MAT 0120 Lista 4 (Congruências)

Definição: Seja $m \neq 0$ um inteiro fixo. Dois inteiros a e b dizem-se congruentes módulo m se m divide a diferença $a - b$.

Notação: $a \equiv b \pmod{m}$ - pág 104

obs. Dois números são congruentes módulo 2 se, e somente se ambos são pares ou ímpares

De fato, considere $a \equiv b \pmod{2}$ então

$$2 \mid a - b \Rightarrow a - b = 2k, \quad k \in \mathbb{Z}$$

Portanto, vemos que ambos possuem a mesma paridade, caso contrário a diferença seria ímpar e não seria divisível por 2.

A recíproca é simples. ∎

Proposição 3.2.2: Seja m um inteiro fixo. Dois inteiros a e b são congruentes módulo m se e somente se eles tem o mesmo resto quando divididos por m.

Dem:

($\Rightarrow$) Se $a \equiv b \pmod{m}$ então $m \mid a - b$.

Usando o algoritmo da divisão

$$\begin{cases} a = m a_1 + r_1, & 0 \leq r_1 < m \\ b = m b_2 + r_2, & 0 \leq r_2 < m \end{cases}$$

Daí, $a - b = (m a_1 + r_1) - (m b_2 + r_2) \Rightarrow$

$a - b = m(a_1 - b_2) + (r_1 - r_2)$. Como $m \mid a - b$ e $m \mid m(a_1 - b_1)$, segue que $m \mid r_1 - r_2$. Supomhamos que $r_1 \geq r_2$ (sem perda de generalidade) então $0 \leq r_1 - r_2 < m$. Logo $m \mid r_1 - r_2 \Rightarrow r_1 - r_2 = 0 \Rightarrow$ $r_1 = r_2$.

Agora considere que a e b tenham o mesmo resto quando divididos por m. Isto é,

$$a = m a_1 + r \qquad 0 \leq r < m$$
$$b = m b_1 + r$$

Daí, $a - b = m(a_1 - b_1) \Rightarrow m \mid a - b \Rightarrow$

$a \equiv b \pmod m$.

■

Definição: Uma coleção de inteiros $\{a_1, \ldots, a_m\}$ diz-se um sistema completo de resíduos módulo m se cada um dos inteiros é congruente módulo m a um único a_i.

Note que o sistema de resíduos mais simples de podemos obter é $\{0, 1, 2, \ldots, m-1\}$

obs: (Explicação) Seja $a \in \mathbb{Z}$ então dividindo a por m, temos que

$$a = mq_1 + r, \quad 0 \leq r < m.$$ Como $r \in \mathbb{Z}$ então $r \in \{0, 1, \ldots, m-1\}$. Usando a prop. 3.2.2, se dividirmos r por m, pelo algoritmo da divisão

$$r = 0 \cdot m + r.$$

Logo, os restos de a e r na divisão por m são os mesmos, donde segue que $a \equiv r \pmod{r}$, ou seja a é congruente a algum elemento de $\{0, 1, \ldots, m-1\}$. Pelo próprio algoritmo da divisão como r é único, segue a unicidade.

Observe também que esse não é o único sistema de resíduos módulo m. Seja $a \in \mathbb{Z}$ então

$$a = mq_1 + r, \quad 0 \leq r < m.$$

Tome então $\{a, a+1, \ldots, a+(m-1)\}$.

Proposição 3.2.3

Sejam $m > 0$ um inteiro fixo e a, b, c, d inteiros

arbitrários. Então, valem as seguintes propriedades:

(i) $a \equiv a \pmod{m}$

(ii) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$

(iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

(iv) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a+c \equiv a+d \pmod{m}$

(v) Se $a \equiv b \pmod{m}$ então $a+c \equiv b+c \pmod{m}$

(vi) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ então, $ac \equiv bd \pmod{m}$

(vii) Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$, $\forall n > 0$

(viii) Se $a+c \equiv b+c \pmod{m}$, então $a \equiv b \pmod{m}$.

Demonstração: a cargo de vocês.

Proposição 3.2.4 (É o mais próximo que chegamos de uma prop. cancelativa para a multiplicação)

Seja m um inteiro fixo e sejam a, b e c inteiros arbitrários. Se $mdc(c, m) = 1$, então $ac \equiv bc \pmod{m}$ implica $a \equiv b \pmod{m}$.

