The Chinese Remainder Theorem

R. C. Daileda

February 19, 2018

1 The Chinese Remainder Theorem

We begin with an example.

Example 1. Consider the system of simultaneous congruences

$$\begin{aligned} x &\equiv 3 \pmod 5, \\ x &\equiv 2 \pmod 6. \end{aligned} \tag{1}$$

Clearly $x = 8$ is a solution. If y were another solution, then we would have $y \equiv 8 \pmod 5$ and $y \equiv 8 \pmod 6$. Hence $5|y-8$ and $6|y-8$. As $(5,6) = 1$, this means $30|y-8$ or $y \equiv 8 \pmod{30}$. As this line of reasoning is completely reversible, we find that the set of solutions to the simultaneous congruences (1) is the congruence class $8 + 30\mathbb{Z}$. Hence, modulo 30, there is a unique solution to the system (1). ♦

The *Chinese remainder theorem* tells us that, under an appropriate hypothesis on the moduli, systems of the type in the previous example always have solutions that are unique modulo the product of the moduli. Before we state it, however, we need to generalize a result from the homework.

Lemma 1. *Let $a_1, a_2, \dots, a_n \in \mathbb{Z}$ be pairwise relatively prime. If $b \in \mathbb{Z}$ and $a_i|b$ for all i, then $a_1 a_2 \cdots a_n | b$.*

Proof. By induction on n. We take as our base case $n = 2$. Although this case was given as a homework exercise, in the interest of completeness we prove it here anyway. So suppose a_1 and a_2 are relatively prime and both divide b. Use Bézout's lemma to write $ra_1 + sa_2 = 1$ for some $r, s \in \mathbb{Z}$. Also write $b = b_1 a_1$ and $b = b_2 a_2$. We multiply the Bézout relation by b and then substitute in the divisibility equations:

$$b = bra_1 + bsa_2 = b_2 a_2 ra_1 + b_1 a_1 sa_2 = (b_2 r + b_1 s) a_1 a_2$$

which implies that $a_1 a_2 | b$.

Now assume that the result holds for some $n \geq 2$. Let $a_1, a_2, \dots a_n, a_{n+1} \in \mathbb{Z}$ be pairwise relatively prime and suppose that $a_i|b$ for all i. By the inductive hypothesis, $a_1 a_2 \cdots a_n | b$. It therefore suffices so show that $a_1 a_2 \cdots a_n$ and a_{n+1} are relatively prime, for the result will then follow from the $n = 2$ case. Let $d = (a_1 a_2 \cdots a_n, a_{n+1})$. If $d \neq 1$, then there is a prime $p|d$. It follows that $p|a_1 a_2 \cdots a_n$ and $p|a_{n+1}$. By (the extended version of) Euclid's lemma, we must have $p|a_i$ for some $1 \leq i \leq n$. But then p is a nontrivial common divisor of a_i and a_{n+1}, contradicting the fact that $(a_i, a_{n+1}) = 1$. Hence $d = 1$ and, as noted above, the $n+1$ case is established. By induction, the lemma holds for all $n \geq 2$. □

The auxiliary fact established in the final paragraph of the preceding proof is worth recording independently.

Corollary 1. *If $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ are pairwise relatively prime, then $(a_1 a_2 \cdots a_{n-1}, a_n) = 1$.*

We are now ready for our main result.

Theorem 1 (Chinese remainder theorem)**.** *Let $n_1, n_2, \ldots n_r \in \mathbb{N}$ be pairwise relatively prime. For any $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ the solution set of the system of simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_r \pmod{n_r}, \end{aligned} \tag{2}$$

consists of a unique congruence class modulo $N = n_1 n_2 \cdots n_r$.

