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 March, 2017 (at *14:50*)

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

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

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

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

2a: $$\operatorname{Gcd}(\vec{\mathbf{M}}) \overset{\text{notation}}{=\!=} \operatorname{Gcd}(M_1, \dots, M_L) = 1,$$

and is ***pairwise-coprime*** if

2b: *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***

2c: $$R_k := U / M_k, \quad \text{for each } k \in \mathbb{L}.$$

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

2d: $$\mathbf{\Gamma} := \Omega_1 \times \Omega_2 \times \Omega_3 \times \ldots \times \Omega_L,$$

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

3: Proposition. *With notation from (2):*

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

Pf of (⇒). FTSOContradiction, suppose there are indices $\mathbf{j} < \mathbf{k}$ in $\mathbb{L}$ and a prime p dividing $M_{\mathbf{j}}$ and $M_{\mathbf{k}}$. [This forces that $L \geqslant 2$.] Since $p \bullet\!| \, M_{\mathbf{j}}$:

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

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

Pf of (⇐). FTSOC, suppose a prime q divides each of $R_1, \dots, R_L$. So q divides $R_1 \overset{\text{note}}{=\!=} M_2 \cdot M_3 \cdots M_L$ [which forces $L \geqslant 2$]. Consequently $\exists \mathbf{k} \in [2 .. L]$ such that q divides $M_{\mathbf{k}}$. For each $i \in \mathbb{L} \smallsetminus \{\mathbf{k}\}$, then, q *cannot* divide M_i. Hence q does not divide the product of such M_i. But their product is $R_{\mathbf{k}}$, contradicting that q divides each reduced-product. ♦

4: Lemma. [*Using* (2).] *For an arbitrary $\vec{\mathbf{M}}$ (i.e, no coprimeness requirement), the map $h: \mathbb{Z}_U \to \mathbf{\Gamma}$ 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 <u>only</u> ring-homomorphism from $\mathbb{Z}_U$ to $\mathbf{\Gamma}$. ♢

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

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

5: Lemma. [*Using* (2).] *Suppose $\vec{\mathbf{M}}$ is <u>not</u> pairwise-coprime. Then [not only do rings $\mathbb{Z}_U$ and $\mathbf{\Gamma}$ fail to be ring-isomorphic] the additive groups $(\mathbb{Z}_U, +, 0)$ and $(\mathbf{\Gamma}, +, \vec{\mathbf{0}})$ are not group-isomorphic, because the latter group is not cyclic.* ♢

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

$$\vec{\boldsymbol{\alpha}} + \vec{\boldsymbol{\alpha}} + \vec{\boldsymbol{\alpha}} + \overset{\ell}{\ldots} + \vec{\boldsymbol{\alpha}} \quad = \quad \vec{\mathbf{0}}\,.$$

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

6: Chinese Remainder Thm (CRT). [*Using* (2).] *Product-ring* $\boldsymbol{\Gamma}$ *is ring-isomorphic to* $\mathbb{Z}_U$ *IFF* $\vec{\mathbf{M}}$ *is pairwise-coprime. In that case, the ring-isomorphism* $g\colon \boldsymbol{\Gamma} \hookrightarrow\!\!\!\!\to \mathbb{Z}_U$ *is unique. It has form*

6a: $$g(\vec{\boldsymbol{\alpha}}) \equiv_U \sum_{j \in \mathbb{L}} G_j \alpha_j\,, \quad \textit{for } \vec{\boldsymbol{\alpha}} \in \boldsymbol{\Gamma}.$$

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

6b: $$h(x) \quad := \quad \Big(\langle x \rangle_{M_1}, \langle x \rangle_{M_2}, \ldots, \langle x \rangle_{M_L}\Big)\,.$$ ♢

Proof. Lemmas (4) and (5) have proven most of CRT. Assuming that $\vec{\mathbf{M}}$ is pairwise-coprime, we need but produce a magic tuple $\vec{\mathbf{G}}$ so that (6a) is a ring-iso.

