CMSC 441: Homework #9 Solutions

Monday, April 21, 2008

Parag Namjoshi

Exercise 1

Use Garner's algorithm to find the unique integer $0 \leq x < 5 \cdot 7 \cdot 11$ that satisfies the following three modular equations:

$$\begin{aligned} x &= 2 \bmod 5 \\ x &= 4 \bmod 7 \\ x &= 3 \bmod 11 \end{aligned}$$

Solution
The mixed radix representation of the unique integer x is of the form

$$x = \nu_0 + \nu_1 \cdot 5 + \nu_2 \cdot 5 \cdot 7$$

Hence, the solution is found by determining the integers ν_0, ν_1, and ν_2 as follows:

$x = 2 \bmod 5 \Longrightarrow x = \nu_0 + \nu_1 \cdot 5 + \nu_2 \cdot 5 \cdot 7 \Longrightarrow \nu_0 = 2 \bmod 5.$
$\therefore x = 2 + \nu_1 \cdot 5 + \nu_2 \cdot 5 \cdot 7$
$x = 4 \bmod 7 \Longrightarrow 2 + \nu_1 \cdot 5 + \nu_2 \cdot 5 \cdot 7 \Longrightarrow= 4 \bmod 7 \Longrightarrow 2 + \nu_1 \cdot 5 = 4 \bmod 7 \Longrightarrow \nu_1 \cdot 5 = 2 \bmod 7.$ But But $5^{-1} \bmod 7 = 3.$ Hence $\nu_1 = 6 \bmod 7$. Consequently,

$$x = 2 + 30 + \nu_2 \cdot 5 \cdot 7$$

$x = 3 \bmod 11 \Longrightarrow 32 + 35\nu_2 \Longrightarrow= 3 \bmod 11 \Longrightarrow 10 + 2\nu_2 = 3 \bmod 11 \Longrightarrow 2\nu_2 = 4 \bmod 11.$ But $2^{-1} \bmod 11 = 6.$ Hence $\nu_2 = 24 \bmod 11$. Consequently, $\nu_2 = 2 \bmod 11$ and

$$x = 2 + 30 + 70 = 102$$

Exercise 2

(Step 1)

Compute $5723 \cdot 7956$ modulo each of the pairwise relatively prime integers $101, 103, 107$, and 109. **Solution**

$$\begin{aligned} 5723 \cdot 7956 \bmod 101 &= 75 \\ 5723 \cdot 7956 \bmod 103 &= 8 \\ 5723 \cdot 7956 \bmod 107 &= 50 \\ 5723 \cdot 7956 \bmod 109 &= 54 \end{aligned}$$

(Step 2)

Then use Garner's algorithm to piece together the above four modular solutions into a unique integer $0 \leq x < 101 \cdot 103 \cdot 107 \cdot 109$.

Exercise 2 [(Step 2)] continued on next page...

$$\begin{aligned} x &= 75 \bmod 101 \\ x &= 8 \bmod 103 \\ x &= 50 \bmod 107 \\ x &= 54 \bmod 109 \end{aligned}$$

Following Garner's algorithm as in the previous exercise, we find that $x = 45532188$.

Under what circumstances does this result mod $101 \cdot 103 \cdot 107 \cdot 109$ produce the same integer which would have been produced if you had instead computed the integer product $5723 \cdot 7956$ in the integers Z, and not in $Z_{101 \cdot 103 \cdot 107 \cdot 109}$?

We get the desired results if the four numbers are prime and $x < 101 \cdot 103 \cdot 107 \cdot 109$.

Suggest some potential applications of this method.

This method has applications in cryptography.