Proof. We will give an indirect, nonconstructive proof. We will return to the question of how to actually find the solution to (2) once we have proven the theorem. Consider the map

$$\begin{aligned} \rho : \mathbb{Z}/N\mathbb{Z} &\to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \cdots \times \mathbb{Z}/n_1\mathbb{Z} \\ a + N\mathbb{Z} &\mapsto (a + \mathbb{Z}/n_1\mathbb{Z}, a + \mathbb{Z}/n_2\mathbb{Z}, \ldots, a + \mathbb{Z}/n_r\mathbb{Z}). \end{aligned}$$

i.e. ρ maps the class of a modulo N to the r-tuple of classes of a modulo the n_i. ρ is well-defined since if $a + N\mathbb{Z} = b + N\mathbb{Z}$ then $N|a - b$. As $n_i|N$ for all i, this means $n_i|a - b$ and hence $a + n_i\mathbb{Z} = b + n_i\mathbb{Z}$ for all i.

To prove the theorem it suffices to prove that ρ is a bijection. To see this, first notice that x solves the system (2) if and only if $x + n_i\mathbb{Z} = a_i + n_i\mathbb{Z}$ for all i and that this happens if and only if $\rho(x + N\mathbb{Z}) = (a_1 + \mathbb{Z}/n_1\mathbb{Z}, a_2 + \mathbb{Z}/n_2\mathbb{Z}, \ldots, a_r + \mathbb{Z}/n_r\mathbb{Z})$. If ρ is a bijection, then there exists a unique $a + N\mathbb{Z} \in \mathbb{Z}/N\mathbb{Z}$ so that $\rho(a + N\mathbb{Z}) = (a_1 + \mathbb{Z}/n_1\mathbb{Z}, a_2 + \mathbb{Z}/n_2\mathbb{Z}, \ldots, a_r + \mathbb{Z}/n_r\mathbb{Z})$. According to what we first noticed, this shows that x solves (2) if and only if $x \in a + N\mathbb{Z}$. This is precisely what the theorem states.

It remains to prove that ρ is bijective. To do so we only need to show that ρ is injective since both its domain and codomain have size $n_1 n_2 \cdots n_r = N$. So suppose $\rho(a + N\mathbb{Z}) = \rho(b + N\mathbb{Z})$ for some $a, b \in \mathbb{Z}$. Then $a + n_i\mathbb{Z} = b + n_i\mathbb{Z}$, or $n_i|a - b$, for all i. Since the n_i are pairwise relatively prime, this means their product, N, divides $a - b$ by Lemma 1. Hence $a + N\mathbb{Z} = b + N\mathbb{Z}$ and ρ is injective. This completes the proof. □

Remark 1.

- The Chinese remainder theorem (CRT) asserts that there is a unique class $a + N\mathbb{Z}$ so that x solves the system (2) if and only if $x \in a + N\mathbb{Z}$, i.e. $x \equiv a \pmod{N}$. Thus the system (2) is equivalent to *a single congruence modulo N*.
- Although we only proved one implication, one can actually show that the CRT is *equivalent* to the bijectivity of ρ.

▼

Now we turn to the question of actually producing the solution to the system (2) of the Chinese remainder theorem. Since we know the solution is unique modulo the product

N of the moduli, if we can find a single solution, we can find them all by simply adding $N\mathbb{Z}$. It turns out that producing a particular solution is not that hard if one is just a bit clever. Before describing it, we make a quick observation. Suppose $n_1, n_2, \ldots, n_r$ are pairwise relatively prime. Let $N = n_1 n_2 \cdots n_r$ and $N_i = N/n_i$ (so that N_i is the product of all the n_j *except* n_i). Then n_i and N_i are relatively prime for all i by Corollary 1.

Theorem 2. *Let $n_1, n_2, \ldots, n_r \in \mathbb{N}$ be pairwise relatively prime and define N, N_i as above. Let m_i be a modular inverse of N_i modulo n_i, i.e. $m_i N_i \equiv 1 \pmod{n_i}$. Given $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ set*

$$a = a_1 m_1 N_1 + a_2 m_2 N_2 + \cdots + a_r m_r N_r.$$

Then a solves the system (2) of the Chinese remainder theorem. Therefore the solution set of (2) is $a + N\mathbb{Z}$, i.e. x is a solution if and only if $x \equiv a \pmod{N}$.

