THE CHINESE REMAINDER THEOREM

KEITH CONRAD

We should thank the Chinese for their wonderful remainder theorem.
Glenn Stevens

1. Introduction

The Chinese remainder theorem says we can uniquely solve any system of congruences with pairwise relatively prime moduli.

Theorem 1.1. *For $r \geq 2$, let $m_1, m_2, \ldots, m_r$ be nonzero integers which are pairwise relatively prime: $(m_i, m_j) = 1$ for $i \neq j$. Then, for any integers $a_1, a_2, \ldots, a_r$, the system of congruences*

$$x \equiv a_1 \bmod m_1, \quad x \equiv a_2 \bmod m_2, \quad \ldots, \quad x \equiv a_r \bmod m_r,$$

has a solution, and this solution is uniquely determined modulo $m_1 m_2 \cdots m_r$.

Example. The congruences $x \equiv 1 \bmod 3$, $x \equiv 2 \bmod 5$, $x \equiv 2 \bmod 7$ are satisfied when $x = 37$, and more generally for any $x \equiv 37 \bmod 105$ and for no other x. Note $105 = 3 \cdot 5 \cdot 7$.

We will prove the Chinese remainder theorem and then see some ways it is applied in number theory.

2. A proof of the Chinese remainder theorem

Proof. First we show there is always a solution. Then we will show it is unique modulo $m_1 m_2 \cdots m_r$.

Existence of Solution. We argue by induction on r. The base case $r = 2$ will be the heart of the proof.

The base case is this: we are given two relatively prime nonzero integers m and n and we want to solve the simultaneous congruences

$$x \equiv a \bmod m, \quad x \equiv b \bmod n$$

for any choice of a and b. Here are two proofs that this can be done.

First proof: Lift the first congruence to an equation in $\mathbf{Z}$, as $x = a + my$ for some $y \in \mathbf{Z}$ to be determined. Then the second congruence is the same as

$$a + my \equiv b \bmod n.$$

Subtracting a from both sides, we need to solve for y in

$$my \equiv b - a \bmod n.$$

This is solvable (in y) since $(m, n) = 1$, so $m \bmod n$ is invertible. Having found y, we get a solution $x = a + my$ to both congruences.

Second proof: Lift both congruences to equations in $\mathbf{Z}$: $x = a + my$ and $x = b + nz$ for integers y and z to be determined. (Why would it be a bad idea to write $x = a + my$ and $x = b + ny$?) We need to find y and z in $\mathbf{Z}$ such that

$$a + my = b + nz,$$

which is the same as

$$my - nz = b - a. \tag{2.1}$$

Since $(m, n) = 1$, Bezout tells us 1 is a $\mathbf{Z}$-linear combination of m and n, and therefore any integer is $\mathbf{Z}$-linear combination of m and n (why?). Therefore y and z satisfying (2.1) exist.

Both of these arguments provide constructive recipes for getting a solution x in any particular example of the base case.

Now we pass to the inductive step. Suppose all simultaneous congruences with r pairwise relatively prime moduli can be solved. Consider a system of simultaneous congruences with $r + 1$ pairwise relatively prime moduli:

$$x \equiv a_1 \bmod m_1, \quad \dots, \quad x \equiv a_r \bmod m_r, \quad x \equiv a_{r+1} \bmod m_{r+1},$$

where $(m_i, m_j) = 1$ for all i and the a_i's are arbitrary. By the inductive hypothesis, there is a solution to the first r congruences, say

$$b \equiv a_1 \bmod m_1, \quad b \equiv a_2 \bmod m_2, \quad \dots, \quad b \equiv a_r \bmod m_r.$$

Now consider the system of *two* congruences

$$x \equiv b \bmod m_1 m_2 \cdots m_r, \quad x \equiv a_{r+1} \bmod m_{r+1}. \tag{2.2}$$

