The Chinese Remainder Theorem

R. C. Daileda February 19, 2018

# The Chinese Remainder Theorem

We begin with an example.

**Example 1.** Consider the system of simultaneous congruences

*x* ≡ 3 (mod 5)*,*

*x* ≡ 2 (mod 6)*.*

(1)

Clearly *x* = 8 is a solution. If *y* were another solution, then we would have *y* 8 (mod 5) and *y* 8 (mod 6). Hence 5 *y* 8 and 6 *y* 8. As (5*,* 6) = 1, this means 30 *y* 8 or *y* 8 (mod 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 + 30Z. 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*, . . . , an* ∈ Z *be pairwise relatively prime. If b* ∈ Z *and ai*|*b for all i, then a*1*a*2 · · · *an*|*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 B´ezout’s lemma to write *ra*1 + *sa*2 = 1 for some *r, s* Z. Also write *b* = *b*1*a*1 and *b* = *b*2*a*2. We multiply the B´ezout 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* 2. Let *a*1*, a*2*, . . . an, an*+1 Z be pairwise relatively prime and suppose that *ai b* for all *i*. By the inductive hypothesis, *a*1*a*2 *an b*. It therefore suffices so show that *a*1*a*2 *an* and *an*+1 are relatively prime, for the result will then follow from the *n* = 2 case. Let *d* = (*a*1*a*2 *an, an*+1). If *d* = 1, then there is a prime *p d*. It follows that *p a*1*a*2 *an* and *p an*+1. By (the extended version of) Euclid’s lemma, we must have *p ai* for some 1 *i n*. But then *p* is a nontrivial common divisor of *ai* and *an*+1, contradicting the fact that (*ai, an*+1) = 1. Hence *d* = 1 and, as noted above, the *n* + 1 case is established. By induction, the lemma holds for all *n* ≥ 2.

| ≤ ≤

| | · · · |

· · · /

· · ·

| · · · |

≥ ∈

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

**Corollary 1.** *If a*1*, a*2*, . . . , an* ∈ Z *are pairwise relatively prime, then* (*a*1*a*2 · · · *an−*1*, an*) = 1*.*

We are now ready for our main result.

**Theorem 1** (Chinese remainder theorem)**.** *Let n*1*, n*2*, . . . nr* ∈ N *be pairwise relatively prime.*

*For any a*1*, a*2*, . . . , ar* ∈ Z *the solution set of the system of simultaneous congruences*

*x* ≡ *a*1 (mod *n*1)*,*

*x* ≡ *a*2 (mod *n*2)*,*

*.*

*x* ≡ *ar* (mod *nr*)*,*

*consists of a unique congruence class modulo N* = *n*1*n*2 · · · *nr.*

(2)

*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

*ρ* : Z*/N* Z → Z*/n*1Z × Z*/n*2Z · · · × Z*/n*1Z

*a* + *N* Z ›→ (*a* + Z*/n*1Z*, a* + Z*/n*2Z*, . . . , a* + Z*/nr*Z)*.*

i.e. *ρ* maps the class of *a* modulo *N* to the *r*-tuple of classes of *a* modulo the *ni*. *ρ* is well- defined since if *a* + *N* Z = *b* + *N* Z then *N a b*. As *ni N* for all *i*, this means *ni a b* and hence *a* + *ni*Z = *b* + *ni*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* + *ni*Z = *ai* + *ni*Z for all *i* and that this happens if and only if *ρ*(*x* + *N* Z) = (*a*1 +Z*/n*1Z*, a*2 +Z*/n*2Z*, . . . , ar* +Z*/nr*Z). If *ρ* is a bijection, then there exists a unique *a*+*N* Z Z*/N* Z so that *ρ*(*a*+*N* Z) = (*a*1+Z*/n*1Z*, a*2+Z*/n*2Z*, . . . , ar*+Z*/nr*Z). According to what we first noticed, this shows that *x* solves (2) if and only if *x a* + *N* 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 *nr* = *N* . So suppose *ρ*(*a* + *N* Z) = *ρ*(*b* + *N* Z) for some *a, b* Z. Then *a* + *ni*Z = *b* + *ni*Z, or *ni a b*, for all *i*. Since the *ni* are pairwise relatively prime, this means their product, *N* , divides *a b* by Lemma 1. Hence *a* + *N* Z = *b* + *N* 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* Z so that *x* solves the system (2) if and only if *x a* + *N* Z, i.e. *x a* (mod *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 *equiv- alent* to the bijectivity of *ρ*.

