

Chinese Remainder Theorem.

The CRT is a method for solving certain systems of congruencies. The CRT reconstructs integers from their residue values modulo a set of relatively prime moduli. The CRT is a mechanism for manipulating very large numbers in terms of tuples of smaller integers. The CRT can be calculated in 5 steps. Given a set of congruencies such as:

$$\begin{aligned}x &\equiv a_1 \pmod{m_1} \\x &\equiv a_2 \pmod{m_2} \\x &\equiv a_3 \pmod{m_3} \\&\dots \\x &\equiv a_i \pmod{m_i}\end{aligned}$$

1. Calculate $M = m_1 * m_2 * m_3 * \dots, m_i$
2. Calculate $M_1 = M/m_1, M_2 = M/m_2$ and $M_3 = M/m_3, \dots, M_i = M/m_i$
3. Calculate your a's (if necessary)
4. Find the multiplicative inverse for each $M_1, M_2, M_3, \dots, M_i, \pmod{m_1, m_2, m_3, \dots, m_i}$ respectively
5. $\Sigma(A_i * M_i * M_i^{-1}) \pmod{M} = \text{Result}$

Example

Let's say that you want to find the answer to $3^{203} \pmod{5005}$.

(Step 1) We know that $M = 5005$ can be broken down into its prime factors:

$$m_1 = 5, m_2 = 7, m_3 = 11, m_4 = 13$$

(Step 2) In getting the M's we have:

$$\begin{aligned}M_1 &= 1001 = 5005/5 \\M_2 &= 715 = 5005/7 \\M_3 &= 455 = 5005/11 \\M_4 &= 385 = 5005/13\end{aligned}$$

(Step 3) While using Fermat's theorem we can get the following:

$$\begin{aligned}a_1 &= 3^{302} \pmod{5} \equiv 4 \pmod{5} \\a_2 &= 3^{302} \pmod{7} \equiv 2 \pmod{7} \\a_3 &= 3^{302} \pmod{11} \equiv 9 \pmod{11} \\a_4 &= 3^{302} \pmod{13} \equiv 9 \pmod{13}\end{aligned}$$

(Step 4) Now we have to solve for multiplicative inverses using Euclid's Extended Algorithm for each one:

$$\begin{aligned}1001 * M_1^{-1} &\equiv 1 \pmod{5} \rightarrow 1 * M_1^{-1} \equiv 1 \pmod{5} \rightarrow M_1^{-1} = 1 \\715 * M_2^{-1} &\equiv 1 \pmod{7} \rightarrow 1 * M_2^{-1} \equiv 1 \pmod{7} \rightarrow M_2^{-1} = 1 \\455 * M_3^{-1} &\equiv 1 \pmod{11} \rightarrow 4 * M_3^{-1} \equiv 1 \pmod{11} \rightarrow M_3^{-1} = 3 \\385 * M_4^{-1} &\equiv 1 \pmod{13} \rightarrow 8 * M_4^{-1} \equiv 1 \pmod{13} \rightarrow M_4^{-1} = 5\end{aligned}$$

(Step 5) Finally summing everything taken modulo 5005 we have:

$$\begin{aligned} & [(4 * 1001 * 1) + (2 * 715 * 1) + (9 * 435 * 3) + (9 * 385 * 5)] \\ \text{mod } 5005 & \\ & = 35044 \text{ mod } 5005 \\ & = 9 \end{aligned}$$

Thus, $3^{302} \text{ mod } 5005 = 9$. Notice also that 9 is the answer to each of the congruent equations in step 3.

Links

<http://www.swox.com/gmp/>

<http://www.cacr.math.uwaterloo.ca/hac/>

http://www.claymath.org/prizeproblems/p_vs_np.pdf

<http://www.utm.edu/research/primers/ftp/all.txt>

http://documents.wolfram.com/v4/AddOns/NumT_NumberTheoryFunctions-.html

<http://www.utm.edu/research/primers/prove/>

http://directory.google.com/Top/Science/Math/Applications/Communication_Theory/Cryptography

http://directory.google.com/Top/Science/Math/Number_Theory/Computational/

<http://sigact.acm.org/>