Since $(m_i, m_{r+1}) = 1$ for $i = 1, 2, \dots, r$, we have $(m_1 m_2 \cdots m_r, m_{r+1}) = 1$, so the two moduli in (2.2) are pairwise relatively prime. Then by the base case of two congruences, there is a solution to (2.2), call it c. Since $c \equiv b \bmod m_1 m_2 \cdots m_r$, we have $c \equiv b \bmod m_i$ for $i = 1, 2, \dots, r$. From the choice of b we have $b \equiv a_i \bmod m_i$ for $i = 1, 2, \dots, r$. Therefore $c \equiv a_i \bmod m_i$ for $i = 1, 2, \dots, r$. Also, $c \equiv a_{r+1} \bmod m_{r+1}$ from the choice of c, so we see c satisfies the $r + 1$ given congruences.

This concludes the inductive step, so a solution exists.

Uniqueness of Solution. If $x = c$ and $x = c'$ both satisfy

$$x \equiv a_1 \bmod m_1, \quad x \equiv a_2 \bmod m_2, \quad \dots, \quad x \equiv a_r \bmod m_r,$$

then we have $c \equiv c' \bmod m_i$ for $i = 1, 2, \dots, r$, so $m_i | (c - c')$ for $i = 1, 2, \dots, r$. Since the m_i's are pairwise relatively prime, their product $m_1 m_2 \cdots m_r$ divides $c - c'$, which means $c \equiv c' \bmod m_1 m_2 \cdots m_r$. This shows any two solutions to the given system of congruences are the same when viewed modulo $m_1 m_2 \cdots m_r$. □

3. Applications

The significance of the Chinese remainder theorem is that it often reduces questions about modulus mn, where $(m, n) = 1$, to the same question for modulus m and n separately. In this way, questions about modular arithmetic can often be reduced to the special case of prime power modulus. We will see how this works for several counting problems: counting units mod m, counting squares mod m, counting square roots of a square mod m, and more general root counting mod m.

In the coming discussions, we will often use two features of modular arithmetic with two moduli:

- if $d|m$ it makes sense to reduce integers mod m to integers mod d: if $x \equiv y \bmod m$ then $x \equiv y \bmod d$. For example, if $x \equiv y \bmod 10$ then $x \equiv y \bmod 5$ since $x - y$ is divisible by 10 and thus is also divisible by 5. (In contrast, it makes no sense to reduce $x \bmod 10$ to $x \bmod 3$, since there are congruent numbers mod 10 which are incongruent mod 3, such as 5 and 15.)
- if $x \equiv y \bmod m$ and $x \equiv y \bmod n$ and $(m, n) = 1$ then $x \equiv y \bmod mn$. This was used in the uniqueness part of the proof of the Chinese remainder theorem.

Our first application is to counting units.

Theorem 3.1. *For relatively prime positive integers m and n, $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. We work with the sets

$$U_m = \{a \bmod m, (a, m) = 1\}, \quad U_n = \{b \bmod n, (b, n) = 1\},$$

$$U_{mn} = \{c \bmod mn, (c, mn) = 1\}.$$

Then $\#U_m = \varphi(m)$, $\#U_n = \varphi(n)$, and $\#U_{mn} = \varphi(mn)$. To show $\varphi(mn) = \varphi(m)\varphi(n)$, we will write down a bijection between U_{mn} and $U_m \times U_n$, which implies the two sets have the same size, and that is what the theorem is saying (since $\#(U_m \times U_n) = \varphi(m)\varphi(n)$).

Let $f\colon U_{mn} \to U_m \times U_n$ by the rule

$$f(c \bmod mn) = (c \bmod m, c \bmod n).$$

For $c \in U_{mn}$, we have $(c, mn) = 1$, so (c, m) and (c, n) equal 1, so $c \bmod m$ and $c \bmod n$ are units. Let's stop for a moment to take a look at an example of this function.

Take $m = 3$ and $n = 5$: $U_3 = \{1, 2\}$, $U_5 = \{1, 2, 3, 4\}$, and $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. The following table shows the values of the function f on each number in U_{15}. Notice that the values fill up all of $U_3 \times U_5$ without repetition.

