A Generalization of The Chinese Remainder Theorem

Klaus Crusius

June 28, 2019

Contents

Abstract

It is well known, that the Chinese Remainder Theorem is valid under the condition of mutual co-prime multiple modules. This paper gives a generalization to the case of non-co-prime modules. The constructive proof allows to derive an efficient algorithm, which can be easily parallelized.

1 Theorems and Proofs

It is well known that the following Theorem is valid.

Theorem 1. *Chinese Remainder Theorem*

Given $n \geq 1$ *and a set of mutual co-prime positive integers* m_i *and corresponding remainders* a_i *with* $0 \leq a_i < m_i$ *for* $i = 1, 2, \ldots n$. *Then there exists exactly one* x *with* $0 \leq x < m_1 m_2 \cdots m_n$ *which solves the equations* $x \equiv a_i \mod m_i$ *for all* $i = 1 \cdots n$. *[2, ch. 4.3.2, p. 286]*

This theorem becomes invalid, if we drop the condition of mutual co-primeness. For example there is no solution for $x \equiv 0 \mod 20$; $x \equiv 1 \mod 50$, while for $x \equiv 1 \mod 20$; $x \equiv 11 \mod 50$ we have 10 solutions $\{61, 161, \ldots, 961\}$.

At first, we will proof a necessary condition on the remainders, if a solution is to exist.

Theorem 2. *Necessary condition on remainders*

Let $m_1, m_2, \ldots, m_n$ *be positive and* $x, a_1, a_2, \ldots, a_n$ *be integers, which solve the equations*

$$\forall_{i \in 1 \cdots n}\, x \equiv a_i \mod m_i. \tag{2.1}$$

Then we have

$$\forall_{i,j \in 1 \cdots n}\, a_i \equiv a_j \mod \gcd(m_i, m_j) \tag{2.2}$$

Proof. From (2.1) and because $\gcd(m_i, m_j) \,|\, m_i$ we conclude, that $x \equiv a_i \mod \gcd(m_i, m_j)$ for all i, j. By eliminating x for each pair of i, j the assertion follows immediately. □

We will give a generalization of Theorem 1, which replaces the co-primeness condition on m_i by the necessary condition (2.1). We restrict in a first step to the case $n = 2$ and prove the following:

Theorem 3. *Generalized Chinese Remainder Theorem - two modules*

Let $p, q, a, b \in \mathbb{Z}$ integers with $0 \leq a < p$ and $0 \leq b < q$. If

$$a \equiv b \mod \gcd(p, q), \tag{3.1}$$

then there exists a unique $x \in \mathbb{Z}$ with

$$x \equiv a \mod p \text{ and } x \equiv b \mod q. \tag{3.2}$$

$$0 \leq x < \operatorname{lcm}(p, q) \text{ and} \tag{3.3}$$

The solution is given by formula

$$\begin{gathered} x = a + p \mod \left(u \left(\frac{b-a}{c} \right), \frac{q}{c} \right) \\ \text{with } c = \gcd(p, q) \text{ and } u = \left(\frac{p}{c} \right)^{-1} \mod \frac{q}{c}. \end{gathered} \tag{3.4}$$

Proof. Uniqueness: Assume x and y solve equations (3.2). Then by subtracting we obtain $x \equiv y \mod p$ and $x \equiv y \mod q$. Then $x \equiv y \mod \operatorname{lcm}(p, q)$ by equation (L2) of Lemma 1. Because of (3.3) $x = y$.

Construction of solution: We give a closed formula for an x solving (3.2) and (3.3) under condition (3.1).

Let $c := \gcd(p, q)$. We can write $a = a_2 + ca_1$ and $b = a_2 + cb_1$ with $0 \leq a_2 < c$, because $a \equiv b \mod c$. The equations become $x = a_2 + ca_1 + cp_1 r$ and $x = a_2 + cb_1 + cq_1$. Here $p_1 := p/c$ and $q_1 := q/c$. p_1 and q_1 are co-prime. By introducing a new variable y, substituting

$$x = cy + a_2, \text{ and dividing by } c, \text{ we obtain} \tag{1}$$

$$y = a_1 + p_1 r \text{ and } y = b_1 + q_1 s. \tag{2}$$

Theorem 1 asserts the existence and uniqueness of y with $0 \leq y < p_1 q_1$. We try to calculate y, r, and s.

