P2 Matemática Discreta

November 30, 2024

Aritmética Modular

Notação: Dizemos $a|b$ se existe $n \in \mathbb{Z}$ tal que $an = b$.
Congruência: $a \equiv_m b$ se, e somente se, $m|a-b$. Podemos entender isso como b sendo o resto da divisão de a por m.
Inversos Modulares: Dados $n \in \mathbb{N}_{>0}$ e $a, b \in \mathbb{Z}$, dizemos que b é o inverso de a módulo n se $ab \equiv_n = 1$.

Lema: O inverso de 3 módulo $6k-2$ é igual a $4k-1$.

Sejam $n \in \mathbb{N}_{>0}$ e $a \in \mathbb{Z}$. Se a e n possuem um divisor primo em comum, então existe $b \not\equiv_n 0$ tal que $ab \equiv_n 0$. Além disso, então a não admite inverso módulo n.

Dados $n \in \mathbb{N}_{>0}$ e $a, b \in \mathbb{Z}$ tais que b é inverso de a módulo n. Se $c \in \mathbb{Z}$ também é inverso de a, então $b \equiv_n c$.

Uma utililidade do inverso é o cancelamento: Sejam $n \in \mathbb{N}_{>0}$ e $a, b, c \in \mathbb{Z}$, com c sem divisores primos com n. Se $ac \equiv_n bc$, então $a \equiv_n b$.

Função totiente: $\varphi(n)$ é a quantidade de números menores ou iguais a n e coprimos em relação a ele.
Propriedade 1: $\varphi(p) = p-1$ se p é primo;
Propriedade 2: $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$;
Pequeno Teorema de Fermat: Seja p um número primo. Então: $a^p \equiv_p a$. Se $a \nmid p$, então $a^{p-1} \equiv_p 1$.
Teorema de Euler: Se $mdc(a, n) = 1$, então $a^{\varphi(n)} \equiv_n 1$. No caso particular onde n é primo, $a^{n-1} \equiv_n 1$ (Pequeno Teorema de Fermat).

Teorema chinês do resto:

Corolário 1: Sejam $a_1, a_2, ..., a_n, b \in \mathbb{N}_{>1}$ primos entre si. Então $a_1 \cdots a_n$ e b são primos entre si.
Proposição: Sejam a, b primos entre si. Sejam r e s inteiros, então o sistema: $\begin{cases} x \equiv_a r \\ x \equiv_b s \end{cases}$, admite alguma solução c e é equivalente a $x \equiv_{ab} c$.
Caso particular: Sejam p, q primos entre si e r tal que $0 \leq r < \min(p, q)$. Se $\begin{cases} x \equiv_p r \\ x \equiv_q r \end{cases}$, então: $x \equiv_{pq} r$.

Criptografia

Blocos: Os valores dos blocos de codificação não podem iniciar em 0 e precisam ser menores que um número n, tal que $n = pq$, com p, q primos.

Como exemplo, vamos utilizar $p = 17$ e $q = 23$. Assim, $n = 391$.
Codificação: A função de codificação $c(b)$ é dada por:

$$c(b) = \text{resto da divisão de } b^{\lambda} \text{por } n.$$

No nosso exemplo, usaremos $\lambda = 3$.
Decodificação: Primeiro, devemos encontrar x que é o inverso de λ módulo $(p-1)(q-1)$. Ou seja: $\lambda x \equiv_{(p-1(q-1)} 1$. Depois de encontrarmos x, a função de decodificação é dada por:

$$d(a) = \text{resto da divisão de } a^{x} \text{por } n.$$

Pelo nosso exemplo, $x = 235$.