$c \bmod 15$	$f(c \bmod 15)$
1	$(1, 1)$
2	$(2, 2)$
4	$(4, 4) = (1, 4)$
7	$(7, 7) = (1, 2)$
8	$(8, 8) = (2, 3)$
11	$(11, 11) = (2, 1)$
13	$(13, 13) = (1, 3)$
14	$(14, 14) = (2, 4)$

There are 2 units modulo 3 and 4 units modulo 5, leading to 8 ordered pairs of units modulo 3 and units modulo 5: (1,1), (1,2), (1,3), (1,4), (2,1), (2,2), (2,3), and (2,4). All these pairs show up (and just once) in the second column of the table.

We return to the general situation and show $f\colon U_{mn} \to U_m \times U_n$ is a bijection.

To see that f is one-to-one, suppose $f(k \bmod m) = f(\ell \bmod n)$ Then $k \equiv \ell \bmod m$ and $k \equiv \ell \bmod n$, so since $(m, n) = 1$ (aha!), we have $k \equiv \ell \bmod mn$. That means $k = \ell$ in U_{mn}, so f is one-to-one.

Now we show f is onto. Pick any pair $(a \bmod m, b \bmod n) \in U_m \times U_n$. By the Chinese remainder theorem we can solve $c \equiv a \bmod m$ and $c \equiv b \bmod n$ for a $c \in \mathbf{Z}$. Is $(c, mn) = 1$? Since $a \bmod m$ is a unit and $c \equiv a \bmod m$, $c \bmod m$ is a unit so $(c, m) = 1$. Since $b \bmod n$ is a unit and $c \equiv b \bmod n$, $c \bmod n$ is a unit so $(c, n) = 1$. From $(c, m) = 1$ and $(c, n) = 1$ we get $(c, mn) = 1$, so $c \in U_{mn}$. From the congruence conditions on c, we have $f(c) = (a, b)$. $\square$

Corollary 3.2. *For a positive integer m,*

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right),$$

where the product runs over the primes p dividing m.

Proof. The formula is clear for $m = 1$ (interpreting an empty product as 1).

Now suppose $m > 1$, and factor m into prime powers:

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

The $p_i^{e_i}$'s are pairwise relatively prime. By an extension of Theorem 3.1 from two relatively prime terms to any number of pairwise relatively prime terms (just induct on the number of terms), we have

$$\varphi(m) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_r^{e_r}).$$

Now using the formula for φ on prime powers,

$$\begin{aligned} \varphi(m) &= p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \cdots p_r^{e_r-1}(p_r - 1) \\ &= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) p_2^{e_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{e_r}\left(1 - \frac{1}{p_r}\right) \\ &= m \prod_{p|m}\left(1 - \frac{1}{p}\right). \end{aligned}$$

□

Example 3.3. To compute $\varphi(540) = \varphi(2^2 \cdot 3^3 \cdot 5)$, we have

$$\begin{aligned} \varphi(540) &= 540\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) \\ &= 540 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \\ &= 18 \cdot 8 \\ &= 144. \end{aligned}$$

An alternate calculation is

$$\begin{aligned} \varphi(540) &= \varphi(4)\varphi(27)\varphi(5) \\ &= (4 - 2)(27 - 9)(5 - 1) \\ &= 2 \cdot 18 \cdot 4 \\ &= 144. \end{aligned}$$

We now leave units mod m and look at squares mod m.

Theorem 3.4. *For $m \in \mathbf{Z}^+$ with $m \geq 2$, let $S_m = \{x^2 \bmod m\}$ be the set of squares modulo m. When $(m, n) = 1$, $\#S_{mn} = \#S_m \cdot \#S_n$.*

Note S_m is *all* squares modulo m, including 0. So $S_5 = \{0, 1, 4\}$, for example.

Proof. This proof will be like that of Theorem 3.1, except we will get to use the Chinese remainder theorem *twice*.