There is a unique inverse u of p_1 modulo q_1, i.e. $up_1 = 1 + q_1 v$ with $0 \leq u < q_1$, which can be calculated by a the Extended Euclid's algorithm [2, ch. 4.5.2, Theorem X, p.342]. We subtract equations (2) and multiply with u to obtain

$$\begin{aligned} u(b_1 - a_1) &= up_1 r - uq_1 s \\ &= r + q_1 vr - uq_1 s \\ &= r + (vr - us) q_1, \text{ hence} \\ p_1 r &= p_1 [u(b_1 - a_1)] + (us - vr) p_1 q_1, \end{aligned}$$

thus (2) becomes

$$y = a_1 + p_1 \left[u\left(b_1 - a_1\right)\right] + \left(us - vr\right) p_1 q_1.$$

If we perform the calculation of $u\left(b_1 - a_1\right)$ modulo q_1, we get $u\left(b_1 - a_1\right) = \operatorname{mod}\left(u\left(b_1 - a_1\right), q_1\right) + kq_1$ for some k, to obtain finally the solution in terms of y:

$$y = a_1 + p_1 \operatorname{mod}\left(u\left(b_1 - a_1\right), q_1\right) + \left(us - vr + k\right) p_1 q_1.$$

Because $0 \leq a_1 < p_1$ and $0 \leq \operatorname{mod}\left(\cdot, q_1\right) \leq q_1 - 1$, we have

$$0 \leq a_1 + p_1 \operatorname{mod}\left(u\left(b_1 - a_1\right), q_1\right) \leq a_1 + p_1\left(q_1 - 1\right) < p_1 q_1.$$

Therefore

$$y = a_1 + p_1 \operatorname{mod}\left(u\left(b_1 - a_1\right), q_1\right)$$

is the unique solution of (2), with $0 \leq y < p_1 q_1$. Re-substituting x in (1) gives $x = a_2 + ca_1 + p \operatorname{mod}\left(u\left(b_1 - a_1\right), q_1\right)$ and using the original values

$$\begin{gathered} x = a + p \operatorname{mod}\left(u\left(\left(b - a\right)/c\right), q/c\right) \\ \text{with } c = \gcd\left(p, q\right) \text{ and } u = \operatorname{mod}\left(p/c, q/c\right). \end{gathered} \tag{3.4}$$

We claim that x of (3.4) is the unique solution of (3.2) and (3.3). First part of (3.2) is obvious. For the second we have to prove $a + p\left(u\left(b - a\right)/c - kq/c\right) \equiv b \mod q$. That is equivalent to $a - b + p_1 u\left(b - a\right) - p_1 kq \equiv 0 \mod q$. Since $p_1 u = 1 + q_1 v$, that reduces further to $a - b + b - a + q_1 v\left(b - a\right) \equiv 0 \mod q$, or $qv\left(b_1 - a_1\right) \equiv 0 \mod q$, which is valid.

To prove (3.3), we use $0 \leq a < p$ and $0 \leq \operatorname{mod}\left(\cdot, q/c\right) \leq q/c - 1$ to conclude $0 \leq x < p + p\left(q/c - 1\right) = pq/c = \operatorname{lcm}\left(p, q\right)$.

□

We can now formulate the main theorem of this article.

Theorem 4. *Generalized Chinese Remainder Theorem*

Let $m_1, m_2, \ldots, m_n$ be positive and $a_1, a_2, \ldots, a_n$ be integers with $0 \leq a_i < m_i$ satisfying for all $i, j \in \{1 \cdots n\}$ the conditions

$$a_i \equiv a_j \mod \gcd\left(m_i, m_j\right)$$

Then there is exactly one integer x with $0 \leq x < \operatorname{lcm}\left(m_i \mid i \in \{1 \cdots n\}\right)$, which satisfies

$$x \equiv a_i \mod m_i \text{ for } i \in \{1 \cdots n\}\ .$$

Proof.
For the purpose of this proof, we define $\text{lcm}_I := \text{lcm}\left(\{m_i \mid i \in I\}\right)$

The theorem is valid independent of the chosen finite index set. So we can write m_i for $i \in I$ with $|I| < \infty$ without changing the proof.

If $n = 1$ the assertion is trivially true with $x = a_1$.
If $n > 1$ we conduct a proof by induction on n.

