number Theory: Structures, Examples, and Problems*, Birkhäuser, Boston (2009) 404pp.

[3] F. B. Martinez, C. G. A. T. Moreira, N. Saldanha, E. Tengan, *Teoria dos Números: Um passeio com primos e outros números familiares pelo munto inteiro*, **3ª Ed.** (Projeto Euclides),IMPA, Rio de Janeiro, (2013) 497pp.

[4] P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul, *Basic Abstract Algebra*, Cambridge University Press, Cambridge, (1994) 487pp.

[5] S. Lang, *Algebra*, Graduate Texts in Mathematics **(211)**, Springer Science & Business Media, (2005) 914pp.

[6] Art of Problem Solving - https://artofproblemsolving.com/