On the Chinese Remainder Theorem

CS 8113e

Winter 1996

Throughout this note, all variables are integers. The integers $m_0, \ldots, m_r$ are assumed to be mutually relatively prime. We define M to be the product of all the m_i's, and for each i, we define M_i to be M/m_i, i.e. the product of all the m_j's such that $j \neq i$. Also, for each i, we define y_i to be the multiplicative inverse of M_i mod m_i, that is, $M_i y_i \stackrel{m_i}{\equiv} 1$. The existence of a multiplicative inverse of M_i mod m_i follows from the fact that M_i and m_i are relatively prime, which follows from the fact that all of the m_i's are relatively prime (this was proved in class).

The Chinese Remainder Theorem defines a bijection between the sets of integers $\mathbb{Z}_M$ and $\mathbb{Z}_{m_0} \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$. The theorem is usually stated as follows:

> The set of congruences
>
> $$\begin{aligned} x &\stackrel{m_0}{\equiv} a_0 \\ x &\stackrel{m_1}{\equiv} a_1 \\ &\cdots \\ x &\stackrel{m_r}{\equiv} a_r \end{aligned}$$
>
> has exactly one solution modulo M, given by
>
> $$x = (\sum_{i=0}^{r} y_i M_i a_i) \bmod M.$$

To understand how this defines a bijection, observe that each $r+1$-tuple $(a_0, a_1, \ldots, a_r)$ is an element of $\mathbb{Z}_{m_0} \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$. Given such an $r+1$-tuple $(a_0, \ldots, a_r)$, the theorem defines $\rho(a_0, \ldots, a_r) = x$, an element of $\mathbb{Z}_M$. The inverse mapping is defined by $\pi(x) = (x \bmod m_0, \ldots, x \bmod m_r)$. Proving the theorem involves showing that (i) x actually maps back to the original $r+1$-tuple, i.e. x is congruent to each a_i mod m_i, and (ii) x is congruent (mod M) to any integer that satisfies the congruences. Part (i) follows immediately from the definition of the M_i's and y_i's, which imply that for each i, the terms $M_j y_j a_j$ are all congruent to 0 mod m_i for any $j \neq i$. Part (ii) follows by assuming that x_0 and x_1 are both solutions of all the congruences, and then observing that $m_i | (x_0 - x_1)$ for each i, and thus $M | (x_0 - x_1)$, i.e. $x_0 \stackrel{M}{\equiv} x_1$, as required.

One of the neat things about the Chinese Remainder Theorem is that it provides a way to manipulate (potentially very large) numbers mod M in terms of tuples of smaller numbers. This can be quite useful when M is 150 digits or more. Let's consider what operations in $\mathbb{Z}_{m_0} \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ correspond to addition and multiplication in $\mathbb{Z}_M$. Suppose we have a number $x \in \mathbb{Z}_M$ that we have represented as the tuple of residues $(a_0, a_1, \ldots, a_r)$, and we want to add n to x. What operation do we perform on $(a_0, a_1, \ldots, a_r)$? Well, we can compute $\pi(n) = (b_0, \ldots, b_r)$, where

$$\begin{aligned} n &\stackrel{m_0}{\equiv} b_0 \\ &\cdots \\ n &\stackrel{m_r}{\equiv} b_r \end{aligned}$$

and then observe that

$$\begin{aligned} x + n &\stackrel{M}{\equiv} (\sum_{i=0}^{r} y_i M_i a_i) + (\sum_{i=0}^{r} y_i M_i b_i) \\ &\stackrel{M}{\equiv} \sum_{i=0}^{r} y_i M_i (a_i + b_i) \end{aligned}$$

Thus the analog of addition in $\mathbb{Z}_M$ for numbers represented as tuples in $\mathbb{Z}_{m_0} \times \cdots \times \mathbb{Z}_{m_r}$ is element-wise addition.

Multiplication of x by p is similarly easy:

$$\begin{aligned} px &\stackrel{M}{\equiv} p(\sum_{i=0}^{r} y_i M_i a_i) \\ &\stackrel{M}{\equiv} \sum_{i=0}^{r} y_i M_i (p a_i) \end{aligned}$$

that is, we multiply each element of the tuple by p and reduce.

An example may help make this clearer. We want to represent 973 mod 1813 as a pair of numbers mod 37 and 49. That is, we define

$$\begin{aligned} m_0 &= 37 \\ m_1 &= 49 \\ M &= 1813 \\ x &= 973 \end{aligned}$$

We also have $M_0 = 49$ and $M_1 = 37$; using the extended Euclid's algorithm, we compute $y_0 = M_0^{-1} = 34$ and $y_1 = M_1^{-1} = 4$. (Note that we only need to compute the M_i's and y_i's once for all.)

Taking residues modulo 37 and 49, our representation of 973 is $(11, 42)$, because 973 mod $37 = 11$ and 973 mod $39 = 42$.

Now suppose we want to add 678 to 973. What do we do to $(11, 42)$? First we compute $\pi(678) = (678 \bmod 37, 678 \bmod 49) = (12, 41)$. Then we add the tuples element-wise and

reduce: $(11 + 12 \bmod 37, 42 + 41 \bmod 49) = (23, 34)$. To verify that this has the correct effect, we compute

$$\begin{aligned} \rho(23, 34) &= M_0 y_0(23) + M_1 y_1(34) \bmod 1813 \\ &= (49)(34)(23) + (37)(4)(34) \bmod 1813 \\ &= 1651. \end{aligned}$$

and check that it is equal to $973 + 678 \bmod 1813 = 1651$.

Suppose we want to multiply 1651 (mod 1813) by 73? We multiply $(23, 34)$ by 73 and reduce, to get $(23 \cdot 73 \bmod 37, 34 \cdot 73 \bmod 49) = (14, 32)$. It is easily verified that

$$\begin{aligned} \rho(14, 32) &= (49)(34)(14) + (37)(4)(32) \bmod 1813 \\ &= 865 \\ &= 1651 \cdot 73 \bmod 1813 \end{aligned}$$

Exercise. Suppose we want to compute x^e? What manipulation do we perform on $(a_0, \ldots, a_r)$?