If $a \equiv x^2 \bmod mn$ then $a \equiv x^2 \bmod m$ and $a \equiv x^2 \bmod n$. Thus any square modulo mn reduces to a square modulo m and a square modulo n. So we have a function $f\colon S_{mn} \to S_m \times S_n$ by $f(a \bmod mn) = (a \bmod m, a \bmod n)$. Let's take a look at an example.

Set $m = 3$ and $n = 5$, so $S_3 = \{0, 1\}$, $S_5 = \{0, 1, 4\}$ and $S_{15} = \{0, 1, 4, 6, 9, 10\}$. The table below gives the values of f on S_{15}. The values fill up $S_3 \times S_5$ without repetition.

$c \bmod 15$	$f(c \bmod 15)$
0	$(0, 0)$
1	$(1, 1)$
4	$(4, 4) = (1, 4)$
6	$(6, 6) = (0, 1)$
9	$(9, 9) = (0, 4)$
10	$(10, 10) = (1, 0)$

Returning to the general case, to show f is one-to-one let's suppose $f(c \bmod 15) = f(c' \bmod 15)$. Then $c \equiv c' \bmod 3$ and $c \equiv c' \bmod 5$, so $c \equiv c' \bmod 15$ since $(3, 5) = 1$. (This part is basically the same as the proof that the function in Theorem 3.1 is one-to-one.

To show f is onto, pick a pair of squares $b \bmod m$ and $c \bmod n$, say $b \equiv y^2 \bmod m$ and $c \equiv z^2 \bmod n$. By the Chinese remainder theorem, there is $a \in \mathbf{Z}$ satisfying

$$a \equiv b \bmod m, \quad a \equiv c \bmod n.$$

We want to say $f(a) = (b, c)$, but is $a \bmod mn$ a square? From the expressions for $b \bmod m$ and $c \bmod n$ as squares, $a \equiv y^2 \bmod m$ and $a \equiv z^2 \bmod n$, but y and z are not related to each other. They certainly don't have to be the same integer, so these two congruences on their own don't tell us $a \bmod mn$ is a square. Using the Chinese remainder theorem *again*, however, there is $x \in \mathbf{Z}$ such that

$$x \equiv y \bmod m, \quad x \equiv z \bmod n,$$

so $x^2 \equiv y^2 \bmod m$ and $x^2 \equiv z^2 \bmod n$. Therefore $a \equiv x^2 \bmod m$ and $a \equiv x^2 \bmod n$, so $a \equiv x^2 \bmod mn$, so $a \bmod mn$ is in fact a square and $f(a) = (b, c)$. $\square$

Example 3.5. For a prime p, the number of nonzero squares mod p is $(p - 1)/2$, so the total number of squares mod p is $1 + (p - 1)/2 = (p + 1)/2$. Thus $\#S_p = (p + 1)/2$. So if $n = p_1 p_2 \dots p_r$ is squarefree, $\#S_n = \#S_{p_1} \cdots \#S_{p_r} = \frac{p_1+1}{2} \cdots \frac{p_r+1}{2}$. If $n = p_1^{e_1} \cdots p_r^{e_r}$, we also have $\#S_n = \#S_{p_1^{e_1}} \cdots \#S_{p_r^{e_r}}$, but at the moment we don't have a formula for S_{p^e} when $e > 1$ so we don't get an explicit formula for $\#S_m$ as we have for $\varphi(m)$ (where we know a formula for $\varphi(p^e)$).

We turn now from counting all the squares mod m to counting how often something is a square mod m.

Example 3.6. We can write $1 \bmod 15$ as a square in *four* ways: $1 \equiv 1^2 \equiv 4^2 \equiv 9^2 \equiv 14^2 \bmod 15$.

