DISMAT 1MI

by: RaVeN

Note Title .17.10.2009

① a) $a = 777 \quad b = 629$

$777 = 1 \cdot 629 + 148$

$629 = 4 \cdot 148 + 37 \qquad g = 37$

$148 = 4 \cdot 37$

i) $37 = 629 - 4 \cdot 148 = 629 - 4 \cdot (777 - 629)$

$= \underset{y}{5} \cdot 629 - \underset{x}{4} \cdot 777$

ii)

i	-1	0	1	2
q_i			1	4
x_i	1	0	1	-4
y_i	0	1	-1	5

$x = -4 \quad y = 5$

b) $a = 1643 \quad b = 901$

$1643 = 1 \cdot 901 + 742$

$901 = 1 \cdot 742 + 159$

$742 = 4 \cdot 159 + 106 \qquad g = 53$

$159 = 1 \cdot 106 + 53$

$106 = 2 \cdot 53$

i	-1	0	1	2	3	4
q_i			1	1	4	1
x_i	1	0	1	-1	5	-6
y_i	0	1	-1	2	-9	11

$x = -6$

$y = 11$

c) $a = 1105 \quad b = 481$

$1105 = 2 \cdot 481 + 143$

$481 = 3 \cdot 143 + 52$ $\qquad g = 13$

$143 = 2 \cdot 52 + 39$

$52 = 1 \cdot 39 + 13$

$39 = 3 \cdot 13$

i	-1	0	1	2	3	4
q_i			2	3	2	1
x_i	1	0	1	-3	7	-10
y_i	0	1	-2	7	-16	23

$x = -10$

$y = 23$

② $713! \quad 1713!$

$$\left\lfloor \frac{713}{5} \right\rfloor + \left\lfloor \frac{713}{25} \right\rfloor + \left\lfloor \frac{713}{125} \right\rfloor + \left\lfloor \frac{713}{625} \right\rfloor =$$

$$= 142 + 28 + 5 + 1 = 176$$

$$\left\lfloor \frac{1713}{5} \right\rfloor + \left\lfloor \frac{1713}{25} \right\rfloor + \left\lfloor \frac{1713}{125} \right\rfloor + \left\lfloor \frac{1713}{625} \right\rfloor =$$

$$= 342 + 68 + 13 + 2 = 425$$

(3) a) $311x \equiv 7 \pmod{401}$

$401 = 1 \cdot 311 + 90$

$311 = 3 \cdot 90 + 41$

$90 = 2 \cdot 41 + 8$

$41 = 5 \cdot 8 + 1$

$8 = 8 \cdot 1$

i	-1	0	1	2	3	4
q_i			1	3	2	5
y_i	0	1	-1	4	-9	49

$u \equiv 49 \pmod{401}$

$x \equiv 49 \cdot 7 \pmod{401}$

$\equiv 343 \pmod{401}$

4) $153x \equiv 71 \pmod{391}$

$391 = 2 \cdot 153 + 85$

$153 = 1 \cdot 85 + 68$

$85 = 1 \cdot 68 + 17$

$68 = 4 \cdot 17$

c) $213x \equiv 75 \pmod{333}$

$71x \equiv 25 \pmod{111}$

$111 = 1 \cdot 71 + 40$
$71 = 1 \cdot 40 + 31$
$40 = 1 \cdot 31 + 9$
$31 = 3 \cdot 9 + 4$
$9 = 2 \cdot 4 + 1$
$4 = 4 \cdot 1$

i	-1	0	1	2	3	4	5
q_i			1	1	1	3	2
y_i	0	1	-1	2	-3	11	-25

$-25 + 111 = 86$

$u \equiv 86 \pmod{111}$

$x \equiv 86 \cdot 25 \pmod{111} \equiv 2150 \pmod{111}$
$\equiv 41 \pmod{111}$

$x \equiv 41, 152, 263 \pmod{333}$

④ a) $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, $x \equiv 3 \pmod 7$

$42 \cdot x_1 \equiv 1 \pmod 5 \Rightarrow 2x_1 \equiv 1 \pmod 5$
$35 \cdot x_2 \equiv 2 \pmod 6 \Rightarrow 5x_2 \equiv 2 \pmod 6$
$30 \cdot x_3 \equiv 3 \pmod 7 \Rightarrow 2x_3 \equiv 3 \pmod 7$

$x_1 = 3 \quad x_2 = 4 \quad x_3 = 5$

$x \equiv x_0 \pmod{m_1 \cdot m_2 \cdot m_3}$
$x \equiv 416 \pmod{210}$
$x \equiv 206 \pmod{210}$

$x_0 = 42 \cdot 3 + 35 \cdot 4 + 30 \cdot 5$
$x_0 = 416$

b) $x_1 \equiv 5 \pmod 7$, $x_2 \equiv 9 \pmod{13}$, $x_3 \equiv 8 \pmod{11}$

$143 x_1 \equiv 5 \pmod 7 \Rightarrow 3 \cdot x_1 \equiv 5 \pmod 7$

$77 x_2 \equiv 9 \pmod{13} \Rightarrow 12 \cdot x_2 \equiv 9 \pmod{13}$

$91 x_3 \equiv 8 \pmod{11} \Rightarrow 3 \cdot x_3 \equiv 8 \pmod{11}$

$x_1 = 4 \quad x_2 = 4 \quad x_3 = 10$

$x_0 = 143 \cdot 4 + 77 \cdot 4 + 91 \cdot 10$

$x_0 = 1790$

$x = 1790 \pmod{1001}$

$x = 789 \pmod{1001}$

c) $x_1 \equiv 1 \pmod 4$, $x_2 \equiv 7 \pmod 9$, $x_3 \equiv 22 \pmod{25}$

$225 \cdot x_1 \equiv 1 \pmod 4 \Rightarrow 1 \cdot x_1 = 1 \pmod 4$

$100 \cdot x_2 \equiv 7 \pmod 9 \Rightarrow 1 \cdot x_2 = 7 \pmod 9$

$36 \cdot x_3 \equiv 22 \pmod{25} \Rightarrow 11 \cdot x_3 = 22 \pmod{25}$

$x_1 = 1 \quad x_2 = 7 \quad x_3 = 2$

$x_0 = 225 \cdot 1 + 100 \cdot 7 + 36 \cdot 2$

$x_0 = 997$

$x = 997 \pmod{900}$

$x = 97 \pmod{900}$

⑤ $\varphi(n) = 30 \qquad 30 = 2 \cdot 3 \cdot 5$

$p \in \{2, 3, 7, 11, 31\}$

$n = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 7^{\alpha_3} \cdot 11^{\alpha_4} \cdot 31^{\alpha_5}$

$\varphi(n) = p_i^{\alpha_i - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1)$

$\alpha_1 = \alpha_2 \leq 2$

$\alpha_3 = \alpha_4 = \alpha_5 \leq 1$

1) $n = 31 \cdot k \Rightarrow \varphi(n) = 30 \cdot \varphi(k) \qquad k = 1, 2$

($\varphi(k) = 1$)

$n = 31 \cdot 1 = 31$

$n = 31 \cdot 2 = 62$

2) $n = 11 \cdot k \Rightarrow \varphi(n) = 10 \cdot \underbrace{\varphi(k)}_{3}$ k - nema rj.

3) $n = 7 \cdot k \Rightarrow \varphi(n) = 6 \cdot \underbrace{\varphi(k)}_{5}$ k - nema rj

4) $n = k \quad k = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3}$

$$\varphi(k) = 2^{\alpha_1 - 1} \cdot 1 \cdot 3^{\alpha_2 - 1} \cdot 5^{\alpha_3 - 1} \cdot 4$$

5 rij u kanpu P

⑥ $\varphi(n) = 58 \quad = 2 \cdot 29$

$p \in \{2, 3, 59\}$ $\quad n = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 59^{\alpha_3}$

$\alpha_1 \leq 2$

$\alpha_2 = \alpha_3 \leq 1$

1) $n = 59 \cdot k \Rightarrow \varphi(n) = 58 \cdot \underbrace{\varphi(k)}_{1}$ $k = 1, 2$ $n = 59, 118$

2) $n = 3 \cdot k \Rightarrow \varphi(n) = 2 \cdot \underbrace{\varphi(k)}_{29}$ k - nema rj.

(7) a) $p = 61$ $\quad p-1 = 60$ $\quad 60 = \underbrace{2 \cdot 2 \cdot 3 \cdot 5}_{q}$

$$g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$$

$$g^{\frac{60}{2}} \not\equiv 1 \pmod{61}$$

$$g^{\frac{60}{3}} \not\equiv 1 \pmod{61}$$

$$g^{\frac{60}{5}} \not\equiv 1 \pmod{61}$$

$$2^{30} \not\equiv 1 \pmod{61} \checkmark$$

$$2^{20} \not\equiv 1 \pmod{61} \checkmark$$

$$2^{12} \not\equiv 1 \pmod{61} \checkmark$$

2 je prim. korijen

b) $x^7 \equiv 24 \pmod{61} \quad / \ ind_2$

$$7\, ind_2(x) \equiv ind_2(24) \pmod{60}$$

$$2^y \equiv 24 \pmod{61}$$

$$2^3 \equiv 8 \pmod{61}$$

$$2^6 = 64 \equiv 3 \pmod{61}$$

$$2^3 \cdot 2^6 = 2^9 \equiv 24 \pmod{61}$$

$$7\, ind_2(x) = ind_2(2^9) \pmod{60}$$

$$7 \underbrace{\operatorname{ind}_2(x)}_{y} \equiv 9 \pmod{60}$$

$$\Downarrow$$

$$7y \equiv 9 \pmod{60}$$

$60 = 8 \cdot 7 + 4$

$7 = 1 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$3 = 3 \cdot 1$

i	-1	0	1	2	3
q_i			8	1	1
y_i	0	1	-8	9	-17

$-17 + 60 = 43$

$$u \equiv 43 \pmod{60}$$

$$y \equiv 387 \pmod{60}$$

$$y \equiv 27 \pmod{60}$$

$$\operatorname{ind}_2(x) = 27 \pmod{60}$$

$$x \equiv 2^{27} \pmod{61}$$

$$x \equiv 38 \pmod{61}$$

(8) a) $p = 67$ $\quad p-1 = 66$ $\quad 66 = 2 \cdot 3 \cdot 11$

$$g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$$

$$g^{\frac{66}{2}} \not\equiv 1 \pmod{67}$$

$$g^{\frac{66}{3}} \not\equiv 1 \pmod{67}$$

$$g^{\frac{66}{11}} \not\equiv 1 \pmod{67}$$

$$2^{33} \not\equiv 1 \pmod{67} \quad \checkmark$$

$$2^{22} \not\equiv 1 \pmod{67} \quad \checkmark$$

$$2^{6} \not\equiv 1 \pmod{67} \quad \checkmark$$

2 it is...

b) $x^5 \equiv 61 \pmod{67} \quad / \ ind_2$

$$5 \cdot ind_2(x) \equiv ind_2(61) \pmod{66}$$

$$2^y \equiv 61 \pmod{67} \Rightarrow y = 7$$

$$5 \cdot ind_2(x) \equiv 7 \pmod{66}$$

$$5z \equiv 7 \pmod{66}$$

$$z = 41 \pmod{66}$$

$$\text{ind}_2(x) \equiv 41 \pmod{66}$$

$$x \equiv 2^{41} \pmod{67}$$

$$x \equiv 12 \pmod{67}$$

(9) a) $\left(\frac{51}{97}\right) = \left(\frac{97}{51}\right) \Rightarrow 1 \cdot \left(\frac{46}{51}\right) = \underbrace{\left(\frac{2}{51}\right)}_{-1} \cdot \left(\frac{23}{51}\right) = -\frac{23}{51} = -\left(-\frac{51}{23}\right)$

$51 \equiv 3 \pmod 4$ } $\Rightarrow 1$

$97 \equiv 1 \pmod 4$

$$= -\left(-\frac{1}{23}\right) \cdot \left(\frac{51}{23}\right) = \left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$$

b) $\left(\frac{321}{991}\right) = 1 \cdot \left(\frac{991}{321}\right) = \left(\frac{28}{321}\right) = \underbrace{\left(\frac{2}{321}\right)}_{1} \cdot \underbrace{\left(\frac{2}{321}\right)}_{1} \cdot \left(\frac{7}{321}\right) =$

$321 \equiv 1 \pmod 4$ } $\Rightarrow 1$

$991 \equiv 3 \pmod 4$

$$= \left(\frac{7}{321}\right) = \left(\frac{321}{7}\right) = \left(\frac{6}{7}\right) = \underbrace{\left(\frac{2}{7}\right)}_{1} \cdot \left(\frac{3}{7}\right)$$

$$= \left(\frac{3}{7}\right) = \left(\frac{-7}{3}\right) = \underbrace{\left(\frac{-1}{3}\right)}_{-1} \left(\frac{7}{3}\right)$$

$$= (-1) \cdot \left(\frac{7}{3}\right) = (-1) \cdot \left(\frac{1}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

c) $\left(\frac{-31}{101}\right) = \underbrace{\left(\frac{-1}{101}\right)}_{1} \cdot \left(\frac{31}{101}\right) = \left(\frac{31}{101}\right) =$

$= \left(\frac{101}{31}\right) = \left(\frac{8}{31}\right) = \underbrace{\left(\frac{2}{31}\right)}_{1} \cdot \left(\frac{2}{31}\right) \cdot \left(\frac{2}{31}\right)$

$= 1$

d) $\left(\frac{58}{269}\right) = \left(\frac{2}{269}\right) \cdot \left(\frac{29}{269}\right) = (-1) \cdot \left(\frac{29}{269}\right)$

$= (-1) \cdot \left(\frac{269}{29}\right) = (-1)\left(\frac{8}{29}\right) =$

$= (-1) \cdot \underbrace{\left(\frac{2}{29}\right)}_{-1} \cdot \left(\frac{2}{29}\right) \cdot \left(\frac{2}{29}\right) = 1$

ako je brojnik parni - rastavi na (2/vxx)*(nekaj/vxx)
ako je brojnik neparni a manji od nazivnika preokreni (ali samo ako je brojnik prosti)
kod preokretanja
ako su I brojnik I nazivnik kod djeljenja s 4 dali ostatak 3 onda stavljaš minus u brojnik
ako je brojnik veći od nazivnika, a nije niti -1 niti 2 niti parni, onda radiš modulo brojnik nazivnik
i ako imaš negativni brojnik onda rastaviš na (-1/nazivnik)(ostatak/nazivnik)
i moraš svesti na (-1/nešto= , i onda to nešto djeliš sa 4, ako je ostatak 1 to ti je 1 ako je ostatak 3 onda je -1
ili svedeš na (2/nešto)
to nešto djeliš sa 8
ako je ostatak 1 ili 7 onda je to 1
ako je ostatak 3 ili 5 onda je to -1
eto to je to :D
by MitO