Alguns problemas

Problema 1: Qual o último algarismo de 27^220? *Ideia:* Para encontrar o último algarismo, devemos achar o resto da divisão de 27^{220} por 10. Temos então: $27^{220} \equiv_{10} 7^{220}$. Vamos tentar achar um padrão das potências de 7 módulo 10: $7^0 \equiv_{10} 1$, $7^1 \equiv_{10} 7$, $7^2 \equiv_{10} 9$, $7^3 \equiv_{10} 3$, $7^4 \equiv_{10} 1$. Portanto, o resto das potências de 7 módulo 10 se repetem de 4 em 4. Assim: $220 \equiv_4 0$. Ou seja, $7^220 \equiv_{10} 7^0 \equiv_{10} 1$. Logo, o último algarismo de 27^220 é 1.
Problema 2: Considere uma pista circular. O carro A demora 5 minutos para dar uma volta completa. Já o carro B, demora 3 minutos para dar uma volta completa e larga 17 minutos depois do carro A. Finalmente, o carro C demora 4 minutos para dar uma volta e larga 8 minutos depois do carro B. Supondo que esses carros fiquem dando voltas com velocidades constantes, é verdade que eles passarão pela chegada ao mesmo tempo em algum momento? Se sim, quantos minutos depois da largada do carro A será o primeiro momento em que isso ocorre? *Ideia:* Podemos montar um sistema da seguinte forma:

$$\begin{cases} x & \equiv_5 0 \\ x-17 & \equiv_3 0 \\ x-25 & \equiv_4 0 \end{cases} \iff \begin{cases} x \equiv_5 0 & (1) \\ x \equiv_3 17 \equiv_3 2 & (2) \\ x \equiv_4 25 \equiv_4 1 & (3) \end{cases}$$

Queremos verificar se há um ponto em que eles se encontrem na origem, por isso todas as equações devem ser congruentes a 0 módulo sua própria velocidade. Essas subtrações na segunda e terceira equação existem, pois os carros B e C largaram 17min e 25min depois que o carro A, respectivamente. Agora, só precisamos resolver o sistema.

Pela equação (3), temos: $x = 4a + 1$.

Substituindo em (2): $4a + 1 \equiv_3 2 \Leftrightarrow a + 1 \equiv_3 2 \Leftrightarrow a \equiv_3 1$. Logo, $a = 3b+1$. Podemos substituir em x: $x = 4(3b+1)+1 = 12b+5$.

Por fim, podemos substituir x em (1): $12b + 5 \equiv_5 0 \Leftrightarrow 2b \equiv_5 0 \Leftrightarrow b \equiv_5 0$. Assim, $b = 5c + 0$. Novamente, substituindo em x, temos: $x = 12(5c) + 5 = 60c + 5$.

Como em $c = 0$, somente o carro A vai ter dado largada, o primeiro momento em que os carros se encontram na origem é em $c = 1$. Portanto, $x = 60 + 5 = 65$min.
Problema 3: Qual o resto da divisão por 33 de um $x \in \mathbb{N}$, sabendo que tal x tem resto 2 na divisão por 3 e resto 2 na divisão por 11? *Ideia:* Sabemos, pelo caso particular do teorema chinês do resto que, se

$$\begin{cases} x \equiv_3 2 \\ x \equiv_1 12 \end{cases},$$

então $x \equiv_{3 \cdot 11} 2$. Portanto, $x \equiv_{33} 2$.
Problema 4: Qual é o resto de 13^{166} na divisão por 83? *Ideia:* Como 83 é primo e 13 não é divisível por 83, podemos utilizar o pequeno teorema de Fermat: $13^{82} \equiv_{83} 1$. Escrevendo 166 em termos de 82, temos $166 = 82 \cdot 2 + 2$. Assim: $13^{166} \equiv_{83} (13^{82})^2 \cdot 13^2 \equiv_{83} 1^2 \cdot 13^2 \equiv_{83} 169 \equiv_{83} 3$.
Problema 5: Fixados $a, b \in \mathbb{N}$com$b > a$, sabe-se que tanto a como b possuem resto 1 na divisão por 17 e na divisão por 23. Também se sabe que entre a e b nenhum outro número tem resto 1 na divisão por 17 e por 23 ao mesmo tempo. Quanto é $b - a$? *Ideia:* Podemos utilizar o teorema chinês do resto nesse exercício. Sabemos que

$$\begin{cases} a \equiv_{17} 1 \\ a \equiv_{23} 1 \end{cases}, \begin{cases} b \equiv_{17} 1 \\ b \equiv_{23} 1 \end{cases}$$

