

## The Chinese Remainder Theorem

Jonathan L.F. King

University of Florida, Gainesville FL 32611-2082, USA  
squash@ufl.edu

Webpage <http://squash.1gainesville.com/>

18 July, 2018 (at 10:49)

**Morphisms.** Consider a ring  $R = (R, +, 0, \cdot, 1)$ , and another ring,  $\Gamma = (\Gamma, +, 0, \cdot, 1)$ . A map  $h: R \rightarrow \Gamma$  is a **ring-homomorphism** if:

i: The maps sends the mult-identity in  $R$  to the mult-identity in  $\Gamma$ , i.e  $h(1) = 1$ .

ii: For each  $x, y \in R$  we have  $h(x) + h(y) = h(x + y)$ .

iii: For each  $x, y \in R$  we have  $h(x) \cdot h(y) = h(x \cdot y)$ .

These imply that  $h(0) = 0$ , that  $h(-x) = -h(x)$ , and for each  $x$  with a reciprocal, that  $h(x^{-1}) = [h(x)]^{-1}$ .

Our  $h: R \rightarrow \Gamma$  is a **ring-isomorphism** if:

1:  $h$  is a bijection,  $h$  is a ring-hom, and the inverse-map  $h^{-1}$  is a ring-hom.

It turns out that  $h$  being a bijective ring-hom automatically insures that  $h^{-1}$  is a ring-homomorphism, so this last condition never needs to be checked.

**2: Lemma.** *A cartesian product of rings is a ring.*

*Proof.* Exer. N.B. The product-ring will have ZDs.  $\diamond$

**3: Standing Notation.** With  $L \in \mathbb{Z}_+$  (but the  $L=1$  case is trivial), let  $\mathbb{L} := [1 .. L]$ . A tuple  $\vec{M} = (M_1, \dots, M_L)$  of positive integers is a **coprime tuple** if

3a:  $\text{Gcd}(\vec{M}) \stackrel{\text{notation}}{=} \text{Gcd}(M_1, \dots, M_L) = 1$ ,

and is **pairwise-coprime** if

3b: For all indices  $j < k$  in  $\mathbb{L}$ :  $M_j \perp M_k$ .

With  $U := \prod_{j=1}^L M_j$  the prodUct of the moduli, define the **Reduced product**

3c:  $R_k := U/M_k$ , for each  $k \in \mathbb{L}$ .

As a shorthand, let  $\Omega_j$  mean the ring  $\mathbb{Z}_{M_j}$ , and let

3d:  $\Gamma := \Omega_1 \times \Omega_2 \times \Omega_3 \times \dots \times \Omega_L$ ,

be the cartesian-product ring. Let  $\vec{1} = (1, \dots, 1)$  and  $\vec{0} = (0, \dots, 0)$  denote the multiplicative and additive identity-elements in  $\Gamma$ .  $\square$

**4: Proposition.** *With notation from (3):*

*The reduced-product tuple  $\vec{R}$  is a coprime tuple IFF  $\vec{M}$  is pairwise-coprime.*  $\diamond$

*Pf of ( $\Rightarrow$ ).* FTSSOContradiction, suppose there are indices  $\mathbf{j} < \mathbf{k}$  in  $\mathbb{L}$  and a prime  $p$  dividing  $M_j$  and  $M_k$ . [This forces that  $L \geq 2$ .] Since  $p \bullet M_j$ :

For each  $i \in \mathbb{L} \setminus \{\mathbf{j}\}$ , our  $p$  divides  $R_i$ .

Similarly,  $p \bullet R_i$  for each  $i \in \mathbb{L} \setminus \{\mathbf{k}\}$ . But the union of  $\mathbb{L} \setminus \{\mathbf{j}\}$  with  $\mathbb{L} \setminus \{\mathbf{k}\}$  is all of  $\mathbb{L}$ . This produces the contradiction that  $p$  divides  $\text{Gcd}(\vec{R})$ .  $\blacklozenge$

