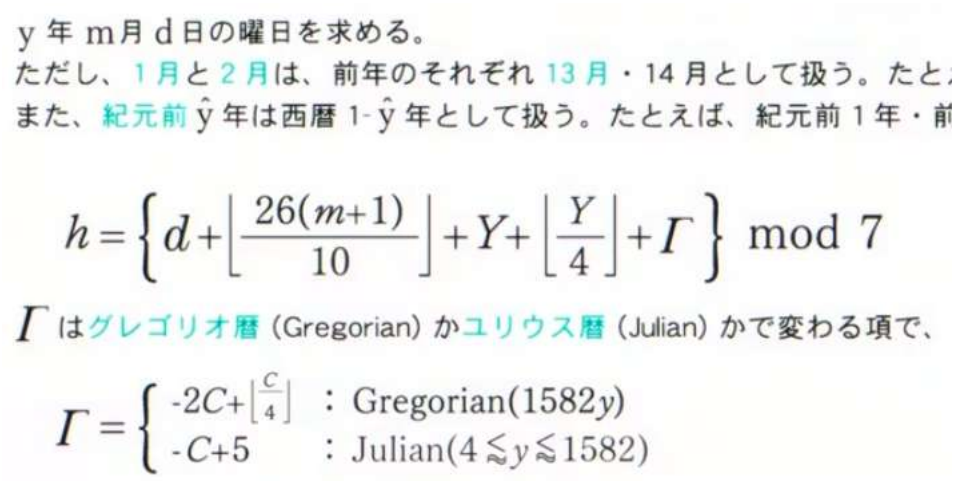
Congruência modular: sua aparição nos animes e diversos usos

Vitória Aparecida Santos Ferreira - vitoriaaparecida94@gmail.com

25° Semana Olímpica - Julho 2022 - Nível 1


y 年 m月 d日の曜日を求める。
ただし、1月と2月は、前年のそれぞれ13月・14月として扱う。たと
また、紀元前 ŷ 年は西暦 1-ŷ 年として扱う。たとえば、紀元前1年・前

$$h=\left\{d+\left\lfloor\frac{26(m+1)}{10}\right\rfloor+Y+\left\lfloor\frac{Y}{4}\right\rfloor+\Gamma\right\} \bmod 7$$

Γ はグレゴリオ暦 (Gregorian) かユリウス暦 (Julian) かで変わる項で、

$$\Gamma=\begin{cases}-2C+\left\lfloor\frac{C}{4}\right\rfloor & : \text{Gregorian}(1582y)\\ -C+5 & : \text{Julian}(4\lesssim y\lesssim 1582)\end{cases}$$

1 Definições iniciais

Serão apresentados alguns conceitos de Aritmética que conduzirão ao título acima.

1.1 Divisão euclidiana

Dados $a, b \in \mathbb{Z}_+, a > 0$, existem únicos inteiros q, r, chamados de *quociente* e *resto*, respectivamente, tais que

$$b = aq + r, 0 \leq r \leq a - 1.$$

1.2 Congruência modular

A noção de congruência modular foi introduzida pelo matemático suíço Leonhard Euler, por volta de 1750, tendo ocorrido maior exploração da aritmética dos restos pelo matemático alemão Friedrich Gauss, que, em 1798, aos 21 anos, escreveu a obra *Disquisitiones Arithmeticae*.

Seja $m \in \mathbb{Z}, m > 1$ fixado. Diz-se que *a é congruente a b módulo m* se a, b têm mesmo resto na divisão por m, ou, equivalentemente, se $b - a$ é divisível por m. Escreve-se que

$$a \equiv b \pmod{m}.$$

Exemplos:

1. $23 \equiv 8 \equiv 2 \pmod 3$, pois 23, 8 e 2 deixam mesmo resto na divisão por 3 ($r = 2$).

2. $10^n \equiv 1 (\text{mod } 9)$, isto é, qualquer potência de 10 deixa resto 1 na divisão por 9. Note que

$$10^n - 1 = \underbrace{1 \cdots 1}_{n \text{ vezes}} \times 9,$$

isto é, 9 divide a diferença acima e, portanto, tem-se a congruência $10^n \equiv 1 \pmod 9$.

3. Em um ano bissexto, a maior quantidade de meses que possuem o 1° dia do mês no mesmo dia da semana é 3, isto é, existe algum dia da semana (domingo, segunda-feira,..., sexta-feira, sábado) tal que exatamente três meses se iniciam neste dia e, para nenhum dos outros seis dias, ocorre que há mais que 3 meses tendo início nele.