Theorem 3.7. *Let $m \in \mathbf{Z}^+$ have prime factorization $p_1^{e_1} \cdots p_r^{e_r}$. For any integer a, the congruence $x^2 \equiv a \bmod m$ is solvable if and only if the separate congruences $x^2 \equiv a \bmod p_i^{e_i}$ are solvable for $i = 1, 2, \dots, r$.*

Furthermore, if the congruence $x^2 \equiv a \bmod p_i^{e_i}$ has N_i solutions, then the congruence $x^2 \equiv a \bmod m$ has $N_1 N_2 \cdots N_r$ solutions.

Example 3.8. The congruences $x^2 \equiv 1 \bmod 3$ and $x^2 \equiv 1 \bmod 5$ each have two solutions, so $x^2 \equiv 1 \bmod 15$ has $2 \cdot 2 = 4$ solutions; we saw the four square roots of 1 mod 15 before the statement of Theorem 3.7.

Proof. If $x \in \mathbf{Z}$ satisfies $x^2 \equiv a \bmod m$, then $x^2 \equiv a \bmod p_i^{e_i}$ for all i.

Conversely, suppose each of the congruences $x^2 \equiv a \bmod p_i^{e_i}$ has a solution, say $x_i^2 \equiv a \bmod p_i^{e_i}$ for some integers x_i. Since the $p_i^{e_i}$'s are pairwise relatively prime, the Chinese remainder theorem tells us there is an x such that $x \equiv x_i \bmod p_i^{e_i}$ for all i. Then $x^2 \equiv x_i^2 \bmod p_i^{e_i}$ for all i, so $x^2 \equiv a \bmod p_i^{e_i}$ for all i. Since $x^2 - a$ is divisible by each $p_i^{e_i}$ it is divisible by m, so $x^2 \equiv a \bmod m$.

To count the solutions modulo m, we again use the Chinese remainder theorem. Any choice of solution $x_i \bmod p_i^{e_i}$ for each i fits together in exactly one way to a number $x \bmod m$, and this number will satisfy $x^2 \equiv a \bmod m$. Therefore we can count solutions modulo m by counting solutions modulo each $p_i^{e_i}$ and multiplying the counts thanks to the independence of the choice of solutions for different primes. □

Example 3.9. To decide if 61 is a square modulo 75, we check whether 61 is a square modulo 3 and modulo 25. Since $61 \equiv 1 \bmod 3$, it is a square modulo 3. Since $61 \equiv 11 \equiv 6^2 \bmod 25$, it is a square modulo 25. Therefore 63 is a square modulo 75. In fact, we can get a square root by solving the congruences

$$x \equiv 1 \bmod 3, \quad x \equiv 6 \bmod 25.$$

A solution is $x = 31$, so $61 \equiv 31^2 \bmod 75$.

If you scrutinize the two previous proofs about squares mod m (how many squares there are and how often something is a square) to see why it was important we were working with squares, you'll see that it really wasn't; the only thing which really matters is that squaring is a polynomial expression. With this in mind, we get the following generalizations from squares to values of other polynomials.

Theorem 3.10. *Let $f(x)$ be any polynomial with integer coefficients. For a positive integer $m \geq 2$, let $N_f(m) = \#\{f(x) \bmod m : x \in \mathbf{Z}/(m)\}$ be the number of values of f on $\mathbf{Z}/(m)$. If m has prime factorization*

$$m = p_1^{e_1} \cdots p_r^{e_r},$$

we have $N_f(m) = N_f(p_1^{e_1}) \cdots N_f(p_r^{e_r})$.

Proof. Proceed as in the proof of Theorem 3.4, which is the special case $f(x) = x^2$. □

Theorem 3.11. *Let $f(x)$ be any polynomial with integer coefficients. For a positive integer m with prime factorization*

$$m = p_1^{e_1} \cdots p_r^{e_r},$$

the congruence $f(x) \equiv 0 \bmod m$ is solvable if and only if the congruences $f(x) \equiv 0 \bmod p_i^{e_i}$ are each solvable.

Moreover, if $f(x) \equiv 0 \bmod p_i^{e_i}$ has N_i solutions, then the congruence $f(x) \equiv 0 \bmod m$ has $N_1 N_2 \cdots N_r$ solutions.

