XIX Semana Olímpica de Matemática

Nível 3

Polinômios Ciclotômicos e Congruência Módulo p

Samuel Feitosa

O projeto da XIX Semana Olímpica de Matemática foi patrocinado por:

impa
instituto nacional de matemática pura e aplicada

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

fundação lemann

Semana Olímpica 2016
Polinômios Ciclotômicos e congruências módulo p.
Nível 3

Samuel Feitosa

1 Ordens e Raízes Primitivas

Definição 1 O menor inteiro positivo k para o qual $a^k \equiv 1 \pmod{m}$, onde $mdc(a,m) = 1$, é chamado *ordem de a módulo m* e será denotado por $ord_m a$.

Teorema 1 Se a é um inteiro relativamente primo com m, então $a^n \equiv 1 \pmod{m}$ se, e somente se, $ord_m a | n$. Ademais, $a_0^n \equiv a_1^n \pmod{m}$ se , e somente se, $n_0 \equiv n_1 \pmod{ord_m a}$

Demonstração. Sejam $b = ord_m a$ e $n = qb + r$ com $0 \leq r < b$. Como $a^b \equiv 1 \pmod{m}$,

$$\begin{aligned} a^n \equiv 1 \pmod{m} &\Leftrightarrow a^{qb+r} \equiv 1 \pmod{m} \\ &\Leftrightarrow a^r \equiv 1 \pmod{m} \end{aligned}$$

Como $0 \leq r < b$, devemos ter $r = 0$. Usando que $mdc(a,m) = 1$ e supondo que $n_0 > n_1$,

$$\begin{aligned} a_0^n \equiv a_1^n \pmod{m} &\Leftrightarrow a^{n_0 - n_1} \equiv 1 \pmod{m} \\ &\Leftrightarrow n_0 - n_1 \equiv 0 \pmod{b} \end{aligned}$$

Corolário 1 Se $mdc(a,m) = 1$, $ord_m a | \phi(m)$

Demonstração. Pelo teorema de Euler, $a^{\phi(m)} \equiv 1 \pmod{m}$. O resultado segue do teorema anterior.

Exercício 1. (Putnam 1972) Prove que não existe inteiro positivo $n > 1$ tal que $n | 2^n - 1$.

Exercício 2. (Leningrado 1990) Prove que para todos os inteiros $a > 1$ e n , $n | \phi(a^n - 1)$.

Exercício 3. Mostre que

a) $ord_{3^n} 2 = 2 \cdot 3^{n-1}$

b) Se $2^m \equiv -1 \pmod{3^n}$, então $\Rightarrow 3^{n-1} \mid m$.

Exercício 4. (Bulgária 1997) Encontre todos os números inteiros $m, n \geq 2$ tais que

$$\frac{1 + m^{3^n} + m^{2 \cdot 3^n}}{n}$$

é um inteiro

Exercício 5. Prove que que se p é primo, então $p^p - 1$ tem um fator primo congruente a 1 módulo p

Exercício 6. Se $ord_a m = h, ord_m b = k$ e $mdc(h,k) = 1$ mostre que $ord_m ab = hk$.

Exercício 7. Prove que se a, b são números naturais tais que $a > b$, $n > 1$, então cada divisor primo do número $a^n - b^n$ é ou da forma $nk + 1$, onde k é um inteiro, ou um divisor de um número $a^{n_1} - b^{n_1}$, onde $n_1 | n$ e $n_1 < n$.

Exercício 8. Prove que se a, b são números naturais tais que $a > b$, $n > 1$, então cada divisor primo do número $a^n + b^n$ é ou da forma $2nk + 1$, onde k é um inteiro, ou um divisor de um número $a^{n_1} + b^{n_1}$, onde n_1 é o quociente obtido por dividir o número n por um número ímpar mairo que 1.

Exercício 9. Seja p um primo que não divide 10, e seja n um inteiro, $0 < n < p$. Seja d a ordem de 10 módulo p.