Demonstração. Atribua o número 0 ao dia da semana em que caiu 1° de janeiro. Como uma semana possui 7 dias, dia 8 de janeiro também terá o número 0 atribuído, assim como os dias 15/01, 22/01, 29/01. Continuando com esta associação, 01/02 recebe o número 3. De forma mais geral, ocorre que 01/02 está em correspondência com 3 porque 3 é o resto da divisão de 31 por 7. Pode-se, assim, fazer a seguinte tabela

	Jan	*Fev*	*Mar*	*Abr*	*Mai*	*Jun*	*Jul*	*Ago*	*Set*	*Out*	*Nov*	*Dez*
Qtde. dias	31	29	31	30	31	30	31	31	30	31	30	31
Qtde. de dias desde 01/01	0	31	60	91	121	152	182	213	244	274	305	335
Resto na div. por 7	0	3	4	0	2	5	0	3	6	1	4	6

Contando as repetições dos números de 0 a 6 na última linha, tem-se que 0 tem maior incidência, aparecendo três vezes. Assim, o dia da semana que mais se repete nos dias primeiro ocorre três vezes e coincide com o dia de 01/01. □

Propriedades: se $a \equiv b \pmod m$ e $c \equiv d \pmod m$, vale que

(i) $a + c \equiv b + d \pmod m$.

(ii) $a - c \equiv b - d \pmod m$.

(iii) $ac \equiv bd \pmod m$.

(iv) Da unicidade garantida pelo algoritmo de Euclides, se $a \equiv b \pmod m$, com $m > 1$ e $a \leq b \leq m - 1$, então b é o resto da divisão de a por m.

(v) Se $ka \equiv kb \pmod m$, com $\text{mdc}(k, m) = 1$, então $a \equiv b \pmod m$. Note que a regra do "cancelamento"não é sempre válida. Por exemplo,

$$3 \cdot 7 = 21 \equiv 27 = 3 \cdot 9 \pmod 6,$$

mas $7 \not\equiv 9 \pmod 6$.

(vi) (Pequeno teorema de Fermat) Se p é primo e a é um inteiro, então $a^p \equiv a \pmod p$. De maneira mais geral, vale o teorema de Euler, enunciado abaixo.

(vii) (Teorema de Euler) Seja φ a função phi de Euler, que, para $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, associa o número $n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$. Então, para $a, n \in \mathbb{Z}, n > 0$ e $\text{mdc}(a, n) = 1$, tem-se que

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

1.3 Função piso ou parte inteira

É a função $f : \mathbb{R} \to \mathbb{Z}$ dada por $f(x) := \lfloor x \rfloor = \max\{m \in \mathbb{Z} \mid m \leq x\}$.
Exemplos:

1. $\lfloor \pi \rfloor = 3$.
2. $\lfloor -\pi \rfloor = -4$.
3. Seja p primo. Se $n \in \mathbb{N}$, o número de fatores p em $n!$ é dado pela expressão

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots .$$

Demonstração. Considere o produto $n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$. Para se saber o número de fatores múltiplos de p, toma-se o quociente da divisão de n por p, isto é, calcula-se $\left\lfloor \frac{n}{p} \right\rfloor$. Mas, pode haver múltiplos de p^2, que contabilizam exatamente $\left\lfloor \frac{n}{p^2} \right\rfloor$ números. Contando-se esta última quantidade, acumula-se mais 1 fator p referente a cada múltiplo de p^2. Continuando desta forma, tem-se exatamente o número de fatores p em $n!$, sendo a soma acima finita porque, a partir de algum momento, $p^k > n \Rightarrow \frac{n}{p^k} = 0, \ldots$ e, assim, $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$. □

2 Uma aplicação: A congruência de Zeller ([4])

Christian Zeller foi um matemático alemão que viveu na segunda metade do século XIX e que criou a chamada congruência de Zeller. Esta é um algoritmo para calcular o dia da semana em que cai qualquer data do calendário gregoriano ou juliano. A fórmula aparece no episódio 6 da produção japonesa *Yuyushiki* e, para o calendário gregoriano, é dada por

$$h = \left(d + \left\lfloor \frac{13(m+1)}{5} \right\rfloor + y + \left\lfloor \frac{y}{4} \right\rfloor + \left\lfloor \frac{c}{4} \right\rfloor - 2c \right) \pmod 7,$$

onde h é o dia da semana (varia de 0 = sábado a 6 = sexta-feira). É o que se quer descobrir!;

d é o dia;

m é o mês, com março = 3, abril = 4,..., dezembro = 12, janeiro = 13, fevereiro = 14, isto é, os dias de janeiro e fevereiro são considerados como dias dos 13° e 14° meses do ano anterior, respectivamente;

y é ano (mod 100). Ex.: se o ano é 1997, $y = 97$;

c é $\left\lfloor \frac{\text{ano}}{100} \right\rfloor$. Ex.: se o ano é 2031, então $c = 20$.