•

V

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* 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*, . . . , nr* are pairwise relatively prime. Let *N* = *n*1*n*2 *nr* and *Ni* = *N/ni* (so that *Ni* is the product of all the *nj except ni*). Then *ni* and *Ni* are relatively prime for all *i* by Corollary 1.

· · ·

**Theorem 2.** *Let n*1*, n*2*, . . . , nr* N *be pairwise relatively prime and define N, Ni as above. Let mi be a modular inverse of Ni modulo ni, i.e. miNi* 1 (mod *ni*)*. Given a*1*, a*2*, . . . , ar* Z *set*

≡ ∈

∈

*a* = *a*1*m*1*N*1 + *a*2*m*2*N*2 + · · · + *armrNr.*

*Then a solves the system* (2) *of the Chinese remainder theorem. Therefore the solution set of* (2) *is a* + *N* Z*, i.e. x is a solution if and only if x* ≡ *a* (mod *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 a*1 (mod *n*1). The same argument works for all of the other congruences. Since *n*1 *Nj* for *j* 2, *a a*1*m*1*N*1 *a*1 (mod *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

•

*ρ*(*a* + *N* Z) = (*a*1 + Z*/n*1Z*, a*2 + Z*/n*2Z*, . . . , ar* + Z*/nr*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*Nϕ*(*n*1) + *a*2*Nϕ*(*n*2) + · · · + *arNϕ*(*nr* )

1

2

*r*

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

V

**Example 2.** Solve the system of congruences

*x* ≡ 1 (mod 25)*,*

*x* ≡ 17 (mod 26)*,*

*x* ≡ 11 (mod 27)*.*

We have *n*1 = 25 = 5 · 5, *n*2 = 26 = 2 · 13 and *n*3 = 33. Since their factorizations involve

distinct primes, *n*1, *n*2 and *n*3 are certainly pairwise relatively prime. Moreover

*N*1 = *n*2*n*3 = 26 · 27 ≡ 1 · 2 ≡ 2 (mod 25) (25 = *n*1)*,*

*m*1 ≡ 13 (mod 25)*,*

*N*2 = *n*1*n*3 = 25 · 27 ≡ −1 (mod 26) (26 = *n*2)*,*

*m*2 ≡ −1 (mod 26)*,*

*N*3 = *n*1*n*2 = 25 · 26 ≡ (−2)(−1) ≡ 2 (mod 27) (27 = *n*3)*,*

*m*3 ≡ 14 (mod 27)*.*

Thus *x* is a solution if and only if

*x* ≡ 1 · 26 · 27 · 13 + 17 · 25 · 27 · (−1) + 11 · 25 · 26 · 14 (mod 25 · 26 · 27)

≡ 97751 (mod 17550)

≡ 10001 (mod 17550)*.*

◆

**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

*x* ≡ 4 (mod 8)*,*

*x* ≡ 15 (mod 17)*,*

*x* ≡ 4 (mod 25)*.*

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 · 25 ≡ 1 · 1 ≡ 1 (mod 8) ⇒ *m*1 ≡ 1 (mod 8)*,* (3)

*N*2 = 8 · 25 ≡ 8 · 8 = 64 ≡ 13 (mod 17) ⇒ *m*2 ≡ 4 (mod 17)*,* (4)

*N*3 = 8 · 17 ≡ 8(−8) = −64 ≡ −14 ≡ 11 (mod 25) ⇒ *m*3 ≡ 16 (mod 25)*.* (5)

Hence the solutions to this set of congruences are given by

*x* ≡ 4 · 17 · 25 · 1 + 15 · 8 · 25 · 4 + 4 · 8 · 17 · 16 (mod 8 · 17 · 25)

≡ 22404 (mod 3400)