Proof. As noted above, in light of Theorem 1 it suffices to simply show that a is a solution to the system (2). We will show that $a \equiv a_1 \pmod{n_1}$. The same argument works for all of the other congruences. Since $n_1 | N_j$ for $j \geq 2$, $a \equiv a_1 m_1 N_1 \equiv a_1 \pmod{n_1}$ by our choice of m_1. That's it. □

Remark 2.

- According to comments that we've already made, the element a constructed in Theorem 2 satisfies

  $$\rho(a + N\mathbb{Z}) = (a_1 + \mathbb{Z}/n_1\mathbb{Z}, a_2 + \mathbb{Z}/n_2\mathbb{Z}, \ldots, a_r + \mathbb{Z}/n_r\mathbb{Z}).$$

  We have therefore proven, independently and constructively, that ρ is surjective. Once more appealing to the fact that the domain and codomain of ρ have the same size, we conclude that ρ must be injective as well and is thus a bijection. This provides a second proof of the CRT.

- Another choice for a in Theorem 2 is

  $$a = a_1 N_1^{\varphi(n_1)} + a_2 N_2^{\varphi(n_2)} + \cdots + a_r N_r^{\varphi(n_r)}$$

  as is easily seen by appealing to Euler's theorem. The main difficulty with using this expression, however, is that $\varphi(n)$ can be difficult to compute.

▼

Example 2. Solve the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod{25}, \\ x &\equiv 17 \pmod{26}, \\ x &\equiv 11 \pmod{27}. \end{aligned}$$

We have $n_1 = 25 = 5 \cdot 5$, $n_2 = 26 = 2 \cdot 13$ and $n_3 = 3^3$. Since their factorizations involve

distinct primes, n_1, n_2 and n_3 are certainly pairwise relatively prime. Moreover

$$\begin{aligned}
&N_1 = n_2 n_3 = 26 \cdot 27 \equiv 1 \cdot 2 \equiv 2 \pmod{25} \quad (25 = n_1),\\
&m_1 \equiv 13 \pmod{25},\\
&N_2 = n_1 n_3 = 25 \cdot 27 \equiv -1 \pmod{26} \quad (26 = n_2),\\
&m_2 \equiv -1 \pmod{26},\\
&N_3 = n_1 n_2 = 25 \cdot 26 \equiv (-2)(-1) \equiv 2 \pmod{27} \quad (27 = n_3),\\
&m_3 \equiv 14 \pmod{27}.
\end{aligned}$$

Thus x is a solution if and only if

$$\begin{aligned}
x &\equiv 1 \cdot 26 \cdot 27 \cdot 13 + 17 \cdot 25 \cdot 27 \cdot (-1) + 11 \cdot 25 \cdot 26 \cdot 14 \pmod{25 \cdot 26 \cdot 27}\\
&\equiv 97751 \pmod{17550}\\
&\equiv 10001 \pmod{17550}.
\end{aligned}$$

♦

Example 3. One day Dr. Daileda decided to sort through his CD collection. When he put them into piles of 8 CDs, he had 4 left over. When he put them into piles of 17 CDs he had 15 left over. And when he put them into piles of 25 he had 4 left over. What is the smallest possible number of CDs that Dr. Daileda had?

The number of CDs must simultaneously solve the congruences

$$\begin{aligned}
&x \equiv 4 \pmod{8},\\
&x \equiv 15 \pmod{17},\\
&x \equiv 4 \pmod{25}.
\end{aligned}$$

Since $n_1 = 8$, $n_2 = 17$ and $n_3 = 25$ are clearly relatively prime, we may apply the Chinese remainder theorem. We have

$$N_1 = 17 \cdot 25 \equiv 1 \cdot 1 \equiv 1 \pmod{8} \quad \Rightarrow \quad m_1 \equiv 1 \pmod{8}, \tag{3}$$

$$N_2 = 8 \cdot 25 \equiv 8 \cdot 8 = 64 \equiv 13 \pmod{17} \quad \Rightarrow \quad m_2 \equiv 4 \pmod{17}, \tag{4}$$

$$N_3 = 8 \cdot 17 \equiv 8(-8) = -64 \equiv -14 \equiv 11 \pmod{25} \quad \Rightarrow \quad m_3 \equiv 16 \pmod{25}. \tag{5}$$