Demonstração:

Se $ac \equiv bc \pmod{m}$, temos que $m \mid ac - bc = c(a-b)$

Como $mdc(c, m) = 1$, pelo teorema de Euclides,

$m \mid a-b \Rightarrow a \equiv b \pmod{m}$. ∎

Note que se $mdc(c, m) \neq 1$, então não vale o cancelamento

$3 \cdot 3 \equiv 3 \cdot 5 \pmod 6$, mas $3 \equiv 5 \pmod 6$.

Observe que se $mdc(c, m) = d \neq 1$, sempre existem a e b tais que $a \not\equiv b \pmod m$ mas $ac \equiv bc \pmod m$

Se $d = m$, i.e, $m \mid c \Rightarrow (c \equiv 0 \mod m)$, daí, para quaisquer inteiros arbitrários a e b, tem-se que

$m \mid c(a-b) \Rightarrow ac \equiv bc \pmod m$.

Agora, se $d < m$ (note que d não pode ser maior que m) então podemos escrever

$m = kd$

$c = k' \cdot d \Rightarrow ck = k'kd = ck = k'm$

Daí, $k \not\equiv 0 \mod m$ (pois $k < m$), mas

$ck \equiv c \cdot 0 \pmod m$, ou seja estamos tomando $a = k$ e $b = 0$.

obs/ leiam os exemplos

→ Solução da lista 4:

Ex 1

(i) Note que

$11 \equiv 4 \pmod 7$

$18 \equiv 4 \pmod 7$

$2322 \equiv 5 \pmod 7$

$13 \equiv 6 \pmod 7$

$19 \equiv 5 \pmod 7$

Então $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv \underbrace{4 \cdot 4}_{16} \cdot \underbrace{5}_{30} \cdot 6 \cdot 5 \pmod 7$. Assim,

como $16 \equiv 2 \pmod 7$ e $30 \equiv 2 \pmod m$ segue que

$11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv 2 \cdot 2 \cdot 5 \pmod 7$ e como

$20 \equiv 6 \pmod 7$, então $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv 6 \pmod 7$

(ii)

Primeiro, observe que para $a \geq 1$ par temos que

$a = 2 \cdot k$ daí, $2^a = 2^{2k} = 4^k \equiv 0 \pmod 4 \Rightarrow$

$2^a \equiv 0 \pmod 4$.

Se $a \geq 1$ é ímpar então $a = 2k+1$, daí

$2^a = 2^{(2k+1)} = 2^{2k} \cdot 2 = 4^k \cdot 2 \equiv 0 \cdot 2 \equiv 0 \pmod 4$

Assim, $(1+2) + 2^2 + \dots + 2^{19} \equiv \underbrace{3}_{3} + 0 \pmod 4$, pois

$2^2 + \dots + 2^{19} \equiv 0 \pmod 4$

Ex 2)

($\Rightarrow$) Suponha que $a \equiv b \pmod r$, então

$$r \mid a-b.$$

Daí, $(a-b) = r \cdot k$, $k \in \mathbb{Z} \Rightarrow (a-b)s = rs \cdot k \Rightarrow$

$rs \mid (as-bs) \Rightarrow as \equiv bs \pmod{rs}$.

Reciprocamente, se $as \equiv bs \pmod{rs}$, então

$rs \mid as-bs \Rightarrow (a-b)s = rs \cdot k$, $k \in \mathbb{Z} \Rightarrow$

$a-b = r \cdot k$, $k \in \mathbb{Z}$. Logo, $a \equiv b \pmod r$.

Ex 3)

Considere p um primo. Suponha que $p^2 \mid m$. Daí,

$m = p^2 c$. Note que $x = pc$ é solução de $X^2 \equiv 0 \pmod m$

pois $(pc)^2 = p^2c^2 = (p^2 c)\, c = mc \Rightarrow m \mid (pc)^2$. No

entanto, $x = pc$ não é solução de $X \equiv 0 \pmod m$, pois

se $m \mid pc \Rightarrow$ ~~pc~~ $= p^2 c \cdot k \Rightarrow 1 = p \cdot k \Rightarrow$

$p \mid 1$, contradição.

Assim, $m = p_1 \cdots p_k$. (livre de quadrados). De fato,

se X é solução de $X^2 \equiv 0 \mod m \Rightarrow$

$$m \mid X^2 \Rightarrow p_1 \cdots p_k \mid X^2 \Rightarrow$$

$p_i \mid X^2$, $i = 1, \ldots, k$.

Logo $p_i \mid X$, $i = 1, \ldots, k$ então $m \mid X$ (porque?)

obs: Deriam o teorema fundamental da Aritmética (seção 2.6).

Ex 4) Vamos provar que $n^7 \equiv n \pmod{42}$, $\forall n \in \mathbb{Z}$.