1. Mostre que o comprimento do período da representação decimal de n/p é d.
2. Prove que que se d é par, então o período da representação decimal de n/p pode ser dividido em duas partes cuja soma é $10^{d/2} - 1$. Por exmeplo, $1/7 = 0, \overline{142857}$, então $d = 6$, e $142 + 857 = 999 = 10^3 - 1$.

3. Se $ord_m a = h \Rightarrow ord_m a^k = \dfrac{h}{mdc(h,k)}$

Exercício 10. Se p é um primo maior que 3, então qualquer divisor maior que 1 do número $\dfrac{2^p+1}{3}$ é da forma $2kp+1$, onde k é um número natural.

Teorema 2 Se p é um primo maior que 2, então qualquer número natural que divida o número 2^p-1 é da forma $2kp+1$, onde k é um inteiro.

Exercício 11. (Bulgária 1995) Encontre todos os primos p e q tais que o número 2^p+2^q seja divisível por pq.

Exercício 12. Mostre que se $k>1$ então $2^{k-1} \not\equiv -1 \pmod{k}$

Exercício 13. Mostre que se $3 \leq d \leq 2^{n-1}$, então $d \nmid (a^{2^n}+1)$ para qualquer inteiro positivo a.

Exercício 14. (Eureka) Prove que se p é um primo da forma $4k+3$, então $2p+1$ também é primo se e somente se $2p+1$ divide 2^p-1.

Exercício 15. Prove que todos os divisores dos números de Fermat $2^{2^n}+1$, $n>1$, são da forma $2^{n+2}k+1$.

Exercício 16. (IMO 1990) Encontre todos os inteiros positivos $n>1$ tais que

$$\frac{2^n+1}{n^2}$$

é um inteiro.

Exercício 17. (Teste Cone Sul 2002) Encontre o período na representação decimal de $\dfrac{1}{3^{2002}}$.

Exercício 18. (Teste de Seleção do Irã para a IMO) Seja a um natural fixo. Mostre que o conjunto dos divisores primos de $2^{2^n}+a$, para $n \in \mathbb{N}$, é infinito.

Exercício 19. (Colômbia 2009) Encontre todas as triplas de inteiros positivos (a,b,n) que satisfazem a equação:

$$a^b = 1+b+\ldots+b^n.$$

Teorema 3 (Euler) Um inteiro a satisfazendo $mdc(a,p)=1$ é o resíduo de uma potência n-ésima nódulo p se e somente se vale a relação:

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p} \text{ com } d = mdc(p-1,n).$$

Exercício 20. (IMO 2003) Seja p um número primo. Demonstre que existe um número primo q tal que, para todo inteiro n, o número n^p-p não é divisível por q.

Exercício 21. (Olimpiada Indiana) Seja p um primo ímpar e seja r um natural ímpar. Mostre que $rp+1$ não divide p^p-1.

Exercício 22. Mostre que para quaisquer inteiros positivos ímpares a e b

$$mdc(2^a+1, 2^b+1) = 2^{mdc(a,b)}+1$$

Exercício 23. (Teste IMO 2003) Seja n um inteiro positivo, e sejam $p_1, p_2, \ldots, p_n$, primos distintos maiores que 3. Prove que $2^{p_1 p_2 \cdots p_n}+1$ tem pelo menos 4^n divisores.

Exercício 24. Ache todos os inteiros positivos n tais que vale $a^{n+1} \equiv a \pmod{n}$ para todo a inteiro.

Exercício 25. Mostre que se $k>1$ então $2^{k-1} \not\equiv -1 \pmod{k}$

Exercício 26. Prove que todos os divisores dos números de Fermat $2^{2^n}+1$, $n>1$, são da forma $2^{n+2}k+1$.

Exercício 27. (Putnam 1972) Prove que não existe um inteiro $n>1$ tal que $n|2^n-1$.

Exercício 28. (IMO 1990) Encontre todos os inteiros positivos $n>1$ tais que

$$\frac{2^n+1}{n^2}$$

é um inteiro.

Exercício 29. (Proposto por Paul Erdos para a American Mathematical Monthly) Seja p um número primo maior que 3. Se $n = \dfrac{2^{2p}-1}{3}$, mostre que 2^n-2 é divisível por n.