Hence the solutions to this set of congruences are given by

$$\begin{aligned}
x &\equiv 4 \cdot 17 \cdot 25 \cdot 1 + 15 \cdot 8 \cdot 25 \cdot 4 + 4 \cdot 8 \cdot 17 \cdot 16 \pmod{8 \cdot 17 \cdot 25}\\
&\equiv 22404 \pmod{3400}\\
&\equiv 2004 \pmod{3400}.
\end{aligned}$$

Since 2004 is the least positive element in its congruence class modulo 3400 (it's a remainder), this is the fewest number of CDs. ♦

Example 4. Use the second remark after Theorem 2 to solve the system of congruences

$$\begin{aligned}
&x \equiv 4 \pmod{5},\\
&x \equiv 2 \pmod{7},\\
&x \equiv 2 \pmod{8},\\
&x \equiv 1 \pmod{9}.
\end{aligned}$$

We have $N = 2520$ and

$$\begin{aligned}
N_1^{\varphi(n_1)} &= (7 \cdot 8 \cdot 9)^4 = 64524128256 \equiv 2016 \pmod{2520},\\
N_2^{\varphi(n_2)} &= (5 \cdot 8 \cdot 9)^6 = 2176782336000000 \equiv 1800 \pmod{2520},\\
N_3^{\varphi(n_3)} &= (5 \cdot 7 \cdot 9)^4 = 9845600625 \equiv 945 \pmod{2520},\\
N_4^{\varphi(n_4)} &= (5 \cdot 7 \cdot 8)^6 = 481890304000000 \equiv 280 \pmod{2520}.
\end{aligned}$$

Hence

$$a \equiv 4 \cdot 2016 + 2 \cdot 1800 + 2 \cdot 945 + 1 \cdot 280 = 13834 \equiv 1234 \pmod{2520}$$

so that the solution is

$$\boxed{x \equiv 1234 \pmod{2520}.}$$

♦

2 CRT and Units Modulo n

2.1 Direct Products of Rings

Given rings $R_1, R_2, \ldots, R_n$ the set $R_1 \times R_2 \times \cdots \times R_n$ is endowed with two binary operations which arise by simply applying the operations of the individual R_i coordinate-wise:

$$\begin{aligned}
(r_1, r_2, \ldots, r_n) + (s_1, s_2, \ldots, s_n) &= (r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n),\\
(r_1, r_2, \ldots, r_n) \cdot (s_1, s_2, \ldots, s_n) &= (r_1 \cdot s_1, r_2 \cdot s_2, \ldots, r_n \cdot s_n).
\end{aligned}$$

It is not difficult to show that $R_1 \times R_2 \times \cdots \times R_n$ together with these operations is again a ring, called the *direct product* of $R_1, R_2, \ldots, R_n$. Its zero is $(0_{R_1}, 0_{R_2}, \ldots, 0_{R_n})$ and its identity is $(1_{R_1}, 1_{R_2}, \ldots, 1_{R_n})$. Consequently, it is not difficult to show that

$$(R_1 \times R_2 \times \cdots \times R_n)^\times = R_1^\times \times R_2^\times \times \cdots \times R_n^\times.$$

That is, an element of the direct product is a unit if and only if every coordinate is a unit (in its respective ring).