Assim, $a \equiv_{391} 1$ e $b \equiv_{391} 1$. Podemos reescrever essas expressões da seguinte forma, sejam $n, m \in \mathbb{N}$, temos: $a = 391n + 1$, $b = 391m + 1$. Como $b > a$, então podemos escolher $n = 0, m = 1$. Portanto, $a = 1$ e $b = 392$ e, consequentemente $b - a = 391$ (isso vai valer para quaisquer n, m escolhidos, desde que $m > n$).
Problema 6: Qual o resto da divisão de 1000! por 3^{300}?
Ideia: Na fatoração em primos de 1000! existe um fator 3^k. Como $1000! = 1000 \cdot 999 \cdots 2 \cdot 1$, k depende do número de múltiplos de 3 entre 1 e 1000. Mas entre 1 e n, existem $\lfloor \frac{n}{m} \rfloor$ múltiplos de m. Logo, existem $\lfloor \frac{1000}{3} \rfloor = 333$ múltiplos de 3 entre 1 e 1000, portanto k é no mínimo $333 > 300$, então $3^{300} \mid 1000! \implies 1000! \equiv_{3^{300}} 0$.

Problema 7: Sendo $S(n)$ a soma dos dígitos de n em base decimal e $N = 4444^{4444}$, qual o valor de $S(S(S(N)))$?
Ideia: O primeiro lema é que $n \equiv_9 S(n)$.
Temos que $4444^{4444} < 10000^{4444} = (10^4)^{4444} = 10^{17776}$, portanto, N tem 17776 dígitos ou menos. Logo, $S(N)$ é, no máximo, $9 \cdot 17776 = 159984$, que por sua vez, tem 6 dígitos. Logo, $S(S(N)) \leq 9 \cdot 6 = 45$. Note que pra todo $k \leq 45$, $S(k) \leq 12$, logo $S(S(S(N))) \leq 12$. Pelo Lema 1, temos que $N \equiv_9 S(S(S(N))) \equiv_9 7^{4444}$, mas $7^k \equiv_9 7$ quando $k \equiv_3 1$. Logo, $S(S(S(N))) = 7$, já que o próximo número congruente a 7 módulo 9 é maior que 12.

Problema 8: Qual o menor $n \in \mathbb{N}$ da forma $8k+2$ (com $k \in \mathbb{N}$) que seja múltiplo de 7? *Ideia:* Queremos achar o menor valor que satisfaça a congruência $8k + 2 \equiv_7 0$. Podemos reescrever a equação da seguinte forma: $k + 2 \equiv_7 0 \Leftrightarrow k \equiv_7 -2 \Leftrightarrow k \equiv_7 5$. Assim, $k = 7c+5$. Substituindo k em n, temos $n = 8(7c+5)+2 = 56c + 42$. Como queremos o menor valor de n, devemos escolher $c = 0$, desse modo $n = 42$.

Problema 9: Qual o menor número inteiro positivo que pode ser escrito nas formas $3a + 1, 2b + 1$ e $23c + 3$ com $a, b, c \in \mathbb{N}$?
Ideia: Podemos reescrever as expressões na forma de congruências:

$$\begin{cases} x \equiv_3 1 & (1) \\ x \equiv_2 1 & (2) \\ x \equiv_{23} 3 & (3) \end{cases}$$

Pela equação (3) temos $x = 23c + 3$.

Substituindo em (2): $23c+3 \equiv_2 1 \Leftrightarrow c+1 \equiv_2 1 \Leftrightarrow c \equiv_2 0$. Logo, $c = 2k$. Substituindo em x, $x = 23(2k) + 3 = 46k + 3$.

Novamente substituindo x, mas agora em (1), temos: $46k+3 \equiv_3 1 \Leftrightarrow k \equiv_3 1$. Assim, $k = 3j + 1$.

Portanto, $x = 46(3j + 1) + 3 = 138j + 49$. Como queremos o menor número, $j = 0$, então $x = 49$.