Proof. Argue as in the proof of Theorem 3.7, which is the special case $f(x) = x^2 - a$. □

Theorem 3.11 tells us that finding solutions to a polynomial equation modulo positive integers is reduced by the Chinese remainder theorem to the case of understanding solutions modulo prime powers.

Consider now the following situation: $f(x)$ is a polynomial with integral coefficients and every value $f(n)$, for $n \in \mathbf{Z}$, is either a multiple of 2 or a multiple of 3. For instance, if $f(x) = x^2 - x$ then $f(n) = n^2 - n$ is even for all n. Or if $f(x) = x^3 - x$ then $f(n) = n^3 - n$ is a multiple of 3 for all n. But these examples are kind of weak: what about a mixed example where every $f(n)$ is a multiple of 2 or 3 but some $f(n)$ are multiples of 2 and not 3 while other $f(n)$ are multiples of 3 and not 2? Actually, no such polynomial exists! The only way $f(n)$ can be divisible either by 2 or 3 for all n is if it is a multiple of 2 for all n or a multiple of 3 for all n. To explain this, we will use the Chinese remainder theorem.

Theorem 3.12. *Let $f(x)$ be a polynomial with integral coefficients. Suppose there is a finite set of primes $p_1, \dots, p_r$ such that, for every integer n, $f(n)$ is divisible by some p_i. Then there is one p_i such that $p_i | f(n)$ for every $n \in \mathbf{Z}$.*

Proof. Suppose the conclusion is false. Then, for each p_i, there is an $a_i \in \mathbf{Z}$ such that p_i does not divide $f(a_i)$. Said differently, $f(a_i) \not\equiv 0 \bmod p_i$.

Since the p_i's are different primes, we can use the Chinese remainder theorem to find a single integer a such that $a \equiv a_i \bmod p_i$ for $i = 1, 2, \dots, r$. Then $f(a) \equiv f(a_i) \bmod p_i$ for $i = 1, 2, \dots, r$ (why?), so $f(a) \not\equiv 0 \bmod p_i$ for all i. However, the assumption in the theorem was that every value of the polynomial on integers is divisible by some p_i, so we have a contradiction. □

Remark 3.13. It is natural to believe an analogous result for divisibility by squares of primes. Specifically, if $f(x)$ is a polynomial with integral coefficients and there is a finite set of primes $p_1, \dots, p_r$ such that, for every integer n, $f(n)$ is divisible by some p_i^2, then there should be one p_i such that $p_i^2 | f(n)$ for every $n \in \mathbf{Z}$. If you try to adapt the proof of Theorem 3.12 to this setting, it breaks down (where?). While this analogue for divisibility by squares of primes is plausible, it is still an open problem as far as I am aware.

Our next application of the Chinese remainder theorem addresses the question of which moduli m could have a generator for the units modulo m.

Theorem 3.14. *If $m \neq 2, 4, p^e$, or $2p^e$ for odd prime p, the units modulo m do not have a generator.*

Proof. At the end of the handout on Euler's theorem, it is proved that when there is a generator for the units modulo m, the only square roots of 1 mod m are $\pm 1 \bmod m$. We will show that if $m \neq 2, 4, p^e$, or $2p^e$, there are additional square roots of 1 mod m, and thus there is no generator modulo m!

First suppose m is odd, so m is not an odd prime power. That means m has at least 2 odd prime factors, so we can write $m = m_1 m_2$ where $(m_1, m_2) = 1$ and $m_1 > 2$, $m_2 > 2$. (For example, let m_1 be one of the prime powers in the factorization of m and let m_2 be the rest of the prime factorization of m.)