Assume, the assertion of the theorem was true for all index sets I with $|I| < n$. Then we can derive the assertion using previous Theorem 3. We split the complete index set into two non-empty subsets $I, J \neq \emptyset$ with $I \cup J = \{1 \cdots n\}$. Because of the induction assumption, for $K \in \{I, J\}$ there is a x_K with

$$0 \le x_K < \text{lcm}_K \text{ and } \forall_{i \in K}\, x_K \equiv a_i \mod m_i. \tag{3}$$

We want to apply Theorem 3 with $a = x_I, b = x_J, p = \text{lcm}_I, q = \text{lcm}_J$. The necessary condition (3.1) reads now

$$x_I \equiv x_J \mod \gcd\left(\text{lcm}_I, \text{lcm}_J\right).$$

Because of (3) $\forall_{i \in I} \forall_{j \in J}\ x_I \equiv a_i \mod \gcd\left(m_i, m_j\right)$ and $x_J \equiv a_j \mod \gcd\left(m_i, m_j\right)$, using conclusion (L1) of Lemma 1.
Hence $\forall_{i \in I} \forall_{j \in J}\ x_I - x_J \equiv a_i - a_j \equiv 0 \mod \gcd\left(m_i, m_j\right)$, which is equivalent by Lemma 1 (L2) to

$$x_I \equiv x_J \mod \text{lcm}\left(\{\gcd\left(m_i, m_j\right) \mid i \in I, j \in J\}\right).$$

Then the necessary condition follows, because of Lemma 1 (L3) and (L1).

Theorem 3 delivers a unique $0 \le x < \text{lcm}\left(\text{lcm}_I, \text{lcm}_J\right)$ with $x \equiv x_I \mod \text{lcm}_I \wedge x \equiv x_J \mod \text{lcm}_J$. Because of Lemma 1 (L1) and $m_i \mid \text{lcm}_I$ we have $\forall_{i \in I}\ x \equiv x_I \mod m_i$. So $x \equiv a_i \mod m_i$ because of (3). The same is true $\forall_{i \in J}$.

□

The proofs need some auxiliary facts from elementary number theory, which are noted in the following:

Lemma 1. *In all statements below let*

$$x, y, a, u \in \mathbb{Z}, I, J \textit{ finite index sets, and } \forall_{i \in I \cup J}\, m_i \in \mathbb{N}$$
$$\text{lcm}_I := \text{lcm}\left(\{m_i \mid i \in I\}\right)$$

then

$$x \equiv y \mod u \implies \forall_{a\,|\,u}\, x \equiv y \mod a \tag{L1}$$

$$\forall_{i \in I}\, x \equiv y \mod m_i \iff x \equiv y \mod \mathrm{lcm}_I \tag{L2}$$

$$\mathrm{lcm}\left(\mathrm{lcm}_I, \mathrm{lcm}_j\right) = \mathrm{lcm}_{I \cup J} \tag{L3}$$

$$\gcd\left(\mathrm{lcm}_I, \mathrm{lcm}_J\right) \text{ divides } \mathrm{lcm}\left(\{\gcd\left(m_i, m_j\right) \mid i \in I, j \in J\}\right) \tag{L4}$$

Proof.
(L1): If $u = ka$ and $x = y + vu$ for some $k, v \in \mathbb{Z}$, then $x = y + (vk)\,a$, hence $x \equiv y \mod a$.

(L2): $\Longleftarrow$ is clear because $\forall_{i \in I}\, m_i \,|\, \mathrm{lcm}_I$ and (L1).

$\Longrightarrow$: To see that we assume $x - y = k \mod \mathrm{lcm}_I$ with $0 \leq k < \mathrm{lcm}_I$ and show, that $k = 0$. Because $\forall_i m_i \,|\, \mathrm{lcm}_I$, we have $x - y = k + \mathrm{lcm}_I\, u = k + m_i u_i$ for some u, u_i. Because $\forall_i\; x – y \equiv 0 \mod m_i$, $\exists_{v_i}\, x - y = m_i v_i$, hence $k = m_i\left(v_i - u_i\right)$. That means k is a multiple of all m_i, hence of lcm_I, by the definition of lcm. The only k with $0 \leq k < \mathrm{lcm}_I$ is $k = 0$.

(L3)"$\geq$": because $\mathrm{lcm}\left(\mathrm{lcm}_I, \mathrm{lcm}_J\right) = \mathrm{lcm}_I\, k_I$ and $lcm_I = m_i k_{iI}$ for some $k_I, k_{iI} \forall_{i \in I}$, we have $\mathrm{lcm}\left(\mathrm{lcm}_I, \mathrm{lcm}_J\right) = m_i k_I k_i I$, that means the left-hand side is a multiple of $m_i \forall_{i \in I}$. Accordingly, it is a multiple of $m_j \forall_{j \in J}$. Then, by definition of lcm it is $\geq \mathrm{lcm}_{I \cup J}$.

"$\leq$": $\mathrm{lcm}_{I \cup J}$ is a multiple of $m_i \forall_{i \in I}$, hence of lcm_I by definition of lcm_I; accordingly also of lcm_J. Then it is also a multiple of $\mathrm{lcm}\left(lcm_I, lcm_J\right)$. So the right-hand side is $\geq$ the left-hand side.

(L4): We make use of the Fundamental Theorem of Arithmetic [1, chapter 1.2.4, exercise 21], which proves the unique prime-factorization of the natural numbers. For each number $n \in \mathbb{N}$ and each prime number p there is a unique exponent $u_p\left(n\right) \in \mathbb{N} \cup \{0\}$, such that

$$n = \prod_{p \text{ prime}} p^{u_p(n)}.$$

where only a finite amount of the $u_p\left(n\right) \neq 0$. Then we have

$$\gcd\left(m, n\right) = \prod_{p \text{ prime}} p^{\min\left(u_p(m), u_p(n)\right)}$$

$$\mathrm{lcm}\left(m, n\right) = \prod_{p \text{ prime}} p^{\max\left(u_p(m), u_p(n)\right)}$$

or for each prime p

$$
\begin{aligned}
m \mid n &\iff \forall_p \, u_p(m) \leq u_p(n) \\
u_p(\gcd(m,n)) &= \min(u_p(m), u_p(n)) \\
u_p(\operatorname{lcm}(m,n)) &= \max(u_p(m), u_p(n))
\end{aligned}
$$

Then (L4) (we set $u_{pi} := u_p(m_i)$) is equivalent to

$$
\begin{aligned}
&\forall_p \min\left(\max\left(\{u_{pi} \mid i \in I\}\right), \max\left(\{u_{pj} \mid j \in J\}\right)\right) \\
&\leq \max\left(\{\min(u_{pi}, u_{pj}) \mid i \in I, j \in J\}\right)
\end{aligned} \tag{4}
$$

There is an $i_{max} \in I$ with $u_{pi_{max}} = \max(\{u_{pi} \mid i \in I\})$; as well as an $j_{max} \in J$. Inserting these into the left-hand side of (4) gives

$$
\min\left(u_{pi_{max}}, u_{pj_{max}}\right) \leq \max\left(\{\min(u_{pi}, u_{pj}) \mid i \in I, j \in J\}\right)
$$

which is obviously true for all prime numbers p. □

2 Algorithms

From Theorem 3 we can straightforward derive the following procedure:

Algorithm 1.
procedure crt2(a, b, p, q)
Input: a, b, p, q: integers p, q > 0
Output: x, lcm: solution, least common multiple of p and q
Errors: fail if $a \neq b \mod \gcd(p,q)$
External: gcdx: calculate greatest common divisor
and inverse of co-prime pair

$$
\begin{aligned}
&c, u := gcdx(p, q) \\
&p_1, q_1 := p/c, q/c \\
&u := \operatorname{mod}(u, q_1) \\
&if\ mod(b-a, c) \neq 0\ Error(\text{"}remainders'condition\text{"}) \\
&bac := (b-a)/c \\
&x := a + p * mod(u * bac, q_1) \\
&lcm := p * q_1 \\
&return\ x, lcm
\end{aligned}
$$

Theorem 4 provides some freedom in partitioning the original set. If $n = 1$ we return the trivial solution or we apply Algorithm 1. Otherwise, we split $\{1 \cdots n\}$ two partitions and apply Theorem 4.

Algorithm 2.
procedure crtg(a, m)
Input: a, m: integer vectors of same lengths, m > 0
Output: x, lcm: solution, least common multiple of m
Errors: fail if $a_i \neq a_j \mod \gcd(m_i, m_j)$ *for any* $i,\ j$
External: crt2: see above

$$
\begin{aligned}
& n := length(a) \\
& x_I, lcm_I := 1,\ 1 \\
& for\ i := 1 \ldots n \\
& \quad x_I, lcm_I := crt2(x_I, a[i], lcm_I, m[i]) \\
& end \\
& return\ x_I, lcm_I
\end{aligned}
$$

References

[1] Donald E. Knuth, *The Art of Computer Programming - Volume 1* Addison-Wesley, New York, 3rd edition, 1998.

[2] Donald E. Knuth, *The Art of Computer Programming - Volume 2* Addison-Wesley, New York, 3rd edition, 1998.