By (3), our $\vec{\mathbf{R}}$ is coprime, so there exists a Bézout tuple $(\mu_1, \ldots, \mu_L)$ such that

6c: $$1 \;=\; \sum_{j \in \mathbb{L}} R_j \mu_j\,. \quad \text{Define } G_j \;:=\; R_j \mu_j\,.$$

Since M_1 divides each of $R_2, \ldots, R_L$, reducing (6c) mod-M_1 gives

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

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

6d: $$\forall j,k \in \mathbb{L}\colon \quad G_j \;\equiv_{M_k}\; \begin{Bmatrix} 1 & \text{if } j = k \\ 0 & \text{otherwise} \end{Bmatrix}.$$

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 (6d), 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 $\boldsymbol{\Gamma}$ 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. ♦

Alternative magic algorithm. The phrase is:

$$R \textit{ times } [\tfrac{1}{R} \text{ mod-}M] \ldots \textit{is Magic!}$$

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

6e: $$G_j \quad := \quad R_j \cdot \langle 1/R_j \rangle_{M_j}\,,$$

and, if desired, reduce modulo-U.

Comparing Iterative vs. Parallel. We call (6c) the "Iterative" algorithm, since we feed the output of one LBolt into the next LBolt; see my *Algorithms in Number Theory* pamphlet. Call (6e) 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,[♡1] 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 $\vec{\mathbf{G}}$ satisfying (6d); 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).

[♡1] 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 $\text{LBolt}(R_1, R_2)$.

7: Corollary. *Euler φ is a multiplicative function.* ♢

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. ♦

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 $\mu := \operatorname{Lcm}(M_1, M_2)$, and τ is some integer.*

[Of course, to τ we can add any multiple of μ without changing the comb.] The operation of computing a value for τ, 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.

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

$$\dagger\text{:} \qquad \alpha_1 M_1 - \alpha_2 M_2 = T_1 - T_2\,.$$

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

A Bézout pair $(\beta_1, \text{-}\beta_2)$ [note the negation] satisfies $\beta_1 M_1 - \beta_2 M_2 = D$. Then $\alpha_j := R\beta_j$ gives (†). So

$$\ddagger\text{:} \qquad x = T_1 - \alpha_1 M_1 \overset{\text{note}}{=\!=} T_2 - \alpha_2 M_2\,,$$

just like the doctor ordered.

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

F1: Compute $D := \operatorname{Gcd}(M_1, M_2)$, and store the quotients. If $D \nmid [T_1 - T_2]$, then report "*Failure*". Else, set $R := [T_1 - T_2]/D$.

F2: [Use your stored quotients to] Compute the β_1 of a β_1,β_2 pair that satisfies $\beta_1 M_1 - \beta_2 M_2 = D$. Let τ' be $T_1 - R\beta_1 M_1$.

F3: You can let τ be τ', or you can reduce it by setting $\tau := \langle\tau'\rangle_\mu$, where $\mu := \operatorname{Lcm}(M_1, M_2)$.

The *fusing congruences* pamphlet has several worked examples, and our NT Archive has several more.

Worked CRT Example

Magic integers $G_1 = \underline{\hspace{3cm}}$, $G_2 = \underline{\hspace{3cm}}$, $G_3 = \underline{\hspace{2.5cm}}$, $G_4 = \underline{\hspace{2.5cm}}$, each in $[0 \,..\, 1260)$, are st. $g\colon \mathbb{Z}_7 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \to \mathbb{Z}_{1260}$ is a ring-iso, where

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

Now 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 table. (Do **not** show work for this step.)

Now use your ring-iso to compute *all* solns x to $\boxed{h(x) \equiv_{1260} 0}$, displaying the results in a table which shows *which* 4tup each came from. There are (<u>not</u> counting multiplicities) $K := \underline{\hspace{1cm}}$ many solns. Explain your method well; then show <u>**one**</u> computation giving a root *different* (mod 1260) from -59, 1, -83.

Filename: `chinese-rt4.H.tex`
As of: *Wednesday 06Feb2013.* Typeset: *18Mar2017* at *14:50.*