Consider the congruences

$$x \equiv 1 \bmod m_1, \quad x \equiv -1 \bmod m_2. \tag{3.1}$$

There is a solution x to this system of congruences, since $(m_1, m_2) = 1$. Notice $x^2 \equiv 1 \bmod m_1$ and $x^2 \equiv 1 \bmod m_2$, so $x^2 \equiv 1 \bmod m_1 m_2$ (since $(m_1, m_2) = 1$). To see $x \not\equiv \pm 1 \bmod m$, suppose for instance that $x \equiv 1 \bmod m$. Then $x \equiv 1 \bmod m_2$, so $1 \equiv -1 \bmod m_2$ by (3.1), but $m_2 > 2$ so this is impossible. Thus, $x \not\equiv 1 \bmod m$. Similarly, $x \not\equiv -1 \bmod m$ since $m_1 > 2$. We have created with (3.1) an unexpected square root of 1 modulo m.

Now suppose m is even. First we treat m a power of 2. Since $m \neq 2$ or 4, $m = 2^k$ with $k \geq 3$. In this case we can write down additional square roots of 1 mod m explicitly: $1 < 2^{k-1}-1 < 2^k-1 < 2^k$ and $(2^{k-1}-1)^2 = 2^{2(k-1)}-2^k+1 \equiv 1 \bmod 2^k$, so $2^{k-1}-1 \bmod m$ is a square root of 1 mod m and is not $\pm 1 \bmod m$.

Now we treat m even and not a power of 2. Since $m \neq 2p^e$ with odd prime p, either $m = 2n$ or $m = 4n$ where $n > 1$ is odd and not a prime power, or $m = 2^k n$ where $k \geq 3$ and $n > 1$ is odd (perhaps here n is a prime power). If $m = 2n$ or $m = 4n$ with $n > 1$ odd and not a prime power then n has at least 2 prime factors. Write $n = p_1^{e_1} \cdots p_r^{e_r}$, so $r \geq 2$. Then m is $2p_1^{e_1} \cdots p_r^{e_r}$ or $4p_1^{e_1} \cdots p_r^{e_r}$, so we can write $m = m_1 m_2$ with $m_1 = 2p_1^{e_1}$ or $m_1 = 4p_1^{e_1}$ and $m_2 = p_2^{e_2} \cdots p_r^{e_r}$. Either way, m_1 and m_2 are relatively prime and $m_1 > 2$ and $m_2 > 2$, so we can create extra square roots of 1 mod m (that is, other than $\pm 1 \bmod m$) from the Chinese remainder theorem just as we did in the case of odd m. Our last case is $m = 2^k n$ with $k \geq 3$ and odd $n > 1$. Then $n \geq 3$, so $m = m_1 m_2$ where $m_1 = 2^k \geq 8$ and $m_2 = n \geq 3$, so once again we can construct extra square roots of 1 mod m from the Chinese remainder theorem in the same way we did for odd m. $\square$

In case the details in the proof got a bit overwhelming at the end, the key point is that when $m \neq 2, 4, p^e$, or $2p^e$ for odd prime p then either $m = 2^k$ with $k \geq 3$ or $m = m_1 m_2$ where $(m_1, m_2) = 1$ with $m_1 > 2$ and $m_2 > 2$. For both types of m extra square roots of 1 mod m can be found, either by a direct example when $m = 2^k$ or by the Chinese remainder theorem (solving (3.1)) in the other case.

Remark 3.15. We have shown that if there is a generator for the units modulo m then $m = 2, 4, p^e$, or $2p^e$. It turns out that when $m = 2, 4, p^e$ or $2p^e$ for an odd prime p that there *is* a generator for the units modulo m, but that requires a completely different argument (having nothing to do with the Chinese remainder theorem) and we don't get into it here.

Our final application of the Chinese remainder theorem is to an interpolation problem. Given n points in the plane, $(a_1, b_1), \ldots, (a_n, b_n)$, with the a_i's distinct, we would like to find a polynomial $f(T)$ in $\mathbf{R}[T]$ whose graph passes through these points: $f(a_i) = b_i$ for $i = 1, 2, \ldots, n$. This task can be converted to a set of simultaneous congruences in $\mathbf{R}[T]$, which can be solved using the Chinese remainder theorem in $\mathbf{R}[T]$, not $\mathbf{Z}$. First let's state the Chinese remainder theorem for polynomials.

