Congruências e Ordem

Gustavo Empinotti - gustavoempinotti@gmail.com

Janeiro 2020

Congruências

Dizemos que $a \equiv b \pmod{m}$ (a é *congruente* a b módulo m) se a e b deixam o mesmo resto na divisão por m.
Em outras palavras, $a \equiv b \pmod{m} \leftrightarrow m|a-b$

Exemplo 1: 7 deixa resto 3 na divisão por 4, portanto $7 \equiv 3 \pmod{4}$ (7 é congruente a 3 módulo 4). 19 também deixa resto 3 na divisão por 4. Portanto, por exemplo, $7 \equiv 19 \pmod{4}$

Qual a utilidade disso? é que adição, subtração e multiplicação são preservadas por congruências de mesmo módulo (cuidado: divisão não!).

Mais precisamente, se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a+b \equiv c+d \pmod{m}$ $a-b \equiv c-d \pmod{m}$ e $ab \equiv cd \pmod{m}$ (você sabe provar isso?)

Exercícios:

1. Calcule o resto de:
   a) 6^{1000} na divisão por 5
   b) 2^{50} na divisão por 7
   Solução: $2^3 = 8 \equiv 1 \pmod{7}$. Logo, $2^{50} = 2^{48} * 2^2 = (2^3)^{16} * 2^2 \equiv 1^{16} * 2^2 = 1 * 4 = 4 \pmod{7}$
   c) 4^{2013} na divisão por 15
   d) 3^{90} na divisão por 10
2. Prove que todo quadrado perfeito deixa resto 0 ou 1 na divisão por 4.
3. Prove que não existe inteiro n tal que $4n^2 - 3$ é divisível por 7.

Critérios de divisibilidade

Você deve conhecer o critério de divisibilidade por 3. O resto de um número na divisão por 3 é o mesmo da soma dos seus algarismos. Por exemplo, 325 tem o mesmo resto de 3+2+5=10, ou seja, $325 \equiv 3+2+5 \pmod{4}$. Você sabe por quê?

Nós usamos os algarismos em sistema decimal. Isto é, $325 = 3.10^2 + 2.10 + 5$. Mas 10 deixa resto 1 na divisão por 3, isto é, $10 \equiv 1 \pmod{3}$. Portanto, assim como no exemplo do 101, temos que qualquer potência de 10 também deixará resto 1, assim:

$10^2 \equiv 1^2 \equiv 1 \pmod{3}$

$10^3 \equiv 1^3 \equiv 1 \pmod{3}$

$10^4 \equiv 1^4 \equiv 1 \pmod{3}$ etc.

Portanto, temos $325 = 3.10^2 + 2.10 + 5 \equiv 3.1 + 2.1 + 5 \pmod{3}$, ou seja, $325 \equiv 3 + 2 + 5 \pmod{3}$

Exercícios:

4. O mesmo critério (soma dos dígitos) vale para divisibilidade por 9. Por quê?

5. Você sabe o critério de divisibilidade por 11? Prove-o!

Aritmética módulo p

Vimos acima que podemos fazer as operações $a+b, a-b, ab \bmod n$. Em geral, não podemos fazer a divisão.

Mas às vezes podemos. Vamos investigar quando:

Sob quais condições, sabendo que $ma \equiv mb \pmod{n}$, podemos concluir que $a \equiv b \pmod{n}$?

$ma \equiv mb \pmod{n} \leftrightarrow ma - mb \equiv 0 \pmod{n} \leftrightarrow m(a-b) \equiv 0 \pmod{n} \leftrightarrow n|m(a-b)$

A partir de $n|m(a-b)$, podemos concluir que $n|a-b$ quando $\text{mdc}(n,m) = 1$, pois então n e m não têm primos em comum, e todos os primos de n que estão em $m(a-b)$ têm que estar em $a-b$. Logo:

Resultado 1: Se $\text{mdc}(m,n) = 1$, então $ma \equiv mb \pmod{n}$ implica $a \equiv b \pmod{n}$.