Queremos que $42 \mid n^7 - n$. Repare que se

$2 \mid n^7 - n$, $3 \mid n^7 - n$ e $7 \mid n^7 - n$ então $42 \mid n^7 - n$.

Como n^7 e n tem a mesma paridade, segue que

$2 \mid n^7 - n$.

Vamos mostrar que $3 \mid n^7 - n$. Observe que

$$n^7 - n = n(n^6 - 1) = n((n^3)^2 - 1) =$$

$$n(n^3 - 1)(n^3 + 1) = n(n-1)(n^2 + n + 1)(n^3 + 1) =$$

$$n(n-1)(n^2+n+1)(n+1)(n^2-n+1) \quad (*)$$

Temos que $n = 3k + r$, $r = 0, 1, 2$. Se $n = 3k$ então $3 \mid n^7 - n$. Se $n = 3k+1$, temos que $n - 1 = 3k$, daí, $3 \mid n^7 - n$. Por fim, se $n = 3k + 2$, $n + 1 = 3(k+1)$ e segue que $3 \mid n^7 - n$.

Agora, precisamos mostrar que $7 \mid n^7 - n$. Considere $n = 7k + r$, $r = 0, 1, 2, 3, 4, 5, 6$. Se $n = 7k$, usando (*), $7 \mid n^7 - n$.

Se $n = 7k + 1$ então $n - 1 = 7k$, daí, $7 \mid n^7 - 7$.

Se $n = 7k + 2$ então $(7k+2)^2 + 7k + 2 + 1 =$

$$7^2k^2 + 7 \cdot 4k + 4 + 7k + 2 + 1 = 7^2k^2 + 7 \cdot 4k + 7k + 7$$

Portanto, $7 \mid n^7 - n$.

Se $n = 7k + 3$ então $(7k+3)^2 - (7k+3) + 1 =$

$$7^2k^2 + 7 \cdot 6k + 9 - 7k - 3 + 1 =$$

$$7^2k^2 + 7 \cdot 6k - 7k + 7$$

Logo $7 \mid n^7 - n$.

Se $n = 7k+4$, então $(7k+4)^2 + (7k+4) + 1 =$

$7^2k^2 + 7\cdot 8k + 16 + 7k + 4 + 1 = 7^2k^2 + 7\cdot 8k + 7k + 21$

Portanto $7 \mid n^7 - n$.

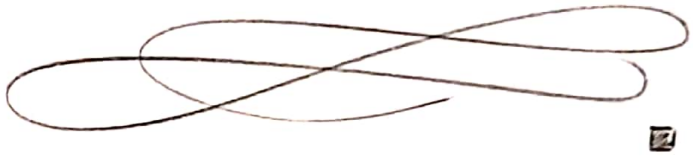
Se $n = 7k+5$, então $(7k+5)^2 - (7k+5) + 1 =$

$7^2k^2 + 7\cdot 10k + 25 - 7k - 5 + 1 =$

$7^2k^2 + 7\cdot 10k - 7k + 21$. Daí, $7 \mid n^7 - n$.

Por fim, se $n = 7k+6$, $n+1 = 7k+7$ e segue que

$7 \mid n^7 + n$.



Ex 5) Queremos provar que $a^{2^n} \equiv 1 \pmod{2^{n+2}}$, $\forall n \geq 1$.

Por indução em n. Se $n = 1$,

$$a^2 - 1 = (a-1)(a+1) = (2k+1-1)(2k+1+1) =$$

$2k(2(k+1)) = 4k\cdot(k+1)$. Note que k ou $k+1$ são pares então $8 \mid a^2 - 1$. Daí, $a^2 \equiv 1 \pmod 8$.

Suponhamos que $a^{2^n} \equiv 1 \pmod{2^{n+2}}$. Vamos mostrar que $a^{2^{n+1}} \equiv 1 \pmod{2^{n+3}}$. Temos que

$$a^{2^{n+1}} - 1 = a^{2\cdot 2^n} = (a^{2^n})^2 - 1 = (a^{2^n} - 1)(a^{2^n} + 1).$$

Como $a^{2^n} \equiv 1 \pmod{2^{n+2}} \Rightarrow 2^{n+2} \mid a^{2^n} - 1 \Rightarrow$

