Solving C Modular Equations in Linear Time

Jack Schumann

10/20/17

For a set of c arithmetic sequences $S = \{A_1, \ldots, A_c\}$ where $A_i = \{x_{io}, \delta_i\}$
The sequences A_i and A_j intersect at x when

$$x \equiv x_{io}\ [\delta_i] \text{ and } x \equiv x_{jo}\ [\delta_j]$$

this occurs when

$$x \equiv x_{io} - \delta_i \tfrac{x_{io} - x_{jo}}{gcd(\delta_i, \delta_j)} u\ [\tfrac{\delta_i \delta_j}{gcd(\delta_i, \delta_j)}]$$

where u is the Bèzout coefficient that is guaranteed to exist by the Bèzout Identity such that

$$\delta_i u + \delta_j v = gcd(\delta_i, \delta_j)$$

Both u and $gcd(\delta_i, \delta_j)$ can be calculated in $O(log(\delta_i) + log(\delta_j))$ time assuming modulus takes constant time using the Extended Euclidean Algorithm.

This result can be seen by writing A_i as

$$x = k\delta_i + x_{io}\ \forall k \in \mathbb{Z}$$

plug into A_j to get

$$\begin{aligned}
k\delta_i &\equiv x_{jo} - x_{io}\ [\delta_j] \\
k\delta_i \frac{u}{gcd(\delta_i, \delta_j)} &\equiv (x_{jo} - x_{io}) \frac{u}{gcd(\delta_i, \delta_j)}\ [\delta_j] \\
k &\equiv (x_{jo} - x_{io}) \frac{u}{gcd(\delta_i, \delta_j)}\ [\delta_j] \\
k &= l\delta_j + (x_{jo} - x_{io}) \frac{u}{gcd(\delta_i, \delta_j)}\ \forall l \in \mathbb{Z} \\
x &= (l\delta_j + (x_{jo} - x_{io}) \frac{u}{gcd(\delta_i, \delta_j)})\delta_i + x_{io} \\
x &\equiv x_{io} - \delta_i \frac{x_{io} - x_{jo}}{gcd(\delta_i, \delta_j)} u\ [\frac{\delta_i \delta_j}{gcd(\delta_i, \delta_j)}]
\end{aligned}$$

Thus, a pair of congruences can be used to represent a pair of arithmetic sequences. This pair of congruences can be reduced to a single congruence in near-constant time that only contains points where the original two congruences intersect. As a result any number of congruences c can be split into many pairs of congruences to be reduced to half as many congruences in $O(\frac{C}{2})$ time.
Therefore, assuming the gcd can be calculated in constant time, the recurrence relation for n congruences is $T(n) = 2T(n/2) + O(1)$ and the total runtime is O(n). The single remaining congruence gives the arithmetic sequence of points where all C arithmetic sequences intersect.