Testando a fórmula para a data 23/07/2022, tem-se que $d = 23; m = 7; y = 22; c = 20$ e, portanto,

$$h = \left(23 + \left\lfloor \frac{13 \cdot 8}{5} \right\rfloor + 22 + 5 + 5 - 40 \right) \pmod 7 \equiv 23 + 20 - 8 \equiv 0 \pmod 7 \Rightarrow \text{é sábado.}$$

3 Outras aplicações da congruência modular ([1],[2],[3])

1. Calcule o resto da divisão de 2^{5345} por 7 e de $2^{10^{10}}$ por 7.
2. Ache os dois últimos algarismos do número 3^{400}.
3. Qual é a maior potência de 2 que divide $2021^{2022} - 1$?

   (Dica: use diferença de quadrados.)
4. Calcula-se a soma dos algarismo de 19^{100}. Depois, efetua-se a soma dos algarismos do resultado anterior e assim sucessivamente, até haver um único algarismo. Qual é ele?

   (Dica: lembre-se do critério de divisibilidade por 9.)
5. O número 1 está escrito em um quadro negro. Depois de cada segundo, o número é aumentado pela soma de seus algarismos. Em algum instante, pode aparecer 123456 escrito na lousa?
6. Resolva a equação $3^y = 2^x + 5, x, y \in \mathbb{N}$.
7. Mostre que a equação $x^3 - 2025y = 2022$ não possui soluções inteiras.

   (Dica: analise a congruência modular de x^3 módulo 9.)
8. Prove que existem infinitos números naturais que não podem ser representados como soma de três cubos.
9. Seja $n \in \mathbb{N}$ tal que $n + 1$ é divisível por 24. Prove que a soma de todos os divisores de n também é divisível por 24.
10. Considere a sequência de números naturais $a_1, a_2, \ldots$ dada por $a_{n+2} = 1 + a_{n+1} \cdot a_n, \forall\ n$.

    a) Se $a_1 = a_2 = 1$, prove que nenhum elemento da sequência é divisível por 4.

    b) Prove que $a_n - 22$ é um número composto (isto é, não é número primo) para todo $n > 10$, quaisquer que sejam a_1, a_2.
11. Seja $a_n = 2^n - 3, n > 1$.

    a) Mostre que há uma infinidade de n tais que a_n é divisível por 5.

    b) Mostre que há uma infinidade de n tais que a_n é divisível por 13.

    c) Mostre que não existe n tal que a_n seja divisível por 65.
12. O número $y \in \mathbb{N}$ foi obtido de x rearrumando-se seus algarismos. Se $x + y = 10^{200}$, prove que x é divisível por 50.
13. Encontre o número de inteiros $n > 1$ para os quais $a^{25} - a$ é divisível por n, para cada inteiro a.
14. Ache n, onde este é formado pelos dois últimos algarismos não nulos de 90!.
15. Seja p primo, $1 \leq n \leq p - 1$. Mostre que

    a) $\binom{p}{n}$ é divisível por p.

    b) $\binom{p}{n} \equiv (-1)^n \pmod{p}$.

    (Dica: use a identidade combinatória $\binom{m}{r} = \binom{m-1}{r-1} + \binom{m-1}{r}$.)

16. É possível arrumar os números de 1 a 21 em disposição triangular (a primeira linha, de cima para baixo, contém 6 números, a segunda contém 5, até a primeira conter apenas 1 número) tal que o número de uma linha é o valor absoluto da diferença dos números imediatamente acima?

    (Exemplo: para os números de 1 a 6, pode-se fazer a disposição: $\begin{array}{ccccccc} & & 6 & & 1 & & 4 \\ & 5 & & & & 3 & \\ & & & 2 & & & \end{array}$)

Referências

[1] D. Fomin, S. Genkin, and Itenberg I. *Círculos matemáticos: a experiência russa*. IMPA, 1st edition, 2012.

[2] A. Hefez. *Iniciação à Aritmética*. IMPA, 1st edition, 2016.

[3] F.B. Martinez, C.G. Moreira, N. Saldanha, and E. Tengan. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. Projeto Euclides, 1st edition, 2011.

[4] R. Sivaraman. Determining day of given date mathematically. *Mathematics and Statistics*, Vol. 8(N° 5):pág. 590–595, 2020.