The map ρ in the proof of the Chinese remainder theorem can therefore be viewed as a bijection between two rings. It actually has another property relative to ring structure that is very useful: it preserves ring operations. For example

$$\begin{aligned}
\rho((a + N\mathbb{Z}) + (b + N\mathbb{Z})) &= \rho((a + b) + n\mathbb{Z})\\
&= ((a + b) + n_1\mathbb{Z}, (a + b) + n_2\mathbb{Z}, \ldots, (a + b) + n_r\mathbb{Z})\\
&= ((a + n_1\mathbb{Z}) + (b + n_1\mathbb{Z}), (a + n_2\mathbb{Z}) + (b + n_2\mathbb{Z}), \ldots, (a + n_r\mathbb{Z}) + (b + n_r\mathbb{Z}))\\
&= (a + n_1\mathbb{Z}, a + n_2\mathbb{Z}, \ldots, a + n_r\mathbb{Z}) + (b + n_1\mathbb{Z}, b + n_2\mathbb{Z}, \ldots, b + n_r\mathbb{Z})\\
&= \rho(a + N\mathbb{Z}) + \rho(b + N\mathbb{Z}).
\end{aligned}$$

An entirely similar computation shows that

$$\rho((a + N\mathbb{Z})(b + N\mathbb{Z})) = \rho(a + N\mathbb{Z})\rho(b + N\mathbb{Z}).$$

Maps between rings that preserve both binary operations are called *ring homomorphisms.* If a ring homomorphism is bijective it is called an *isomorphism* and the domain and codomain

are said to be *isomorphic*. So we see that ρ is an isomorphism. Isomorphic rings are "the same" in the sense that they share their ring-theoretic properties. For example, we have the next result.

Lemma 2. *Let $\alpha : R \to S$ be an isomorphism of rings. Then $\alpha(1_R) = 1_S$ and $\alpha|_{R^\times}$ gives a (multiplication preserving) bijection from $R^\times$ to $S^\times$.*

Proof. Since α is surjective, there is an $r \in R$ so that $\alpha(r) = 1_S$. Then $\alpha(1_R) = \alpha(1_R) \cdot 1_S = \alpha(1_R)\alpha(r) = \alpha(1_R \cdot r) = \alpha(r) = 1_S$. Since $\alpha|_{R^\times}$ is injective, to prove the second part of the theorem it suffices to show that $\alpha(R^\times) = S^\times$. Let $a \in R^\times$. Then $1_S = \alpha(1_R) = \alpha(aa^{-1}) = \alpha(a)\alpha(a^{-1})$. Likewise, $\alpha(a^{-1})\alpha(a) = 1_S$. Hence $\alpha(R^\times) \subseteq S^\times$. Let $s \in S^\times$. Choose $a, b \in R$ so that $\alpha(a) = s$ and $\alpha(b) = s^{-1}$. Then $\alpha(ab) = \alpha(a)\alpha(b) = ss^{-1} = 1_S = \alpha(1_R)$. Since α is injective, we must have $ab = 1_R$. Similarly, $ba = 1_R$. Hence $a \in R^\times$ and therefore $S^\times \subseteq \alpha(R^\times)$. It follows that the two sets are equal which we have already noted finishes the proof. □

2.2 Decomposition of $(\mathbb{Z}/n\mathbb{Z})^\times$

Finally, let's apply the discussion of the preceding section to the isomorphism ρ.

Corollary 2. *Let $n_1, n_2, \ldots, n_r \in \mathbb{N}$ be pairwise relatively prime. If $N = n_1 n_2 \cdots n_r$, then the map*

$$a + N\mathbb{Z} \mapsto (a + n_1\mathbb{Z}, a + n_2\mathbb{Z}, \ldots, a + n_r\mathbb{Z})$$

gives a (multiplication preserving) bijection from $(\mathbb{Z}/N\mathbb{Z})^\times$ to $(\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^\times$.

Corollary 3. *If $n_1, n_2, \ldots, n_r \in \mathbb{N}$ are pairwise relatively prime, then*

$$\varphi(n_1 n_2 \cdots n_r) = \varphi(n_1)\varphi(n_2) \cdots \varphi(n_r),$$

i.e. φ is multiplicative.