2 Polinômios Ciclotômicos

Exercício 30. (IMO 2003 - Adaptado) Seja p um número primo. Demonstre que existem **infinitos** primos q tal que, para todo inteiro n, o número $n^p - p$ não é divisível por q.

Exercício 31. (TST - China - 2004) Determine todos os inteiros positivos m satisfazendo a seguinte propriedade: existe um primo q_m tal que $n^m - m$ não é divisível por q_m para qualquer inteiro n.

Exercício 32. (Propriedades dos polinômios ciclotômicos)

1. $\Phi_n(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}$.
2. $\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots X + 1$, se p é primo.
3. Se $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$, então
$$\Phi_n(X) = \Phi_{p_1 p_2 \cdots p_k}(X^{p_1^{c_1-1} p_2^{c_2-1} \cdots p_k^{c_k-1}}).$$
4. Se $n > 1$ é ímpar, então $\Phi_{2n}(X) = \Phi_n(-X)$.
5. Se p é um primo que não divide n, então
$$\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)},$$
caso contrário, se $p \mid n$, $\Phi_{pn}(X) = \Phi_n(X^p)$.

Exercício 33. Seja n um inteiro positivo e x um inteiro qualquer. Mostre que todo divisor primo p de $\Phi_n(X)$ ou satisfaz $p \equiv 1 \pmod{n}$ ou $p \mid n$.

Teorema 4 Seja p um número primo. Então para todos os inteiros positivos n e a tais que $mdc(n, p) = 1$ temos $p \mid \Phi_n(a)$ se, e somente se, $ord_p(a) = n$.

Exercício 34. Seja p um número primo e x um inteiro qualquer. Então todo divisor primo q de $1 + x + \cdots + x^{p-1}$ ou satisfaz $q \equiv 1 \pmod{p}$ ou $p = q$.

Exercício 35. Sejam a e b inteiros positivos. Suponha que x é um inteiro e que $mdc(\Phi_a(X), \Phi_b(X)) > 1$. Então $\frac{a}{b} = p^k$ para algum número primo p e algum inteiro k.

Exercício 36. Encontre todas as soluções inteiras da equação
$$\frac{x^7 - 1}{x - 1} = y^5 - 1$$

Exercício 37. Mostre que, dado n, existem infinitos primos p da forma $nk + 1$.

Exercício 38. (IMC 2010) Suponha que para uma função $f : \mathbb{R} \to \mathbb{R}$ e números reais $a < b$ tenhamos $f(x) = 0$ para todo $x \in (a, b)$. Prove que $f(x) = 0$ para todo $x \in \mathbb{R}$ se
$$\sum_{k=0}^{p-1} f\left(y + \frac{k}{p}\right) = 0$$
para todo número primo p e todo número real y.

Exercício 39. (IMC 2011) Seja p um número primo. Dizemos que um inteiro positivo n é interessante se
$$x^n - 1 = (x^p - x + 1)f(x) + pg(x)$$
para polinômios f e g com coeficientes inteiros.

a) Prove que o número $p^p - 1$ é interessante.

b) Para quais p o número $p^p - 1$ é o menor número interessante?

Exercício 40. Seja n um inteiro positivo. Prove que o número $2^{2^n} + 2^{2^{n-1}} + 1$ pode ser expresso como o produto de não menos que n fatores primos (não necessariamente distintos).

Respostas e Soluções.

1. Suponha, por absurdo, que existe um inteiro positivo $n > 1$ com essa propriedade e que k é o menor dentre eles. Se $d = ord_k 2$, então $d \mid k$. Como $2^d \equiv 1 \pmod{k}$, temos $2^d \equiv 1 \pmod{d}$. Em virtude da minimalidade de k, temos $d = 1$ ou $d = k$. No primeiro caso, teríamos $k = 1$ produzindo uma contradição. No segundo caso, em decorrência do teorema anterior, $k \mid \phi(k)$. Entretanto, se $k > 1$, $\phi(k) \leq k - 1$ e obtemos assim um absurdo.