*Pf of ( $\Leftarrow$ ).* FTSSOC, suppose a prime  $q$  divides each of  $R_1, \dots, R_L$ . So  $q$  divides  $R_1 \stackrel{\text{note}}{=} M_2 \cdot M_3 \cdot \dots \cdot M_L$  [which forces  $L \geq 2$ ]. Consequently  $\exists \mathbf{k} \in [2 .. L]$  such that  $q$  divides  $M_k$ . For each  $i \in \mathbb{L} \setminus \{\mathbf{k}\}$ , then,  $q$  cannot divide  $M_i$ . Hence  $q$  does not divide the product of such  $M_i$ . But their product is  $R_k$ , contradicting that  $q$  divides each reduced-product.  $\blacklozenge$

**5: Lemma.** [Using (3).] *For an arbitrary  $\vec{M}$  (i.e, no coprimeness requirement), the map  $h: \mathbb{Z}_U \rightarrow \Gamma$  defined by*

$$h(x) := \left( \langle x \rangle_{M_1}, \langle x \rangle_{M_2}, \dots, \langle x \rangle_{M_L} \right)$$

*is a ring-homomorphism. Moreover,  $h$  is the only ring-homomorphism from  $\mathbb{Z}_U$  to  $\Gamma$ .*  $\diamond$

*Pf.* Our  $h$  is a ring-hom simply because each  $M_j \bullet U$ .

To show uniqueness, letting italic  $1$  denote the unit in  $\mathbb{Z}_U$ , note that  $h(1)$  must be  $\vec{1} \in \Gamma$ . And each element  $n \in \mathbb{Z}_U$  is the sum of  $n$  many copies of  $1$ ; hence  $h(n) = h(1) + \dots + h(1)$ .  $\blacklozenge$

**6: Lemma.** [Using (3).] *Suppose  $\vec{M}$  is not pairwise-coprime. Then [not only do rings  $\mathbb{Z}_U$  and  $\Gamma$  fail to be ring-isomorphic] the additive groups  $(\mathbb{Z}_U, +, 0)$  and  $(\Gamma, +, \vec{0})$  are not group-isomorphic, because the latter group is not cyclic.*  $\diamond$

**Proof.** Let  $\ell := \text{Lcm}(\vec{M})$ . Pairwise-coprimeness of  $\vec{M}$  is equivalent to  $\ell = U$ ; hence our  $\ell$  is a *proper* divisor of  $U$ . Each element  $\vec{\alpha} \in \Gamma$  has that

$$\vec{\alpha} + \vec{\alpha} + \vec{\alpha} + \dots + \vec{\alpha} = \vec{0}.$$

But  $|\Gamma| = U \stackrel{\text{note}}{>} \ell$ , so no element of  $(\Gamma, +, \vec{0})$  can generate  $\Gamma$ .  $\blacklozenge$

**7: Chinese Remainder Thm (CRT).** [Using (3).] *Product-ring  $\Gamma$  is ring-isomorphic to  $\mathbb{Z}_U$  IFF  $\vec{M}$  is pairwise-coprime. In that case, the ring-isomorphism  $g: \Gamma \hookrightarrow \mathbb{Z}_U$  is unique. It has form*

$$7a: \quad g(\vec{\alpha}) \equiv_U \sum_{j \in \mathbb{L}} G_j \alpha_j, \quad \text{for } \vec{\alpha} \in \Gamma.$$

Here, the “**maGic tuple**”  $\vec{G} = (G_1, \dots, G_L)$  of integers is unique modulo- $U$ . The inverse ring-isomorphism,  $h := g^{-1}$ , maps  $\mathbb{Z}_U \rightarrow \Gamma$ . It is

$$7b: \quad h(x) := (\langle x \rangle_{M_1}, \langle x \rangle_{M_2}, \dots, \langle x \rangle_{M_L}). \quad \blacklozenge$$

**Proof.** Lemmas (5) and (6) have proven most of CRT. Assuming that  $\vec{M}$  is pairwise-coprime, we need but produce a magic tuple  $\vec{G}$  so that (7a) is a ring-iso.