Resultados como este são o motivo por que é tão útil trabalhar com primos em Teoria dos Números. Um primo p não tem fatores em comum com nenhum dos resíduos módulo p, exceto o 0; isto é, $1, 2, \ldots, p-1$ todos têm mdc 1 com p.

Corolário 1: Se p é primo, $ma \equiv mb \pmod{p}$ e $m \neq 0 \pmod{p}$, então $a \equiv b \pmod{p}$.

Há uma outra maneira de chegar a este resultado, que é a maneira de formalizar divisão módulo n. Pense nos inteiros: a divisão nada mais é que a multiplicação pelo inverso, onde o inverso de a é definido como o número b tal que $ab = 1$. Isto é, quando saímos dos inteiros e queremos passar a trabalhar com os racionais, definimos, por exemplo, $\frac{3}{2} = 3 * \frac{1}{2}$, onde $\frac{1}{2}$ é o inverso de 2. A divisão módulo n é igual em princípio. Porém, para n composto, nem todos os números não-nulos módulo n têm inverso:

Resultado 2: Um inteiro a tem inverso módulo n se e somente se $\text{mdc}(a,n) = 1$

Prova: Se o mdc não for 1, então existe um primo p que divide tanto a quanto n. Então para qualquer b, $p|ab$. Se tivéssemos $ab \equiv 1 \pmod{n}$, então $n|ab-1$, mas $p|n$, logo $p|ab-1$, e $p|ab$, logo $p|1$, absurdo.

Agora, suponha $\text{mdc}(a,n) = 1$. Considere o conjunto das potências de a : $\{a, a^2, a^3, \ldots\} = A$. Como são infinitas, e há apenas finitos restos módulo n, eventualmente os restos que aparecem em A se repetirão, e teremos algum par i, j com $i \neq j$ tal que $a^i \equiv a^j \pmod{n}$. Mas suponha sem perda de generalidade $i > j$. O Resultado 1 acima nos permite dividir por a^j dos dois lados, pois se $(a,m) = 1$, então $(a^j, m) = 1$ (elevar a j não cria fatores primos novos) (aliás, usa-se a abreviação (r,s) para denotar $\text{mdc}(r,s)$).

Assim, $a^i \equiv a^j \pmod{n} \rightarrow a^{i-j} \equiv 1 \pmod{n}$. Mas então $a * a^{i-j-1} \equiv 1$, e a^{i-j-1} é o inverso de a módulo n, e $i-j-1 \geq 0$.

Mas então, como um primo p é primo com $1, 2, \ldots, p-1$, todos os elementos não-nulos módulo p têm inverso! Ou seja, podemos dividir normalmente (exceto por 0) módulo p. Isso é o que torna as coisas módulo p mais fáceis de trabalhar!

Problema 1: Seja p um primo e a um inteiro não divisível por p. Calcule, em função de p, o número de ternas de inteiros (x,y,z), com $0 \leq x, y, z \leq p-1$, tais que p divide $(x+y+z)^2 - axyz$.

Vamos continuar explorando a multiplicação e divisão módulo p.

Seja a um elemento não-nulo módulo p (isto é, não divisível por p). Então temos que se $ax \equiv ay \pmod{p}$, então $x \equiv y \pmod{p}$.

Em particular, se pegarmos os $p-1$ resíduos distintos não-nulos módulo p e multiplicarmos por a, eles têm que continuar sendo distintos. Ou seja,

Resultado 3: O conjunto $\{a, 2a, 3a, \ldots, (p-1)a\}$ é igual, em alguma ordem, ao conjunto $\{1, 2, 3, \ldots, p-1\}$

Isso nos permite fazer um truque legal: se multiplicarmos todos os números dos dois conjuntos, temos que obter o mesmo resultado:

$$a * 2a * 3a * \ldots * (p-1)a \equiv 1 * 2 * 3 * \ldots * (p-1) \pmod{p}$$

$$a^{p-1} * (p-1)! \equiv (p-1)! \pmod{p}$$

Mas $(p-1)!$ não tem fator p, pois p é primo, logo podemos cancelar $(p-1)!$ e obtemos:

$$a^{p-1} \equiv 1 \pmod{p}$$

.