Theorem 3.16. *For $r \geq 2$, let $m_1(T), m_2(T), \ldots, m_r(T)$ be nonzero polynomials in $\mathbf{R}[T]$ which are pairwise relatively prime: $(m_i(T), m_j(T)) = 1$ for $i \neq j$. Then, for any polynomials $a_1(T), a_2(T), \ldots, a_r(T)$, the system of congruences*

$$f(T) \equiv a_1(T) \bmod m_1(T), \quad f(T) \equiv a_2(T) \bmod m_2(T), \quad \ldots, \quad f(T) \equiv a_r(T) \bmod m_r(T),$$

has a solution $f(T)$ in $\mathbf{R}[T]$, and this solution is unique modulo $m_1(T)m_2(T) \cdots m_r(T)$.

The proof of this is identical to that of the Chinese remainder theorem for $\mathbf{Z}$, so we leave it to the reader as an exercise.

Theorem 3.17. *In $\mathbf{R}$, pick n distinct numbers $a_1, a_2, \ldots, a_n$ and any numbers $b_1, b_2, \ldots, b_n$. There is a unique polynomial $f(T)$ of degree $< n$ in $\mathbf{R}[T]$ such that $f(a_i) = b_i$ for all i.*

Proof. To say $f(a_i) = b_i$ is the same as $f(T) \equiv b_i \bmod T - a_i$ (why?). Consider the system of congruences

$$f(T) \equiv b_1 \bmod T - a_1, f(T) \equiv b_2 \bmod T - a_2, \ldots, f(T) \equiv b_n \bmod T - a_n$$

for an unknown $f(T)$ in $\mathbf{R}[T]$. Since the a_i's are *distinct*, the polynomials $T-a_1,\ldots,T-a_n$ are pairwise relatively prime in $\mathbf{R}[T]$. Therefore, by the Chinese remainder theorem in $\mathbf{R}[T]$, there is an $f(T)$ in $\mathbf{R}[T]$ satisfying all of the above congruences. It follows that $f(a_i)=b_i$ for all i.

We have no initial control over $\deg f$ for the common solution f. However, since we can adjust $f(T)$ modulo $(T-a_1)\cdots(T-a_n)$ without changing the congruence conditions, we can replace $f(T)$ with its remainder under division by $(T-a_1)\cdots(T-a_n)$, which has degree n. Then $\deg f < n$ with $f(a_i)=b_i$ for all i.

We have shown a desired $f(T)$ exists. To see it is unique, suppose $f_1(T)$ and $f_2(T)$ both have degree less than n and satisfy

$$f(T)\equiv b_1 \bmod T-a_1, f(T)\equiv b_2 \bmod T-a_2,\ldots,f(T)\equiv b_n \bmod T-a_n.$$

Then, by the uniqueness in the Chinese remainder theorem, we have

$$f_1(T)\equiv f_2(T) \bmod (T-a_1)\cdots(T-a_n).$$

Since $f_1(T)$ and $f_2(T)$ have degree less than n, this congruence modulo a polynomial of degree n implies $f_1(T)=f_2(T)$ in $\mathbf{R}[T]$. □

The fact that polynomial interpolation is identical to solving a system of polynomial congruences (with linear moduli) suggests that we should think about solving a system of integer congruences as *arithmetic* interpolation.

There is nothing essential about $\mathbf{R}$ in Theorem 3.17 except that it's a field. The Chinese remainder theorem goes through for $F[T]$ with F any field, not just $\mathbf{R}$, and Theorem 3.17 carries over to any field:

Theorem 3.18. *Let F be any field. For n distinct numbers $a_1,a_2,\ldots,a_n$ in F and any numbers $b_1,b_2,\ldots,b_n$ in F, there is a unique polynomial $f(T)$ of degree $<n$ in $F[T]$ such that $f(a_i)=b_i$ for all i.*

The proof is identical to that of Theorem 3.17.