By (4), our  $\vec{R}$  is coprime, so there exists a Bézout tuple  $(\mu_1, \dots, \mu_L)$  such that

$$7c: \quad 1 = \sum_{j \in \mathbb{L}} R_j \mu_j. \quad \text{Define } G_j := R_j \mu_j.$$

Since  $M_1$  divides each of  $R_2, \dots, R_L$ , reducing (7c) mod- $M_1$  gives

$$1 = \sum_{j \in \mathbb{L}} G_j \equiv_{M_1} G_1.$$

We get the defining property of  $\vec{G}$ , that

$$7d: \quad \forall j, k \in \mathbb{L}: \quad G_j \equiv_{M_k} \begin{cases} 1 & \text{if } j = k \\ 0 & \text{otherwise} \end{cases}.$$

**Bijection.** For an  $x \in \mathbb{Z}_U$ , note  $g(h(x))$  is mod- $U$  congruent to

$$\sum_{j \in \mathbb{L}} G_j \cdot \langle x \rangle_{M_j}.$$

Reducing this mod- $M_1$  says, courtesy (7d), that

$$g(h(x)) \equiv_{M_1} G_1 \cdot x \equiv_{M_1} x.$$

Similarly,  $g(h(x)) \equiv_{M_k} x$ , for each  $k$ . IOWords,  $g \circ h$  is the identity-map on  $\mathbb{Z}_U$ . And since  $\mathbb{Z}_U$  and  $\Gamma$  have the same cardinality –which is finite– the Pigeon-hole principle says that  $h$  is a bijection. Hence  $g$  is the fnc-inverse of a ring-iso, so  $g$  itself a ring-iso.  $\blacklozenge$

**Alternative magic algorithm.** The phrase is:

*R times  $[\frac{1}{R} \text{ mod-} M]$  . . . is Magic!*

That is, for each  $j \in \mathbb{L}$ , define

$$7e: \quad G_j := R_j \cdot \langle 1/R_j \rangle_{M_j},$$

and, if desired, reduce modulo- $U$ .

**Comparing Iterative vs. Parallel.** We call (7c) the “Iterative” algorithm, since we feed the output of one LBolt into the next LBolt; see my *Algorithms in Number Theory* pamphlet. Call (7e) the “Parallel” algorithm.

ITERATIVE does  $L-1$  many LBolts, each using *both* multiplier columns. PARALLEL does  $L$  many LBolts, but each uses just *one* multiplier column.

ITERATIVE runs iteratively (at least, if implemented naively). PARALLEL can be run in parallel on  $L$  many processors. To compute a *particular*  $G_k$ , our ITERATIVE needs to compute all  $L-1$  many 2-multiplier LBolts. In contrast, PARALLEL needs but a single 1-multiplier LBolt.

The initial LBolts of ITERATIVE use large numbers,<sup>♥1</sup> e.g  $R_1$  and  $R_2$ . PARALLEL does LBolts with one number large and the other small, e.g  $R_1$  and  $M_1$ .

Both algorithms produce a  $\vec{G}$  satisfying (7d); in particular,  $\sum_{j \in \mathbb{L}} G_j$  is mod- $U$  congruent to 1. But ITERATIVE arranges that the sum actually *equals* 1 (if you had some need for that).

<sup>♥1</sup>However, we can make the numbers small at the expense of making ITERATIVE more complicated. E.g, pull out the common factor  $\prod_{i=3}^L M_i$  before computing  $\text{LBolt}(R_1, R_2)$ .

8: Corollary. Euler  $\varphi$  is a multiplicative function.  $\diamond$

*Proof.* For posints  $K$  and  $N$ , the units group in ring  $\mathbb{Z}_K \times \mathbb{Z}_N$  is simply the cartesian product of the units groups;  $\Phi(K) \times \Phi(N)$ . And when  $K \perp N$ , then  $\mathbb{Z}_K \times \mathbb{Z}_N$  is ring-isomorphic to  $\mathbb{Z}_{KN}$ , whose units group is  $\Phi(KN)$ . Now take cardinalities.  $\blacklozenge$

### Fusing congruences

For a modulus  $M > 0$  and “target”  $T \in \mathbb{Z}$ , consider the set of integers  $x$  satisfying

$$x \equiv_M T.$$

Its soln set is  $T + M\mathbb{Z}$ . This is a (*bi-infinite*) *arithmetic progression*, which I also call a *comb*. Abbreviate the congruence by  $(M; T)$ .

