NMMB430 - DÚ 2

Jan Oupický

1

We know $xR = 37 \cdot 100 = 3700 \equiv 48 \pmod{83}$. Similarly $yR = 5000 \equiv 20 \pmod{83}$.

1. $xR \cdot yR = 48 \cdot 20 = 960$. Now we apply $B.1$ for $x = 960$. We assume we know that $q = -83^{-1} = 53 \pmod{100}$. Compute $u = 960 \cdot 53 = 50880 \equiv 80 \pmod{100}$. Poté víme, že $y = \frac{80 \cdot 83 + 960}{100} = 76 = xyR \pmod{83}$.

2. As in 1) we know $xR \cdot yR = 960$. Using the notation introduced in the lecture we have $x = 960 = 9 \cdot 10^2 + 6 \cdot 10$ i.e. $x_0 = 0, x_1 = 6, x_2 = 9$. We need to determine $q' = -83^{-1} \pmod{10}$ we can easily see $q' = -3^{-1} = -7 = 3 \pmod{10}$.

   We have to do 2 iterations for $i = 0, 1$. Now $i = 0$:

   $$u = 0 \cdot 3 = 0 \pmod{10}$$
   $$x = 960 + 0$$

   And for $i = 1$:

   $$u = 6 \cdot 3 = 8 \pmod{10}$$
   $$x = 960 + 83 \cdot 8 \cdot 10 = 7600$$

   And now $y = \frac{7600}{100} = 76$ same as in 1).

3. Now we have $x = 4 \cdot 10 + 8$ and $y = 2 \cdot 10 + 0$ i.e. $x_1 = 4, x_0 = 8, y_1 = 2, y_0 = 0$. Set $z = 0$ and for $i = 0$:

   $$u = (0 + 8 \cdot 0)3 = 0 \pmod{10}$$
   $$z = \frac{0 + 8 \cdot 20 + 83 \cdot 0}{10} = \frac{160}{10} = 16$$

   Now $z = 16$ and $i = 1$:

   $$u = (6 + 4 \cdot 0)3 = 8 \pmod{10}$$
   $$z = \frac{16 + 4 \cdot 20 + 83 \cdot 3}{10} = \frac{760}{10} = 76$$

   The result is the same as in the 2 previous cases. We now know $xyR = 37 \cdot 50 \cdot 100 \equiv 76 \pmod{83}$. But we want to calculate $xy \pmod{83}$ so we apply Montgomery reduction on 76 with $R = 100, p = 83$. We will use the same technique as in 1) so let $u = 76 \cdot 53 = 4028 \equiv 28 \pmod{100}$ and $\frac{28 \cdot 83 + 76}{100} = \frac{2400}{100}$ so $xy \pmod{83} = 24$.