≡ 2004 (mod 3400)*.*

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

*x* ≡ 4 (mod 5)*,*

*x* ≡ 2 (mod 7)*,*

*x* ≡ 2 (mod 8)*,*

*x* ≡ 1 (mod 9)*.*

We have *N* = 2520 and

*Nϕ*(*n*1) = (7 · 8 · 9)4 = 64524128256 ≡ 2016 (mod 2520)*,*

1

*Nϕ*(*n*2) = (5 · 8 · 9)6 = 2176782336000000 ≡ 1800 (mod 2520)*,*

2

*Nϕ*(*n*3) = (5 · 7 · 9)4 = 9845600625 ≡ 945 (mod 2520)*,*

3

*Nϕ*(*n*4) = (5 · 7 · 8)6 = 481890304000000 ≡ 280 (mod 2520)*.*

4

Hence

*a* ≡ 4 · 2016 + 2 · 1800 + 2 · 945 + 1 · 280 = 13834 ≡ 1234 (mod 2520)

so that the solution is

*x* ≡ 1234 (mod 2520)*.*

◆

# CRT and Units Modulo *n*

## Direct Products of Rings

Given rings *R*1*, R*2*, . . . , Rn* the set *R*1 *R*2 *Rn* is endowed with two binary operations which arise by simply applying the operations of the individual *Ri* coordinate-wise:

× × · · · ×

(*r*1*, r*2*, . . . , rn*) + (*s*1*, s*2*, . . . , sn*) = (*r*1 + *s*1*, r*2 + *s*2*, . . . , rn* + *sn*)*,*

(*r*1*, r*2*, . . . , rn*) · (*s*1*, s*2*, . . . , sn*) = (*r*1 · *s*1*, r*2 · *s*2*, . . . , rn* · *sn*)*.*

It is not difficult to show that *R*1 × *R*2 × · · · × *Rn* together with these operations is again a ring, called the *direct product* of *R*1*, R*2*, . . . , Rn*. Its zero is (0*R*1 *,* 0*R*2 *, . . . ,* 0*Rn* ) and its identity is (1*R*1 *,* 1*R*2 *, . . . ,* 1*Rn* ). Consequently, it is not difficult to show that

(*R*1 × *R*2 × · · · × *Rn*)*×* = *R*1*×* × *R*2*×* × · · · × *Rn×.*

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

*ρ*((*a* + *N* Z) + (*b* + *N* Z)) = *ρ*((*a* + *b*) + *n*Z)

= ((*a* + *b*) + *n*1Z*,* (*a* + *b*) + *n*2Z*, . . . ,* (*a* + *b*) + *nr*Z)

= ((*a* + *n*1Z) + (*b* + *n*1Z)*,* (*a* + *n*2Z) + (*b* + *n*2Z)*, . . . ,* (*a* + *nr*Z) + (*b* + *nr*Z))

= (*a* + *n*1Z*, a* + *n*2Z*, . . . , a* + *nr*Z) + (*b* + *n*1Z*, b* + *n*2Z*, . . . , b* + *nr*Z)

= *ρ*(*a* + *N* Z) + *ρ*(*b* + *N* Z)*.*

An entirely similar computation shows that

*ρ*((*a* + *N* Z)(*b* + *N* Z)) = *ρ*(*a* + *N* Z)*ρ*(*b* + *N* 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 α* : *R S be an isomorphism of rings. Then α*(1*R*) = 1*S and α R× gives a (multiplication preserving) bijection from R× to S×.*

→ |

*Proof.* Since *α* is surjective, there is an *r* ∈ *R* so that *α*(*r*) = 1*S*. Then *α*(1*R*) = *α*(1*R*) · 1*S* = *α*(1*R*)*α*(*r*) = *α*(1*R r*) = *α*(*r*) = 1*S*. Since *α R×* is injective, to prove the second part of the theorem it suffices to show that *α*(*R×*) = *S×*. Let *a R×*. Then 1*S* = *α*(1*R*) = *α*(*aa−*1) = *α*(*a*)*α*(*a−*1). Likewise, *α*(*a−*1)*α*(*a*) = 1*S*. Hence *α*(*R×*) *S×*. Let *s S×*. Choose *a, b R* so that *α*(*a*) = *s* and *α*(*b*) = *s−*1. Then *α*(*ab*) = *α*(*a*)*α*(*b*) = *ss−*1 = 1*S* = *α*(1*R*). Since *α* is injective, we must have *ab* = 1*R*. Similarly, *ba* = 1*R*. Hence *a R×* and therefore *S× α*(*R×*). It follows that the two sets are equal which we have already noted finishes the proof.

