/ /

UFRS - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 02 de Maio de 2017

$$\begin{cases} x \equiv 1 \pmod{13} \\ x \equiv 4 \pmod{15} \\ x \equiv 8 \pmod{19} \end{cases}$$

R	Q	x	Y
13	-	1	0
15	-	0	1
13	0	1	0
2	1	-1	1
1	6	7	-6
0	2	-	-

$\to x \equiv 1 + 13k$

$1 + 13k \equiv 4 \pmod{15}$

$13k \equiv 3 \pmod{15}$

$7 \cdot 13k \equiv 7 \cdot 3 \pmod{15}$

$k \equiv 21 \pmod{15}$

$k \equiv 6 \pmod{15}$

$k \equiv 6 + 15l$

$x \equiv 1 + 13k$

$x \equiv 1 + 13(6 + 15l)$

$x \equiv 1 + 78 + 195l$

$x \equiv 79 + 195l$

$x \equiv 79 \pmod{195}$

$$\begin{cases} x \equiv 79 \pmod{195} \\ x \equiv 8 \pmod{19} \end{cases}$$

$\to x = 79 + 195l$

$79 + 195l \equiv 8 \pmod{19}$

$3 + 5l \equiv 8 \pmod{19}$

$5l \equiv 5 \pmod{19}$

$l \equiv 1 \pmod{19}$

$l = 1 + 19m$

$x = 79 + 195\ell$

$x = 79 + 195(1 + 19m)$

$x = 79 + 195 + 3705m$

$x = 274 + 3705m$

$x \equiv 274 \pmod{3705}$

Esse método de resolução de sistemas de congruências é conhecido como Algoritmo Chinês do Resto

- TEOREMA CHINÊS DO RESTO

Sejam m e n inteiros positivos tais que $MDC(m,n) = 1$. Então, o sistema:

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

sempre tem uma única solução módulo mn.

- EXISTÊNCIA (PROVA CONSTRUTIVA):

$x \equiv a \pmod{m}$

$x = a + mk$

$\downarrow$

$x \equiv b \pmod{n}$

$a + mk \equiv b \pmod{n}$

$mk \equiv (b-a) \pmod{n}$

Preciso calcular o inverso de m módulo n. Como $MDC(m,n) = 1$, esse inverso existe e pode ser obtido com o algoritmo euclidiano estendido. Seja m' este inverso. m' é o inverso de m módulo n.

$mm' \equiv 1 \pmod{n}$

Obtemos m' com o algoritmo euclidiano estendido entre m e n

$\Downarrow$

$$\underset{\overset{\shortparallel}{m'}}{\alpha} m + \beta n = 1$$

$$mk \equiv (b-a) \pmod{n}$$

$\Downarrow$ MULTIPLICO DOS DOIS LADOS POR m'

$$m'mk \equiv m'(b-a) \pmod{n}$$
$$k \equiv m'(b-a) \pmod{n}$$

$$k = m'(b-a) + n\ell$$

$$x = a + mk =$$
$$= a + m(m'(b-a) + n\ell) =$$
$$= a + mm'(b-a) + mn\ell$$

Substituindo m' por α:

$$x = a + m\alpha(b-a) + mn\ell =$$
$$= a + m\alpha b - m\alpha a + mn\ell =$$
$$= a\underbrace{(1-m\alpha)}_{\beta n} + m\alpha b + mn\ell =$$
$$= a\beta n + b\alpha m + mn\ell$$

$$x \equiv a\beta n + b\alpha m \pmod{mn}$$

- UNICIDADE

Suponha, por contradição, que existam duas soluções distintas x_1 e x_2 para o sistema

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

módulo mn. Isto é,

$$\left. x_1 \not\equiv x_2 \pmod{mn} \right\} (*)$$

$$\begin{cases} x_1 \equiv a \pmod{m} \\ x_1 \equiv b \pmod{n} \end{cases} \qquad \begin{cases} x_2 \equiv a \pmod{m} \\ x_2 \equiv b \pmod{n} \end{cases}$$

$x_1 \equiv a \pmod{m}$

$\underline{x_2 \equiv a \pmod{m}}$ (SUBTRAIR)

$x_1 - x_2 \equiv 0 \pmod{n}$

$\Downarrow$

m divide $x_1 - x_2$

$x_1 \equiv b \pmod{n}$

$\underline{x_2 \equiv b \pmod{n}}$ (SUBTRAIR)

$x_1 - x_2 \equiv 0 \pmod{n}$

$\Downarrow$

n divide $x_1 - x_2$

$$\left. \begin{array}{l} m \text{ divide } x_1 - x_2 \\ n \text{ divide } x_1 - x_2 \\ MDC(m,n) = 1 \end{array} \right\} mn \text{ divide } x_1 - x_2 \Rightarrow \underbrace{x_1 \equiv x_2 \pmod{mn}}_{(**)}$$

LEMA DA 2ª SEMANA DE AULA

tilibra

$(*) + (**) =$ CONTRADIÇÃO

Logo, a solução é única módulo mn.