Given combs  $T_1 + M_1\mathbb{Z}$  and  $T_2 + M_2\mathbb{Z}$ , either they have empty intersection, or:

*Their intersection is a comb  $\tau + \mu\mathbb{Z}$ , where  $\mu := \text{Lcm}(M_1, M_2)$ , and  $\tau$  is some integer.*

[Of course, to  $\tau$  we can add any multiple of  $\mu$  without changing the comb.] The operation of computing a value for  $\tau$ , I call

\*: *the fusing of congruences  $(M_1; T_1)$  and  $(M_2; T_2)$ , producing  $(\mu; \tau)$ .*

An  $x$  satisfies the two congruences IFF  $\exists \alpha_1, \alpha_2$  integers st.

$$\begin{aligned} x + \alpha_1 M_1 &= T_1 \quad \text{and} \\ x + \alpha_2 M_2 &= T_2. \quad \text{Subtracting,} \end{aligned}$$

$$\dagger: \quad \alpha_1 M_1 - \alpha_2 M_2 = T_1 - T_2.$$

The of linear-combinations of  $M_1, M_2$  are the multiples of  $D := \text{Gcd}(M_1, M_2)$ . So if  $D \nmid [T_1 - T_2]$  then there is no soln; else set  $R := [T_1 - T_2]/D$ .

A Bézout pair  $(\beta_1, -\beta_2)$  [note the negation] satisfies  $\beta_1 M_1 - \beta_2 M_2 = D$ . To see that  $\boxed{\alpha_j := R\beta_j}$  satisfies  $(\dagger)$ , note

$$\begin{aligned} \text{LhS}(\dagger) &= R\beta_1 \cdot M_1 - R\beta_2 \cdot M_2 = R \cdot [\beta_1 M_1 - \beta_2 M_2] \\ &= R \cdot D \stackrel{\text{note}}{=} \text{RhS}(\dagger). \end{aligned}$$

Solving for  $x$  in either of the two lines above  $(\dagger)$ , gives

$$\ddagger: \quad x = T_1 - R\beta_1 M_1 \stackrel{\text{note}}{=} T_2 - R\beta_2 M_2,$$

just like the doctor ordered.

**Fusion algorithm.** Given congruences  $(M_1; T_1)$  and  $(M_2; T_2)$ , we compute  $(*)$  as follows.

F1: Compute  $D := \text{Gcd}(M_1, M_2)$ , and store the quotient-column of LBolt. If  $D \nmid [T_1 - T_2]$ , then report “Failure”.

Else, set  $R := [T_1 - T_2]/D$ .

F2: [Use the stored quotient-col to] Compute the  $\beta_1$  of a  $\beta_1, \beta_2$  pair that satisfies  $\beta_1 M_1 - \beta_2 M_2 = D$ .

Let  $\tau' := T_1 - R\beta_1 M_1$  [or  $T_2 - R\beta_2 M_2$ ].

F3: Reduce  $\tau := \langle \tau' \rangle_\mu$ , where  $\mu := \text{Lcm}(M_1, M_2)$ .

The *fusing congruences* pamphlet [on TEACHING PAGE] has several worked examples, and our NT Archive has several more.

**CRT example takehome problem**

Magic integers  $G_1 = \dots$ ,  $G_2 = \dots$ ,  
 $G_3 = \dots$ ,  $G_4 = \dots$ , each in  $[0..1260)$ ,  
 are st.  $g: \mathbb{Z}_7 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \rightarrow \mathbb{Z}_{1260}$  is a ring-iso,  
 where

$$g((z_1, z_2, z_3, z_4)) := \langle z_1 G_1 + z_2 G_2 + z_3 G_3 + z_4 G_4 \rangle_{1260}.$$

Consider poly  $h(x) := [x + 59][x - 1][x + 83]$ .  
 Find all solutions to congruences  $h(x) \equiv_M 0$ , for  
 $M = 7, 4, 9, 5$ , displaying the *results* in a nice ta-  
 ble. (Do **not** show work for this step.)

Now use your ring-iso to compute *all* solns  $x$   
 to  $\overline{h(x) \equiv_{1260} 0}$ , displaying the results in a table  
 which shows *which* 4tup each came from. There  
 are (not counting multiplicities)  $K := \dots$  many solns.

Explain your method well; then show **one**  
 computation giving a root *different* (mod 1260)  
 from  $-59, 1, -83$ .

Filename: chinese-rt4.H.tex  
 As of: Wednesday 06Feb2013. Typeset: 18Jul2018 at 10:49.