⊆

∈

⊆ ∈ ∈

∈

· |

* 1. **Decomposition of** (Z*/n*Z)*×*

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

**Corollary 2.** *Let n*1*, n*2*, . . . , nr* N *be pairwise relatively prime. If N* = *n*1*n*2 *nr, then the map*

∈ · · ·

*a* + *N* Z ›→ (*a* + *n*1Z*, a* + *n*2Z*, . . . , a* + *nr*Z)

*gives a (multiplication preserving) bijection from* (Z*/N* Z)*× to* (Z*/n*1Z)*×* (Z*/n*2Z)*×* (Z*/nr*Z)*×.*

× × · · · ×

**Corollary 3.** *If n*1*, n*2*, . . . , nr* ∈ N *are pairwise relatively prime, then*

*ϕ*(*n*1*n*2 · · · *nr*) = *ϕ*(*n*1)*ϕ*(*n*2) · · · *ϕ*(*nr*)*,*

*i.e. ϕ is* multiplicative*.*

**Remark 3.** Given an *arithmetic function f* : N 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. V

→

**Corollary 4.** *Let n* ∈ N *and write n as a product of powers of distinct primes:*

*n* = *pm*1 *pm*2 · · · *pmr , pi distinct primes, mi* ∈ N*.*

*Then:*

1 2 *r*

1. (Z*/n*Z)*× is isomorphic to* (Z*/pm*1 Z)*×* × (Z*/pm*2 Z)*×* × · · · × (Z*/pmr* Z)*×;* 1

1 2 *r*

*2. ϕ*(*n*) = *ϕ*(*pm*1 )*ϕ*(*pm*2 ) · · · *ϕ*(*pmr* )*.*

1

2

*r*

*Proof.* Take *ni* = *pmi* in the previous two corollaries.

*i*

1Two 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 (Z*/n*Z)*×* for arbitrary *n* to the study of unit groups of the form (Z*/pm*Z)*×* where *p* is prime. We’ll return to this topic later. The corollary also allows us to determine an explicit formula for *ϕ*(*n*) in terms of the prime factorization of *n*, as we will now see.

**Lemma 3.** *Let p be a prime and m* ∈ N*. Then*

*ϕ*(*pm*) = *pm* − *pm−*1 = *pm−*1(*p* − 1) = *pm* 1 − 1 *.*

*p*

*Proof.* To count (Z*/pm*Z)*×* we will instead count its complement in Z*/pm*Z and subtract that number from *pm*. The integers from 1 to *pm* that are *not* relatively prime to *pm* are precisely the multiples of *p* in that range. So we need to count the positive *k* that satisfy *kp* ≤ *pm*. But if we divide both sides by *p* we immediately obtain 1 ≤ *k* ≤ *pm−*1. So there are exactly

*pm−*1 multiples of *p* less than or equal to *pm*. That leaves *pm* − *pm−*1 positive integers in that

range that are relatively prime to *pm*. Hence *ϕ*(*pm*) = *pm* − *pm−*1.

**Remark 4.** Note that if *p* = 2 then *ϕ*(2*m*) = 2*m−*1(2 1) = 2*m−*1. In other words, exactly half of the elements of Z*/*2*m*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. V

−

**Theorem 3.** *Let n* ∈ N *and write n as a product of powers of distinct primes:*

*n* = *pm*1 *pm*2 · · · *pmr , pi distinct primes, mi* ∈ N*.*

*Then*

2

*r*

1 2 *r*

*ϕ*(*n*) = *pm*1*−*1(*p*1

1

— 1)*pm−*1(*p*2

— 1) · · · *pmr−*1(*pr*

1) = *n* 1 1 *.*

*p*

Y − −

*p|n*

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

## Example 5.

* *ϕ*(100) = *ϕ*(52)*ϕ*(22) = 5(5 − 1) · 2 = 40*.*
* *ϕ*(230) = *ϕ*(23)*ϕ*(2)*ϕ*(5) = 22 · 1 · 4 = 88*.*
* *ϕ*(572) = *ϕ*(22)*ϕ*(11)*ϕ*(13) = 2 · 10 · 12 = 240*.*
* *ϕ*(902016) = *ϕ*(27)*ϕ*(35)*ϕ*(29) = 26 · 34(3 − 1) · 28 = 290304*.*

◆

**Example 6.** Find the remainder when 32049 is divided by 68

We see that *ϕ*(68) = *ϕ*(22)*ϕ*(17) = 2 16 = 32 and 2049 1 (mod 32). Hence, by Euler’s theorem,

· ≡

and the remainder is .

3

32049 ≡ 31 ≡ 3 (mod 68)*,*

◆