- EXEMPLO:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 0 \pmod 7 \\ x \equiv 3 \pmod{11} \\ x \equiv 2 \pmod{14} \end{cases}$$

R	Q	X	Y
3	–	1	0
7	–	0	1
3	0	1	0
1	2	-2	1
0	3	–	–

$\to x \equiv 1 \pmod 3$

$x = 1 + 3k$

$1 + 3k \equiv 0 \pmod 7$

$3k \equiv -1 \pmod 7$

$3k \equiv 6 \pmod 7$

$5 \cdot 3k \equiv 5 \cdot 6 \pmod 7$

$k \equiv 30 \equiv 2 \pmod 7$

$k \equiv 2 \pmod 7$

$k = 2 + 7\ell$

$x = 1 + 3k =$

$= 1 + 3(2 + 7\ell) =$

$= 1 + 6 + 21\ell =$

$= 7 + 21\ell$

$x \equiv 7 \pmod{21}$

$7 + 21\ell \equiv 3 \pmod{11}$

$7 + 10\ell \equiv 3 \pmod{11}$

$(10 \equiv -1 \pmod{11})$

$7 - \ell \equiv 3 \pmod{11}$

$\ell \equiv 4 \pmod{11}$

$\ell = 4 + 11m$

$x = 7 + 21\ell =$

$= 7 + 21(4 + 11m)$

$= 7 + 84 + 231m$

$= 91 + 231m$

$x \equiv 91 \pmod{231}$

$91 + 231m \equiv 2 \pmod{19}$

$15 + 3m \equiv 2 \pmod{19}$

$3m \equiv -13 \pmod{19}$

$3m \equiv 6 \pmod{19}$

$13 \cdot 3m \equiv 6 \cdot 13 \pmod{19}$

$m \equiv 78 \pmod{19}$

$m \equiv 2 \pmod{19}$

$m = 2 + 19n$

R	Q	X	Y
3	–	1	0
19	–	0	1
3	0	1	0
1	6	-6	1
0	3	–	–

$x = 91 + 231m =$

$= 91 + 231(2 + 19n) =$

$= 91 + 462 + 4389n =$

$= 553 + 4389n$

$x \equiv 553 \pmod{4389}$

- ALGORITMO CHINÊS DO RESTO PARA CÁLCULO DE POTÊNCIAS MODULARES

2^{6754} (modulo 1155)

Não posso fazer $2^{1154} \equiv 1 \pmod{1155}$. O teorema de Fermat só é válido se o módulo for primo.!

Começo fatorando:

$1155 = 3 \cdot 5 \cdot 7 \cdot 11$

Vou calcular:

$2^{6754} \equiv \quad \pmod{3}$	$2^{6754} \equiv \quad \pmod{7}$
$2^{6754} \equiv \quad \pmod{5}$	$2^{6754} \equiv \quad \pmod{11}$

- MÓDULO 3

$2 \not\equiv 0 \pmod 3$

$2^2 \equiv 1 \pmod 3$

$2^{6754} \equiv \underbrace{(2^2)}_{\equiv 1}{}^{3377} \equiv 1 \pmod 3$

- MÓDULO 5

$2 \not\equiv 0 \pmod 5$

$2^4 \equiv 1 \pmod 5$

$2^{6754} \equiv \underbrace{(2^4)}_{\equiv 1}{}^{1688} \cdot 2^2 \equiv 4 \pmod 5$

- MÓDULO 7

$2 \not\equiv 0 \pmod 7$

$2^6 \equiv 1 \pmod 7$

$2^{6754} \equiv \underbrace{(2^6)}_{\equiv 1}{}^{1125} \cdot 2^4 \equiv 16 \equiv 2 \pmod 7$

- MÓDULO 11:

$2 \not\equiv 0 \pmod{11}$

$2^{10} \equiv 1 \pmod{11}$

$2^{6754} \equiv \underbrace{(2^{10})}_{\equiv 1}{}^{675} \cdot 2^4 \equiv 16 \equiv 5 \pmod{11}$

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 2 \pmod 7 \\ x \equiv 5 \pmod{11} \end{cases}$$

↳ PRIMOS DISTINTOS

$x = 1+3k$

$1+3k \equiv 4 \pmod 5$

$3k \equiv 4 \pmod 5$

$k \equiv 1 \pmod 5$

$k = 1+5\ell$

$x = 1+3k =$

$= 1+3(1+5\ell)$

$= 1+3+15\ell =$

$= 4+15\ell$

$4+15\ell \equiv 2 \pmod 7$

$4+\ell \equiv 2 \pmod 7$

$\ell \equiv -2 \pmod 7$

$\ell \equiv 5 \pmod 7$

$\ell = 5+7m$

$x = 4+15\ell =$

$= 4+15(5+7m) =$

$= 4+75+105m) =$

$= 79+105m$

$79+105m \equiv 5 \pmod{11}$

$2+6m \equiv 5 \pmod{11}$

$6m \equiv 3 \pmod{11}$

$2 \cdot 6m \equiv 2 \cdot 3$

$m \equiv 6 \pmod{11}$

$m = 6+11n$

R	Q	X	Y
6	–	1	0
11	–	0	1
6	0	1	0
5	1	-1	1
1	1	2	-1
0	5	–	–

$x = 79 + 105m =$

$= 79 + 105(6 + 11n) =$

$= 79 + 630 + 1155n$

$= 709 + 1155n$

$x \equiv 709 \pmod{1155}$

$2^{6754} \equiv 709 \pmod{1155}$

CONCLUSÃO: Quando o módulo é composto, mas é o produto de primos distintos, eu posso usar o algoritmo chinês do resto em conjunto com o Teorema de Fermat para facilitar o cálculo de potências.

- MATÉRIA DA P2:

CAPÍTULO 4 - COLLIER
CAPÍTULO 5 - COLLIER (EXCETO "PRINCÍPIO DA INDUÇÃO")
CAPÍTULO 6 - COLLIER
CAPÍTULO 7 - COLLIER
PARTES EQUIVALENTES DOS CAPÍTULOS 2 E 3 DO MENASCHE