Remark 3. Given an *arithmetic function* $f : \mathbb{N} \to \mathbb{C}$, one usually says it is multiplicative if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$. It is not too hard to show, however, that this is equivalent to the property stated for φ above. ▼

Corollary 4. *Let $n \in \mathbb{N}$ and write n as a product of powers of distinct primes:*

$$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}, \;\; p_i \text{ distinct primes, } m_i \in \mathbb{N}.$$

Then:

1. *$(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to $(\mathbb{Z}/p_1^{m_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{m_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{m_r}\mathbb{Z})^\times$;* [1]
2. *$\varphi(n) = \varphi(p_1^{m_1})\varphi(p_2^{m_2}) \cdots \varphi(p_r^{m_r})$.*

Proof. Take $n_i = p_i^{m_i}$ in the previous two corollaries. □

[1] Two groups are said to be *isomorphic* if there is an operation preserving bijection between them.

Corollary 4 was the true goal of introducing the Chinese remainder theorem. It reduces the study of the structure of the unit group $(\mathbb{Z}/n\mathbb{Z})^\times$ for arbitrary n to the study of unit groups of the form $(\mathbb{Z}/p^m\mathbb{Z})^\times$ where p is prime. We'll return to this topic later. The corollary also allows us to determine an explicit formula for $\varphi(n)$ in terms of the prime factorization of n, as we will now see.

Lemma 3. *Let p be a prime and $m \in \mathbb{N}$. Then*

$$\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1) = p^m\left(1 - \frac{1}{p}\right).$$

Proof. To count $(\mathbb{Z}/p^m\mathbb{Z})^\times$ we will instead count its complement in $\mathbb{Z}/p^m\mathbb{Z}$ and subtract that number from p^m. The integers from 1 to p^m that are *not* relatively prime to p^m are precisely the multiples of p in that range. So we need to count the positive k that satisfy $kp \leq p^m$. But if we divide both sides by p we immediately obtain $1 \leq k \leq p^{m-1}$. So there are exactly p^{m-1} multiples of p less than or equal to p^m. That leaves $p^m - p^{m-1}$ positive integers in that range that are relatively prime to p^m. Hence $\varphi(p^m) = p^m - p^{m-1}$. □

Remark 4. Note that if $p = 2$ then $\varphi(2^m) = 2^{m-1}(2-1) = 2^{m-1}$. In other words, exactly half of the elements of $\mathbb{Z}/2^m\mathbb{Z}$ are units. This is easily explained. In order to be relatively prime to 2^m an integer need only be odd, and exactly half of the positive integers up to 2^m are odd. ▼

Theorem 3. *Let $n \in \mathbb{N}$ and write n as a product of powers of distinct primes:*

$$n = p_1^{m_1}p_2^{m_2}\cdots p_r^{m_r}, \;\; p_i \text{ distinct primes, } m_i \in \mathbb{N}.$$

Then

$$\varphi(n) = p_1^{m_1-1}(p_1-1)p_2^{m-1}(p_2-1)\cdots p_r^{m_r-1}(p_r-1) = n\prod_{p|n}\left(1-\frac{1}{p}\right).$$

Proof. This follows immediately from the Lemma and the multiplicativity of φ. □

Example 5.

- $\varphi(100) = \varphi(5^2)\varphi(2^2) = 5(5-1)\cdot 2 = 40.$
- $\varphi(230) = \varphi(23)\varphi(2)\varphi(5) = 22\cdot 1\cdot 4 = 88.$
- $\varphi(572) = \varphi(2^2)\varphi(11)\varphi(13) = 2\cdot 10\cdot 12 = 240.$
- $\varphi(902016) = \varphi(2^7)\varphi(3^5)\varphi(29) = 2^6\cdot 3^4(3-1)\cdot 28 = 290304.$

♦

Example 6. Find the remainder when 3^{2049} is divided by 68

We see that $\varphi(68) = \varphi(2^2)\varphi(17) = 2\cdot 16 = 32$ and $2049 \equiv 1 \pmod{32}$. Hence, by Euler's theorem,

$$3^{2049} \equiv 3^1 \equiv 3 \pmod{68},$$

and the remainder is $\boxed{3}$. ♦