2. Se $k = ord_{a^n-1} a$, como $a^n \equiv 1 \pmod{a^n - 1}$, temos $k \mid n$ e consequentemente $k \leq n$. Não podemos ter $k < n$ porque $a^n - 1 \mid a^k - 1 \Rightarrow a^n - 1 \leq a^k - 1$. Assim, $k = n$ e usando o teorema anterior podemos concluir que $k \mid \phi(a^n - 1)$.

3. Provaremos por indução que $2^{3^k} + 1 = 3^{k+1} m_k$ com $3 \nmid m_k$. Suponha que a afirmação vale para k. Provemos para $k + 1$:

$$\begin{aligned} 2^{3^{k+1}} &= (3^{k+1} m_k - 1)^3 \\ &= 3^{3k+3} m_k^3 - 3^{2k+3} m_k^2 + 3^{k+2} m_k - 1 \\ &= 3^{k+2}(3^{2k+1} m_k^3 - 3^{k+1} + m_k) - 1 \\ &= 3^{k+2} m_{k+1} - 1 \end{aligned}$$

Claramente $3 \nmid m_{k+1}$. Voltemos ao problema. Seja $b = ord_{3^n} 2$, então $b \mid \phi(3^n) = 2 \cdot 3^{n-1}$. Temos duas possibilidades: ou $b = 2 \cdot 3^j$ ou $b = 3^j$. Como $2^{3^{n-1}} \equiv -1 \pmod{3^n}$ e $3^j \mid 3^{n-1}$ se $j \leq n - 1$, devemos ter $b = 2 \cdot 3^j$. Assim, $(2^{3^j} - 1)(2^{3^j} + 1) \equiv 1 \pmod{3)^n}$. Usando que $2^{3^j} - 1 \equiv 1 \pmod{3}$, temos $2^{3^j} \equiv -1 \pmod{3^n}$. Novamente pelo lema provado no início, $3^j \geq 3^{n-1}$ e assim $b = 2 \cdot 3^{n-1}$. Para o item b), de $2^m \equiv -1 \pmod{3^n}$, podemos concluir que $2^{2m} \equiv 1 \pmod{3)^n}$. Daí, $2 \cdot 3^{n-1} \mid 2m$ e o resultado segue.

4. Claramente n é ímpar, $mdc(m, n) = 1$ e $n > 2$. Se $n = 3$, como $mdc(m, n) = 1$ devemos ter que $m \equiv 1 \pmod{3}$ pois caso contrário $1 + m^{3^n} + m^{2 \cdot 3^n} \equiv 1 - 1 + 1 \equiv 1 \pmod{3}$. É fácil ver que todo par $(m, n) = (3k + 1, 3)$ é solução. Suponha agora $n > 3$ e seja $k = ord_n m$. Se $n > 3 \Rightarrow m^{3^n} \not\equiv 1 \pmod{n}$. Como $1 + m^{3^n} + m^{2 \cdot 3^n} = \dfrac{m^{3^{n+1}} - 1}{m^{3^n} - 1}$ segue que $n \mid m^{3^{n+1}} - 1 \Rightarrow k \mid 3^{n+1}$. Logo, $k = 3^{n+1}$. Pelo teorema de Euler, $m^{\phi(n)} \equiv 1 \pmod{n}$ então $k \leq \phi(n)$ e $3^{n+1} \leq \phi(n) \leq n - 1$, uma contradição.

5. Seja q um primo que divide $\dfrac{p^p - 1}{p - 1}$. Como $q \mid p^p - 1$ segue que $ord_q p \mid p$. Se $ord_q p = 1$ então $q \mid p^p - 1$ e $0 \equiv p^{p-1} + p^{p-2} + \ldots p + 1 \equiv 1 + 1 + \ldots + 1 + 1 \equiv p \pmod{q}$. Mas isso é um absurdo pois $p \neq q$. Logo $ord_q p = p$ e obtemos $p \mid \phi(q) = q - 1$. Daí, todos os divisores primos de $\dfrac{p^p - 1}{p - 1}$ são congruentes a 1 módulo p.