The Chinese Remainder Theorem

The Chinese remainder theorem is an ancient artifact of mathematical knowledge. The oldest written record of it originates in ancient China (hence the name) by the mathematician Sun Tzu, not to be confused with the more famous general and author of *The Art of War*, whose name he shares. This theorem was also known to the ancient Indians and, much later, to some European mathematicians in the middle ages. It provides a criterion for the existence of solutions to multiple congruences, and an useful theorem with many applications in number theory and computer science, one of which we cover in the following sections.

We start by proving such a criterion for two congruences:

Theorem 1. *Suppose* $\gcd(m,n) = 1$. *Then the two congruences* $x \equiv a \pmod{m}$ *and* $x \equiv b \pmod{n}$ *have a unique solution mod* mn.

Proof. To satisfy the first equation, we must have $x = a + mt$ for some integer t. To satisfy the second equation we must have $x = a + mt \equiv b \pmod{n}$, or $mt \equiv b - a \pmod{n}$.

Since $\gcd(m,n) = 1$, m has a multiplicative inverse mod n, so we can determine t uniquely (up to mod n) by multiplying both sides by m^{-1} to get $t \equiv m^{-1}(b-a) \pmod{n}$. Let's say $t \equiv c \pmod{n}$. So there exists integer k such that $t = c + nk$.

So $x = a + m(c+nk) = (a+mc) + mnk$, i.e. $x \equiv a + mc \pmod{mn}$; this is a unique solution to the equations mod mn. □

Notice that this theorem gives us a constructive way of solving the simultaneous congruence itself. Given the two congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, all we need to do is to find $c \equiv m^{-1}(b-a) \pmod{n}$ and plug it into the formula $x \equiv a + mc \pmod{mn}$ to get all possible solutions to the equation.

Example 2. For instance, consider the congruences $x \equiv 3 \pmod{8}$ and $x \equiv 5 \pmod{9}$.

Then $x \equiv 3 + 8c \pmod{72}$, where $c \equiv 8^{-1}(5-3) \pmod{9}$. Noting that $8 \times 8 = 64 \equiv 1 \pmod{9}$, we know $8^{-1} \equiv 8 \pmod{9}$, so $c \equiv 8 \times 2 = 16 \equiv 7 \pmod{9}$. Therefore, it immediately follows that $x \equiv 3 + 8 \times 7 \equiv 59 \pmod{72}$.

We can easily generalize Theorem 1 to more than two recurrences:

Theorem 3. *Let* $m_1, \ldots, m_k$ *be pairwise relatively prime numbers. Then the k congruences* $x \equiv a_1 \pmod{m_1}$, ..., $x \equiv a_k \pmod{m_k}$ *have a unique solution mod* $m_1 m_2 \ldots m_k$.

Proof. By induction on k.

For the base case, let $k = 2$. In this case, the theorem reduces to Theorem 1, which we just proved above.

Now suppose for induction that the theorem holds for up to k congruences. It suffices to show that it holds for $k+1$ congruences as well.

Remove the $k+1$st equation. We have k equations remaining, which (by inductive hypothesis) must have a unique solution mod $m_1 m_2 \ldots m_k$, i.e. $x \equiv t \pmod{m_1 m_2 \ldots m_k}$ for some t.

Now add the last equation back. Since m_{k+1} is relatively prime to each of $m_1, \ldots, m_k$, it must also be relatively prime to their product $m_1 m_2 \ldots m_k$. So by the previous theorem, there is a unique solution mod $(m_1 m_2 \ldots m_k) m_{k+1}$. □

Square Roots in Modular Arithmetic

Since squaring (and, in fact, taking numbers to arbitrary powers) is easy in modular arithmetic, it is natural that we should extend the process of taking square roots to modular arithmetic as well. However, it is not always the case that a square root exists! For instance, consider the integers mod 5: $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 = 9 \equiv 4$, and $4^2 = 16 \equiv 1$. Only 0, 1, and 4 have square roots; the other numbers do not.

This should come as no surprise given that squaring is an even function; i.e. $x^2 = (-x)^2$. Except for those values whose square root satisfies $x \equiv -x \bmod n$ (just 0 and $n/2$ if n is even), all integers mod n must have two distinct square roots. That means that not all integers mod n can have a square root; otherwise, we'd have more square roots than numbers mod n!

The following criterion, whose proof follows directly from Fermat's little theorem, that tells us when a number has a square root mod some prime:

Theorem (Euler's Criterion): Suppose p is an odd prime and a is some integer relatively prime to p. Then $a^{(p-1)/2}$ is 1 (mod p) if and only if there exists some integer x such that $a \equiv x^2 \pmod{p}$ and -1 otherwise.

Proof. The proof for the "only if" direction is beyond the scope of this class. However, the proof for the if direction follows immediately from Fermat's little theorem:

$$a^{(p-1)/2} = (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 \pmod{p}.$$

On the other hand, if no such x exists, then we can write:

$$a^{p-1} = \left(a^{(p-1)/2} - 1\right)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p}.$$

Applying the "only if" direction of the theorem, we get that the first term cannot be congruent to zero. So the second term must be congruent to zero mod p, so $a^{(p-1)/2} + 1 \equiv 0 \pmod{p}$, or, equivalently, $a^{(p-1)/2} \equiv -1 \pmod{p}$, as desired. □

How do we find a square root if one exists? If $p \equiv 3 \pmod 4$, then we can find square roots easily. In fact, if the solutions to $x^2 \equiv a \pmod{p}$ are given by $x \equiv \pm a^{(p+1)/4} \pmod{p}$. To see why this is the case, square it and apply Euler's criterion to get:

$$(\pm a^{(p+1)/4})^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} a \equiv 1a \equiv a \pmod{p}.$$

Notice that this formula requires that $p \equiv 3 \pmod 4$ in order to ensure that the exponent $(p+1)/4$ is an integer.