Para qualquer a não-nulo! Esse resultado é muito importante

Pequeno Teorema de Fermat: Se p é primo $(a, p) = 1$, então $a^{p-1} \equiv 1 \pmod{p}$

Exercícios:

1. Como generalizar o resultado acima para o caso em que o módulo não é primo? Já vimos acima que se $(a, n) = 1$ existe algum expoente k tal que $a^k \equiv 1 \pmod{n}$. Será que, como no Pequeno Teorema de Fermat, expressar tal expoente em função de n, para n composto (em outras palavras, no caso p, o expoente $k = p - 1$ dá certo. E no caso n?)

   Dica: comece pegando todos os resíduos módulo n que são primos entre si com n. Sejam eles $\{a_1, a_2, \ldots, a_k\}$.

   Dica 2: a quantidade de inteiros positivos menores que n que são primos entre si com n é uma função muito usada em Teoria dos Números, expressa por $\phi(n)$

   Assim, prove o:

   Teorema de Euler-Fermat: Para n inteiro positivo e a inteiro com $(a, n) = 1$, temos

   $$a^{\phi(n)} \equiv 1 \pmod{n}$$

2. Você agora pode fazer alguns exercícios como do início deste material mais rápido:
   Calcule o resto na divisão de 7^{202} por 15 usando o Teorema de Euler-Fermat.

3. (OBM 2009) Prove que existem infinitos inteiros n tais que
   $$\frac{5^{n-2} - 1}{n}$$
   é um inteiro.

4. (OBM 2018) Considere a sequência em que $a_1 = 1$ e a_n é obtido justapondo ao final da representação decimal de a_{n-1} a representação decimal de n. Ou seja, $a_1 = 1, a_2 = 12, a_3 = 123, \ldots, a_9 = 123456789, a_{10} = 12345678910$ e assim sucessivamente. Prove que infinitos termos dessa sequência são múltiplos de 7.

5. (CPLP 2019, adaptado) Determine o menor inteiro positivo k tal que existem k inteiros (não necessariamente positivos) $x_1, x_2, \ldots, x_k$ tais que $x_1^5 + x_2^5 + \ldots + x_k^5 = 2018$.

Ordens e raízes primitivas

Já vimos que se $(a, n) = 1$, sempre existe um expoente k tal que $a^k \equiv 1 \pmod{n}$. Agora, buscaremos caracterizar todos tais expoentes. Ou seja, para quais k vale $a^k \equiv 1 \pmod{n}$?

Para responder, podemos começar considerando, dentre todos estes expoentes, o menor. Seja d o menor expoente tal que $a^d \equiv 1 \pmod{n}$. Ele existe pois já provamos que existe pelo menos um ($\phi(n)$).

Então, para qualquer inteiro m, $(a^d)^m \equiv 1$, ou seja $a^{dm} \equiv 1 \pmod{n}$, então todos os múltiplos k de d são tais que $a^k \equiv 1 \pmod{n}$.

Será que esses são todos os k? Para responder, consideramos um exponete k qualquer tal que $a^k \equiv 1 \pmod{n}$ e consideramos a divisão euclidiana de k por d: $k = qd + r$, onde q é inteiro e r é o resto da divisão, $0 \leq r < d$. Gostaríamos de avaliar se esse resto r tem que ser 0.

Temos que $1 \equiv a^k = a^{qd+r} = (a^d)^q * a^r \equiv a^r \pmod{n}$, isto é, $a^r \equiv 1 \pmod{n}$. Mas por hipótese d é o menor expoente positivo tal que $a^d \equiv 1 \pmod{n}$ e $0 \leq r < d$, logo $r = 0$. Assim, temos:

Resultado 4: Seja d o menor expoente positivo tal que $a^d \equiv 1 \pmod{n}$. Então para um inteiro positivo k, $a^k \equiv 1 \pmod{n}$ se e somente se $d|k$.