$a^{2^n} - 1 = 2^{n+2} \cdot x$, $x \in \mathbb{Z}$. Usando que a é ímpar $a^{2^n} + 1$ é par. Daí, $a^{2^n} + 1 = 2l$, $l \in \mathbb{Z}$. Com efeito,

$$(a^{2^n} - 1)(a^{2^n} + 1) = 2^{n+2} \cdot x \cdot 2l \Rightarrow$$

$$(a^{2^n} - 1)(a^{2^n} + 1) = 2^{n+3}(x \cdot l) \Rightarrow$$

$$2^{n+3} \mid (a^{2^n} - 1)(a^{2^n} + 1) \Rightarrow a^{2^{n+1}} \equiv 1 \pmod{2^{n+3}}$$

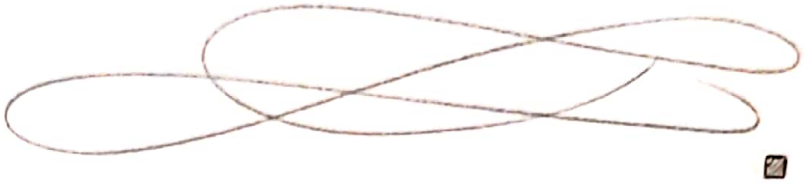
■

Ex 6) Temos que $\{a_1, \ldots, a_n\}$ é um sistema completo de resíduos módulo n. Queremos provar que $\{aa_1, \ldots, aa_n\}$ também é um sistema completo de resíduos módulo n.

Note que $aa_i \not\equiv aa_j \pmod{n}$. Suponhamos por absurdo que $aa_i \equiv aa_j \pmod{n} \Rightarrow n \mid a(a_i - a_j)$. Usando o teorema de Euclides, como $mdc(n, a) = 1$, segue que $n \mid a_i - a_j \Rightarrow a_i \equiv a_j \pmod{n}$, uma contradição.

Agora, note também que para $i \in \{1, \ldots, n\}$ $aa_i \equiv a_j \pmod{n}$ para algum $j \in \{1, \ldots, n\}$. Assim, seja $x \in \mathbb{Z}$, $x \equiv a_j \pmod{n}$ então $x \equiv aa_i \pmod{n}$. Logo, $\{aa_1, \ldots, aa_n\}$ é um sistema

completo de resíduos módulo n.



Ex 7)

(i) $25X \equiv 15 \pmod{29}$

Note que $25 \equiv -4 \pmod{29}$, então

$-4X \equiv 15 \pmod{29} \overset{\text{prop 3.2.4}}{\Leftrightarrow} -4 \cdot 7X \equiv 15 \cdot 7 \pmod{29} \Leftrightarrow$

$-28X \equiv 15 \cdot 7 \pmod{29} \Leftrightarrow X \equiv 15 \cdot 7 \pmod{29} \Leftrightarrow X \equiv 18 \pmod{29}$

$-28 \equiv 1 \pmod{29}$

obs: Considere uma equação da forma $X \equiv b \pmod{m}$

Como $mdc(1, m) = 1$ e $1 | b$ tal equação tem solução.

Note que $m | X - b \Leftrightarrow X - b = my \Rightarrow$

$X - my = b$. Assim vamos resolver a eq. diofantina

Como $mdc(1, -m) = 1$, segue que $\underbrace{1 \cdot 1}_{r} + \underbrace{0 \cdot (-m)}_{s} = 1$.

Portanto, uma solução particular é

$$x_0 = 1 \cdot b = b$$

E a solução geral é

$$x = b + mt, \quad t \in \mathbb{Z}$$

E o conjunto de soluções não congruentes duas a duas

é apenas $\{x = b\}$. Qualquer outra solução é congruente a $x = b$.

Voltando ao ex (i) as soluções são $x = 18 + 29t$, $t \in \mathbb{Z}$.

(ii) $5x \equiv 2 \pmod{26}$ $(\text{mdc}(5, 26) = 1)$

Como $5 \equiv 5 \pmod{26} \iff 25x \equiv 10 \pmod{26}$.

Usando que $25 \equiv -1 \pmod{26}$, segue que

$-x \equiv 10 \pmod{26} \iff x \equiv -10 \pmod{26} \iff$

$x \equiv 16 \pmod{26}$

Portanto as soluções são $x = 16 + 26t$, $t \in \mathbb{Z}$.

(iii) $140x \equiv 133 \pmod{301}$

Primeiro faremos o mdc(140, 301).

	2	6	1	2
301 |	140	21	14	7
21 |	14	7	0	

Como $7 \mid 133$, segue que a equação tem solução. Honestamente, nesse caso a melhor ideia é resolver a equação diofantina

correspondente.

Ex 4) Queremos resolver a equação

$$17X \equiv 3 \mod (2 \cdot 3 \cdot 5 \cdot 7)$$

Uma alternativa é resolver a equação diofantina correspondente.