Example 4. Is there a square root of 8 (mod 1)9. Calculating $8^9 \pmod{19}$, we get $8^9 \equiv 8((8^2)^2)^2 \equiv 8(64^2)^2 \equiv 8(7^2)^2 \equiv 8(49^2) \equiv 8(11^2) \equiv 8(121) \equiv 8(7) \equiv 56 \equiv 18 \equiv -1 \pmod{19}$ so there is no square root.

Other hand, repeating the same calculation with 9, we can see that $9^9 \equiv 1 \pmod{19}$, so it does indeed have a square root. Plugging it into this formula, we find that the square root is $9^{(19+1)/4} \equiv 9^5 \equiv 81 * 81 * 9 \equiv 5 * 5 * 9 \equiv 25 * 9 \equiv 6 * 9 \equiv 54 \equiv 16 \pmod{19}$. Notice that $16^2 = 256 = 19 * 13 + 9 \equiv 9 \pmod{19}$ so 16 is indeed a square root of 9 mod 19.

Remote Coin Flipping

In this section we cover a scheme for flipping a coin over the telephone, first postulated by Manuel Blum in 1982. The basic motivation is this: suppose Alex and David are betting on a coin toss. Alex wants heads to come up and David wants to see a tails.

If any one of them is responsible for performing the coin flip, then the other can accuse him of faking the result for his own gain. As a result, our goal is to find a way of performing this that each side can be assured that the coin flip is fair, without the need to trust each other (or another party).

Here's the procedure:

(1) Alex chooses distinct primes p, q congruent to 3 (mod 4), and computes $n = pq$. He sends n (but not p and q) to David.

(2) David chooses $x \in (0,n)$ relatively prime to n and sends $a = x^2 \pmod{n}$ to Alex.
(3) Alex, armed with knowledge of p, q, computes the square roots $\pm x, \pm y$ of a, mod n, and sends one to David.
(4) If David got $\pm x$, then he says Alex guessed correctly. Otherwise, if he gets $\pm y$, he can factor n and use that to prove that he won.

Why does this work? Alex has no idea whether David chose x or y, so he has a $1/2$ chance of picking x.

If David got $\pm y$: he now has two different square roots of $a \pmod{n}$. Now he can use this to factor n . How? Since $x^2 \equiv a \equiv y^2 \pmod{n}$ (with x, y distinct), $pq|(x+y)(x-y)$, so each prime divides either $(x+y)$ or $(x-y)$ but not both. Furthermore, pq cannot divide $x-y$ or $x+y$ (since $\pm x$ and $\pm y$ are all distinct mod pq), so p must divide either $x-y$ or $x+y$ and q must divide the other.

Therefore, we can find p and q by evaluating $\gcd(x+y,n)$ and $\gcd(x-y,n)$: one will be p and the other is q. All David has to do to factor $n = pq$ is to compute $x^2 - y^2 = (x+y)(x-y)$ and run EGCD twice! Now he can present p and q to Alex to prove that he won.

If David got $\pm x$, he's learned nothing new. The only information he has is n (since he was the one who chose x, and therefore, a) so if he were to factor n, he would have to do so with just the value of n and no additional information. Since we believe integer factorization to be hard, David can't do this.

After the game is over each side can verify the other's honesty: David asks Alex for the factors p, q to make sure they're Blum integers and check that they're primes congruent to $3 \pmod{4}$.

Example 5. Suppose that Alex chooses $p = 3$ and $q = 7$. He sends $n = 21$ to David.

David chooses $x = 1$ and sends $a \equiv x^2 \equiv 1 \pmod{21}$ back to Alex.

Alex now knows that $x^2 \equiv 1 \pmod{3}$ (so $x \equiv \pm 1 \pmod{3}$, or, equivalently, $x \equiv 1$ or $2 \pmod{3}$) and $x^2 \equiv 1 \pmod{7}$ (so $x \equiv \pm 1 \pmod{7}$, or, equivalently, $x \equiv 1$ or $6 \pmod{7}$). There are four ways to put these two congruences together:

$$\begin{aligned}
x &\equiv 1 \pmod{3} \quad \text{and} \quad x \equiv 1 \pmod{7} \\
x &\equiv 1 \pmod{3} \quad \text{and} \quad x \equiv 6 \pmod{7} \\
x &\equiv 2 \pmod{3} \quad \text{and} \quad x \equiv 1 \pmod{7} \\
x &\equiv 2 \pmod{3} \quad \text{and} \quad x \equiv 6 \pmod{7}
\end{aligned}$$

Solving this set of equations (using the same method as we did in Example 2), we get $x \equiv \pm 1$ (i.e. 1 or 20) or ± 8 (i.e. 8 or 13) mod 21.

Alex picks one of these four numbers to send to David. If he sends 8 or 13, David (who chose 1) can write $21|(8-1)(8+1)$. Taking $\gcd(21, 8-1) = 7$ he manages to recover one factor, and taking $\gcd(21, 8+1) = 3$ (or just dividing 21 by 7, now that he knows one factor) he can recover the other factor. He then ships 3 and 7 to Alex as proof that he won the game.

On the other hand, if Alex sends 1 or 20, David has no choice to concede defeat, since all he knows is that $n = 21$; the value of x that he got back is just what what he set Alex (or its negation), and he has no information to help him factor n. If he attempts to cheat and claim victory, Alex can challenge him to send back p and q. Since factoring is hard (and David has no information to help him perform the factorization), he will not be able to, revealing the deception.