Chamamos este menor expoente d de ***ordem*** de a módulo n, e denotamos $d = \text{ord}_n a$

Corolário: Seja d a ordem de a módulo n. Então $d|\phi(n)$.

Outro resultado importante é:

Resultado 5: Se d é a ordem de a módulo n, então $a, a^2, a^3, \ldots, a^d$ são distintos (prove!).

Pelo que vimos acima, segue que se p é primo e d é a ordem de a módulo p, então $d|p-1$. Mas, também é verdade que para todo divisor d de $p-1$, existe um a tal que $\text{ord}_p a = d$.

Resultado 6: Seja d um divisor de $p-1$. Então existe pelo menos um inteiro a tal que $\text{ord}_p a = d$.

Prova: A prova é um pouco longa então não incluirei aqui. Você pode vê-la, por exemplo, na referência [1] (é possível calcular exatamente a quantidade de resíduos cuja ordem é d, e isso também é feito na referência)

Em particular, existe g tal que $\text{ord}_p g = p - 1$. Chamamos tal g de ***raiz primitiva***. Raízes primitivas têm propriedades importantes.

Propriedade 1: Se g é raiz primitiva, então $g, g^2, g^3, \ldots g^{p-1}$ é o conjunto $\{1, 2, \ldots, p-1\}$ módulo p (ou seja, é um sistema reduzido de resíduos módulo p)

O legal de raízes primitivas é justamente que você pode representar todos os resíduos não-nulos como potências de g.

Problemas:

1. Para quais primos p existe x tal que $x^2 \equiv -1 \pmod{p}$? E para quais n compostos?
2. Quantos resíduos quadráticos distintos existem módulo p? (isto é, quantos elementos distintos tem o conjunto $\{1^2, 2^2, \ldots, p^2\}$ mod p?)
3. Quantos resíduos cúbicos distintos existem módulo p? (isto é, quantos elementos distintos tem o conjunto $\{1^3, 2^3, \ldots, p^3\}$ mod p?) Aqui a resposta será diferente dependendo de certas características de p.

4. Usando uma raiz primitiva, calcule, módulo p:

   (i) $1 + 2 + 3 + \ldots + p - 1$

   (ii) $1 * 2 * \ldots * (p - 1)$ (o resultado aqui é conhecido como o Teorema de Wilson)

5. Prove que não existe $n > 1$ tal que $n|2^n - 1$

6. (OBM 2009) Seja q um primo tal que $q = 2p + 1$ onde p também é primo. Prove que existe um múltiplo de q cuja soma dos algarismos na base decimal é menor que ou igual a 3.

7. (IMO 1990) Encontre todos os inteiros positivos n tais que $n|2^n + 1$

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

9. Mostre que se $k > 1$, então $2^{k-1} \neq -1 \pmod{k}$

10. (Bulgária 1995) Encontre todos os primos p e q tais que $pq|2^p + 2^q$.

Referências:

[1] `https://www.urantiagaia.org/educacional/matematica/teoria_numeros3/Aula07-Ordens_e_Raizes_Primitivas.pdf` (contém a prova do Resultado 6 acima, não provado aqui)

Mais conteúdo e exercícios sobre ordem:
[2] `https://www.urantiagaia.org/educacional/matematica/teoria_numeros2/Aula16-Ordem.pdf`

[3] O Material do POTI (`https://poti.impa.br/`) em geral, sobre todos os temas, é uma ótima referência para estudar sozinho.

Os materiais em PDF podem ser baixados integralmente do site, ou encontrados aqui:
`https://www.urantiagaia.org/educacional/matematica/index.html`

Livro de Teoria dos Números excelentes:

[4] *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*, Fabio Martinez, Carlos Gustavo Moreira, Nicolau Saldanha e Eduardo Tengan; IMPA, 2018, 5a edição

[5] *Introdução à Teoria dos Números*, José Plínio de Oliveira Santos; IMPA, 2018, 3a edição