Chinese Remainder theorem with non-pairwise coprime moduli

Let $n_1, \ldots, n_k \in \mathbb{N}$ and let $a_1, \ldots, a_k \in \mathbb{Z}$. How to prove the following version of the Chinese remainder theorem (see here):

There exists a $x \in \mathbb{Z}$ satisfying system of equations:

$$\begin{aligned} x &= a_1 \pmod{n_1} \\ x &= a_2 \pmod{n_2} \\ &\cdots \\ x &= a_k \pmod{n_k} \end{aligned}$$

if and only if $a_i = a_j \pmod{\gcd(n_i, n_j)}$ for all $i, j = 1, \ldots, k$.

If numbers n_i, for $i = 1, \ldots, k$, are pairwise coprime, it is a classical version of Chinese remainder theorem.

Thanks.

(abstract-algebra) (number-theory) (arithmetic)

edited Dec 11 '13 at 15:29

asked Mar 14 '12 at 14:17

Richard
1,642 12 30

1 Try $k = 2$ and then induction. – lhf Mar 14 '12 at 14:19

I think your penultimate sentence should talk about n_i being pairwise coprime, not a_i. – Peter Taylor Mar 14 '12 at 16:53

1 Title edit suggestion: *"Proof of a Chinese Remainder Theorem with non-coprime moduli"*. – user2468 Mar 14 '12 at 17:06

Tag suggestion: number-theory – Ory Band Dec 8 '13 at 18:39

1 @Richard - Look up my answer to the (duplicate) question. – chizhek Aug 29 '14 at 10:23

1 Answer

If we factor n_k into primes, $n_k = p_1^{b_1} \cdots p_r^{b_r}$, then the Chinese Remainder Theorem tells us that $x \equiv a_k \pmod{n_k}$ is equivalent to the system of congruences

$$\begin{aligned} x &\equiv a_k \pmod{p_1^{b_1}} \\ x &\equiv a_k \pmod{p_2^{b_2}} \\ &\vdots \\ x &\equiv a_k \pmod{p_r^{b_r}} \end{aligned}$$

Thus, we can replace the given system of congruences with one in which every modulus is a prime power, $n_i = p_i^{b_i}$.

Note that the assumption that $a_i \equiv a_j \pmod{\gcd(n_i, n_j)}$ "goes through" this replacement (if they were congruend modulo $\gcd(n_i, n_j)$, then they are congruent modulo the gcds of the prime powers as well).

So, we may assume without loss of generality that every modulus is a prime power.

I claim that we can deal with each prime separately, again by the Chinese Remainder Theorem. If we can solve all congruences involving the prime p_1 to obtain a solution x_1 (which will be determined modulo the highest power of p_1 that occurs); and all congruences involving the prime p_2 to obtain a solution x_2 (which will be determined modulo the highest power of p_2 that occurs); and so on until we obtain a solution x_n for all congruences involving the prime p_n (determined modulo the highest power of p_n that occurs), then we can obtain a simultaneous solution by solving the usual Chinese Remainder Theorem system

$$\begin{aligned} x &\equiv x_1 \pmod{p_1^{m_1}} \\ &\vdots \\ x &\equiv x_n \pmod{p_n^{m_n}} \end{aligned}$$

(where m_i is the highest power of p_i that occurs as a modulus).

So we are reduced to solving figuring out whether we can solve the system

$$\begin{aligned} x &\equiv a_1 \pmod{p^{b_1}} \\ x &\equiv a_2 \pmod{p^{b_2}} \\ &\vdots \\ x &\equiv a_n \pmod{p^{b_n}} \end{aligned}$$

with, without loss of generality, $b_1 \leq b_2 \leq \cdots \leq b_n$.

When can this be solved? Clearly, this can be solved if and only if $a_i \equiv a_j \pmod{p^{b_{\min(i,j)}}}$: any solution must satisfy this condition, and if this condition is satisfied, then a_n is a solution.

For example: say the original moduli had been $n_1 = 2^3 \times 3 \times 7^2$, $n_2 = 2^2 \times 5 \times 7$, $n_3 = 3^2 \times 5^3$. First we replace the system with the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{2^3} \\ x &\equiv a_2 \pmod{2^2} \\ x &\equiv a_1 \pmod{3} \\ x &\equiv a_3 \pmod{3^2} \\ x &\equiv a_2 \pmod{5} \\ x &\equiv a_3 \pmod{5^3} \\ x &\equiv a_1 \pmod{7^2} \\ x &\equiv a_2 \pmod{7}. \end{aligned}$$

Then we separately solve the systems:

$$\begin{aligned} x_1 &\equiv a_1 \pmod{2^3} \\ x_1 &\equiv a_2 \pmod{2^2} \end{aligned} \qquad \begin{aligned} x_2 &\equiv a_1 \pmod{3} \\ x_2 &\equiv a_3 \pmod{3^2} \end{aligned}$$

$$\begin{aligned} x_3 &\equiv a_2 \pmod{5} \\ x_3 &\equiv a_3 \pmod{5^3} \end{aligned} \qquad \begin{aligned} x_4 &\equiv a_1 \pmod{7^2} \\ x_4 &\equiv a_2 \pmod{7}. \end{aligned}$$

Assuming we can solve these, x_1 is determined modulo 2^3, x_2 modulo 3^2, x_3 modulo 5^3, and x_4 modulo 7^2, so we then solve the system

$$\begin{aligned} x &\equiv x_1 \pmod{2^3} \\ x &\equiv x_2 \pmod{3^2} \\ x &\equiv x_3 \pmod{5^3} \\ x &\equiv x_4 \pmod{7^2} \end{aligned}$$

and obtain a solution to the original system.

Hence, if the condition $a_i \equiv a_j \pmod{\gcd(n_i, n_j)}$ holds in the original system, then we obtain a solution for each prime, and from the solution for each prime we obtain a solution to the original system by applying the usual Chinese Remainder Theorem twice.

edited Mar 14 '12 at 17:17

answered Mar 14 '12 at 16:58

Arturo Magidin
229k 24 516 821

This is written up nicely and I can't seem to find it anywhere else so +1,000 – ttt Aug 20 '13 at 1:08