RSA and the Chinese remainder theorem

The Chinese remainder theorem

Suppose we have a system of simultaneous equations, like maybe this one:

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 5 \pmod 7 \end{aligned}$$

What can we say about x? Well, notice that one solution is $x = 12$; $x = 12$ satisfies both equations. This is not the only solution: for instance, $x = 12 + 35$ also works, as does $x = 12 + 70$, $x = 12 + 105$, and so on. Evidently adding any multiple of 35 to any solution gives another valid solution, so we might as well summarize this state of affairs by saying that $x \equiv 12 \pmod{35}$ is one solution of the above system of equations.

What about other solutions? For this example, there are no other solutions; every solution is of the form $x \equiv 12 \pmod{35}$. Why not? Well, suppose x and x' are two valid solutions. From the first equation, we know that $x \equiv 2 \pmod 5$ and $x' \equiv 2 \pmod 5$, so we must have $x \equiv x' \pmod 5$. Similarly $x \equiv x' \pmod 7$. But the former means that 5 is a divisor of $x - x'$, and the latter means that 7 is a divisor of $x - x'$, so $x - x'$ must be a multiple of 35 (here we have used that $\gcd(5,7) = 1$), which in turn means that $x \equiv x' \pmod{35}$. In other words, all solutions are the same modulo 35: or, equivalently, if all we care about is $x \bmod 35$, the solution is unique.

You can check that the same would be true if we replaced the numbers $5,7,2,5$ above by any others. The only thing we used is that $\gcd(5,7) = 1$.

Here is the generalization:

Theorem 12.1: *(The Chinese remainder theorem.) Let m,n be relatively prime, and let a,b be arbitrary. Then the pair of equations $x \equiv a \pmod m$, $x \equiv b \pmod n$ have a unique solution for $x \bmod mn$.*

Moreover, the solution x can be computed efficiently (as an exercise, you can check how to do so).

The Chinese remainder theorem is often useful when doing modular arithmetic with a composite modulus; if we want to compute some unknown value modulo mn, a standard trick is to compute it modulo m, compute it modulo n, and then deduce its value mn using the Chinese remainder theorem (CRT).

Euler's theorem

In last lecture, we saw Fermat's little theorem, which tells us something about what happens with exponentiation when the modulus is prime. We can generalize a little bit to the case where we're working modulo a product of two primes.

Theorem 12.2: *Let p,q be two distinct primes. Let $n = pq$. Then $x^{(p-1)(q-1)} \equiv 1 \pmod n$ for all x satisfying* $\gcd(x,n) = 1$.

Proof: First, let's reduce both sides modulo p. (This is permitted, since p divides n.) We find that

$$x^{(p-1)(q-1)} \equiv \left(x^{p-1}\right)^{q-1} \equiv (1)^{q-1} \equiv 1 \pmod{p},$$

where we used Fermat's little theorem to conclude that $x^{p-1} \equiv 1 \pmod{p}$. Similarly, we have $x^{(p-1)(q-1)} \equiv 1 \pmod{q}$. This gives us a system of two equations:

$$\begin{aligned} x^{(p-1)(q-1)} &\equiv 1 \pmod{p} \\ x^{(p-1)(q-1)} &\equiv 1 \pmod{q} \end{aligned}$$

Note that $\gcd(p,q) = 1$. Therefore, by the Chinese remainder theorem, there must exist a unique solution for $x^{(p-1)(q-1)} \pmod{pq}$. We can see that $x^{(p-1)(q-1)} \equiv 1 \pmod{pq}$ is one possible solution, and since the solution is unique, this must be the only possibility. The theorem follows. □

Let's recap. Fermat's little theorem tells us that $x^{p-1} \equiv 1 \pmod{p}$, and we just saw that $x^{(p-1)(q-1)} \equiv 1 \pmod{pq}$. What's the general pattern here? Where did those magical exponents come from? Is there some relationship of $p-1$ to p and $(p-1)(q-1)$ to pq that generalizes? Yes, there is.

The concept we need is that of *Euler's totient function*, $\varphi(n)$. The number $\varphi(n)$ is defined to be the number of positive integers less than n and relatively prime to n. We can see that $\varphi(p) = p-1$ when p is prime, because the integers $1, 2, \ldots, p-1$ are all less than p and relatively prime to p. With a little bit of counting, we can also determine $\varphi(n)$ when $n = pq$ is a product of two primes, and we get the following:

Lemma 12.1: *Let p, q be two distinct primes, and $n = pq$. