①

DÚ 5 BIKS

CHEMPRO Poprad

Engineering Solutions

19.10.2020

PORADOVÉ ČÍSLO: 9 MARTIN CHLEBOVEC

$x = 17$

$y = 20$ $P = [x, y]$

$k = 19$ $E(E_{23}(1,1)) \Rightarrow (a, b)$

$Z = k \cdot P$

VYPRACOVANIE:

$P(17,20)$ Metóda inverzného prvku cez Euklidov algoritmus

$2Y_P = 2 \cdot 20 = 40$

$nsd(40,23)$ - najväčší spoločný deliteľ

$40 = 23 \cdot 1 + 17 \Rightarrow 17 = 40 - 23 \cdot 1$

$23 = 17 \cdot 1 + 6 \Rightarrow 6 = 23 - 17 \cdot 1$

$17 = 6 \cdot 2 + 5 \Rightarrow 5 = 17 - 6 \cdot 2$

$6 = 5 \cdot 1 + 1 \Rightarrow 1 = 6 - 5 \cdot 1$

$5 = 1 \cdot 5 + 0$

↓ posledný nenulový zvyšok

$1 = 6 - 1 \cdot 5 = 6 - 1(17 - 6 \cdot 2) = 3 \cdot 6 - 1 \cdot 17 = -1 \cdot 17 + 3(23 - 1 \cdot 17) =$

SP: (HOD) $= -4 \cdot 17 + 3 \cdot 23 = 3 \cdot 23 - 4 \cdot (40 - 1 \cdot 23) = 7 \cdot 23 - 4 \cdot 40$

inv. prvok $\longrightarrow$ $k^{-1} = -4 + 23 \bmod 23 = 19 \bmod 23$

Head Office: Žilinská 1, 811 05 Bratislava, Slovak Republic
Engineering Center Poprad: Hodžova 3292/3, 058 01 Poprad, Slovak Republic
Company Id No: 31 651 470; Tax Id No: 2020497303
tel.: +421 940 428 911; e-mail: info@chempro.sk
www.chempro.sk

(2)

CHEMPRO Poprad
Engineering Solutions

$E_{23}(1,1)$

$\text{mod } P = \text{mod } 23$

$P = Q$

Vrcholy 8.5:

$$s = \left(\frac{3x_P^2 + a}{2y_P}\right) \text{mod}_p = \left(3x_P^2 + a\right) \cdot k^{-1} \text{ mod } p \quad \text{ak } P = Q$$

$$x_R = \left(s^2 - 2x_P\right) \text{mod}_p \quad \text{ak } P = Q$$

$$Y_R = \left(s\left(x_P - x_R\right) - Y_P\right) \text{mod}_p$$

$$s = \left(\left[3 \cdot 17^2 + 1\right] \cdot 19\right) \text{mod } 23$$

$$s = (868 \cdot 19) \text{ mod } 23$$

$$s = 16492 \text{ mod } 23$$

$$s = 1$$

$$x_R = 1^2 - 2 \cdot 17 = -33 \text{ mod } 23$$
$$= 13 \text{ mod } 23$$

$$Y_R = (1(17 - 13) - 20) \text{ mod } 23$$

$$Y_R = -16 \text{ mod } 23$$

$$Y_R = 7 \text{ mod } 23$$

EC overenie - skúška správnosti - kongruencia

(x_P, y_P): $y_P^2 \equiv x_P^3 + x_P + 1$

kongruencia

$$7^2 \equiv 13^3 + 13 + 1$$
$$49 \equiv 2211$$
$$3 \equiv 3$$

$2P(13,7)$

Head Office: Žilinská 1, 811 05 Bratislava, Slovak Republic
Engineering Center Poprad: Hodžova 3292/3, 058 01 Poprad, Slovak Republic
Company Id No: 31 651 470; Tax Id No: 2020497303
tel.: +421 940 428 911; e-mail: info@chempro.sk
www.chempro.sk

(3)

CHEMPRO Poprad

Engineering Solutions

2P(13,7)

Inverzia k d

$2_{YP} = 14$

$\gcd(23,14)$

$23 = 14 \cdot 1 + 9 \Rightarrow 9 = 23 - 14 \cdot 1$

$14 = 9 \cdot 1 + 5 \Rightarrow 5 = 14 - 9 \cdot 1$

$9 = 5 \cdot 1 + 4 \Rightarrow 4 = 9 - 5 \cdot 1$

$5 = 4 \cdot 1 + 1 \Rightarrow 1 = 5 - 4 \cdot 1$

$4 = 1 \cdot 4 + 0$

$1 = 5 - 4 \cdot 1 = 5 - 1(9 - 1 \cdot 5) = 2 \cdot 5 - 1 \cdot 9 = -1 \cdot 9 + 2(14 - 1 \cdot 9)$

$= -1 \cdot 9 + 2 \cdot 14 - 2 \cdot 9 = 2 \cdot 14 - 3 \cdot 9 = 2 \cdot 14 - 3(23 - 14 \cdot 1) =$

$= 2 \cdot 14 - 3 \cdot 23 + 3 \cdot 14 = 5 \cdot 14 - 3 \cdot 23$

$k^{-1} = 5$

$n = (3 \cdot 13^2 + 1) \cdot 5 \bmod 23$ $\quad n = 508 \cdot 5 = 2540 \bmod 23$ $\quad n = 10 \bmod 23$

$x_R = 10^2 - 2 \cdot 13 \bmod 23$ $\quad x_R = 74 \bmod 23$ $\quad x_R = 5 \bmod 23$

$y_R = (10(13-5)-7) = 130 - 50 \bmod 23$ $\quad x_R = 4 \bmod 23$

$4^2 \equiv 5^3 + 5 + 1$

$16 \equiv 16$ ✓

4P(5,4)

Head Office: Žilinská 1, 811 05 Bratislava, Slovak Republic
Engineering Center Poprad: Hodžova 3292/3, 058 01 Poprad, Slovak Republic
Company Id No: 31 651 470; Tax Id No: 2020497303
tel.: +421 940 428 911; e-mail: info@chempro.sk
www.chempro.sk

(4)

4P (5,4)

$\gcd(23,8)$ $\quad 2_{YR} = \dot{8}$

$23 = 8 \cdot 2 + 7 \Rightarrow 7 = 23 - 2 \cdot 8$

$8 = 7 \cdot 1 + 1 \Rightarrow 1 = 8 - 7 \cdot 1$

$7 = 1 \cdot 7 + 0$

$1 = 8 - 7 \cdot 1 = 8 - 1(23 - 2 \cdot 8) = 8 - 1 \cdot 23 + 2 \cdot 8 = 3 \cdot 8 - 1 \cdot 23$

$\bar{k}^{-1} = 3$

$n = (3 \cdot 5^2 + 1) \cdot 3 \bmod 23$ $\quad x_R = 21^2 - 2 \cdot 5 \bmod 23$

$n = 228 \equiv 21 \bmod 23$ $\quad x_R = 17 \bmod 23$

$Y_R = 21(5 - 17) - 4 \bmod 23$

$Y_{(R)} = 20 \bmod 23$

EC

$20^2 \equiv 17^3 + 17 + 1$

$9 \equiv 9$ ✓

8P (17, 20)

Head Office: Žilinská 1, 811 05 Bratislava, Slovak Republic
Engineering Center Poprad: Hodžova 3292/3, 058 01 Poprad, Slovak Republic
Company Id No: 31 651 470; Tax Id No: 2020497303
tel.: +421 940 428 911; e-mail: info@chempro.sk
www.chempro.sk

(5)

8P (17,20)

$2r_k = 40$

$\text{nsd}(40,23)$

$40 = 23 \cdot 1 + 17 \Rightarrow 17 = 40 - 23 \cdot 1$

$23 = 17 \cdot 1 + 6 \Rightarrow 6 = 23 - 17 \cdot 1$

$17 = 6 \cdot 2 + 5 \Rightarrow 5 = 17 - 6 \cdot 2$

$6 = 5 \cdot 1 + 1 \Rightarrow 1 = 6 - 5 \cdot 1$

$5 = 5 \cdot 1 + 0$ ✗

$1 = 6 - 5 \cdot 1 = 6 - 1(17 - 6 \cdot 2) = 3 \cdot 6 - 1 \cdot 17 = -1 \cdot 17 + 3(23 - 1 \cdot 17)$

$= -4 \cdot 17 + 3 \cdot 23 = 3 \cdot 23 - 4(40 - 1 \cdot 23) = 7 \cdot 23 - 4 \cdot 40$

inv. prvk $k^{-1} = -4 + 23 \text{ mod } 23 = 19 \text{ mod } 23$

$n = (3 \cdot 17^2 + 1) \cdot 19$

$n = 16492 \text{ mod } 23$

$n = 1$

$x_R = 1^2 - 2 \cdot 17$

$x_R = 13 \text{ mod } 23$

$y_R = (1(17 - 13) - 20) \text{ mod } 23$

$y_R = -16 \text{ mod } 23$

$y_R = 7 \text{ mod } 23$

EC

$7^2 \equiv 13^3 + 13 + 1$

$49 \equiv 2211$

$3 \equiv 3$

16P (13,7)

Head Office: Žilinská 1, 811 05 Bratislava, Slovak Republic
Engineering Center Poprad: Hodžova 3292/3, 058 01 Poprad, Slovak Republic
Company Id No: 31 651 470; Tax Id No: 2020497303
tel.: +421 940 428 911; e-mail: info@chempro.sk
www.chempro.sk

6

CHEMPRO Poprad

Engineering Solutions

$Z = 19P$

$k = 19$

$(1\ 0\ 0\ 1\ 1)_2$

$16\ 8\ 4\ 2\ 1$

$19P = 16P + \overline{2P + 1P} \Rightarrow 1.$

$P \neq Q$

$\lambda = \frac{y_q - y_p}{x_q - x_p}$

$(13 - 17) = -4 \bmod 23 = 19 \bmod 23$

$\gcd(23, 19)$

$23 = 1 \cdot 19 + 4 \Rightarrow$ ~~$23 - 1 \cdot 19 = 4$~~ $4 = 23 - 19 \cdot 1$

$19 = 4 \cdot 4 + 3 \Rightarrow$ $3 = 19 - 4 \cdot 4$

$4 = 1 \cdot 3 + 1 \Rightarrow$ $1 = 4 - 3 \cdot 1$

$3 = 3 \cdot 1 + 0 \Rightarrow$

$1 = 4 - 1 \cdot 3 = 4 - 1(19 - 4 \cdot 4) = 5 \cdot 23 - 6 \cdot 19$

$k^{-1} = -6 + 23 = 17$

Head Office: Žilinská 1, 811 05 Bratislava, Slovak Republic
Engineering Center Poprad: Hodžova 3292/3, 058 01 Poprad, Slovak Republic
Company Id No: 31 651 470; Tax Id No: 2020497303
tel.: +421 940 428 911; e-mail: info@chempro.sk
www.chempro.sk

(7)

CHEMPRO Poprad

Engineering Solutions

(A)

$n = (y_Q - y_P) \cdot 17 \mod 23$

$n = (7 - 20) \cdot 17 \mod 23$

$n = 9 \mod 23$

$x_R = (n^2 - 17 - 13) = 9^2 - 17 - 13 \mod 23$

$57 \mod 23$

$x_R = 5 \mod 23$

$y_R = [9 [17 - 5] - 13 \mod 23$

$y_R = 19 \mod 23$

EC

$19^2 \equiv 5^3 + 5 + 1$

$16 \equiv 131$

$16 \equiv 16$ ✓

$3P \in (5, 19)$

$16P + 3P = 19P$

$x_Q - x_P$

$13 - 5 = 8 \mod 23$

Head Office: Žilinská 1, 811 05 Bratislava, Slovak Republic
Engineering Center Poprad: Hodžova 3292/3, 058 01 Poprad, Slovak Republic
Company Id No: 31 651 470; Tax Id No: 2020497303
tel.: +421 940 428 911; e-mail: info@chempro.sk
www.chempro.sk

(8)

CHEMPRO Poprad

Engineering Solutions

$\gcd(23, 8)$

$23 = 8 \cdot 2 + 7 \Rightarrow 7 = 23 - 8 \cdot 2$

$8 = 7 \cdot 1 + 1 \Rightarrow 1 = 8 - 7 \cdot 1$

$7 = 7 \cdot 1 + 0$

$1 = 8 - 7 \cdot 1 = 8 - 1(23 - 2 \cdot 8) = 8 - 1 \cdot 23 + 2 \cdot 8 = 3 \cdot 8 - 1 \cdot 23$

$\bar{8}^{-1} = 3$

~~$a = 13$.~~

$a = \frac{y_Q - y_P}{x_Q - x_P} \pmod{23}$

$a = (7 - 19) \cdot 3 \pmod{23}$

$a = (-12) \cdot 3 \pmod{23}$

$a = 10 \pmod{23}$

EC - krivka nad $\mathbb{Z}_{23}$

$y_R^2 \equiv x_R^3 + x_R + 1$

$16^2 \equiv 13^3 + 13 + 1$

$3 \equiv 3$

$x_{(R)} = a^2 - x_P - x_Q$

$10^2 - 5 - 13$

$x_{(R)} = 13$

$y_R = a(x_P - x_R) - y_P \pmod{23}$

$10(5 - 13) - 19 \pmod{23}$

$y_R = -99 \pmod{23} = 16 \pmod{23}$

$19P = (13, 16)$

18. 10. 2020

Head Office: Žilinská 1, 811 05 Bratislava, Slovak Republic
Engineering Center Poprad: Hodžova 3292/3, 058 01 Poprad, Slovak Republic
Company Id No: 31 651 470; Tax Id No: 2020497303
tel.: +421 940 428 911; e-mail: info@chempro.sk
www.chempro.sk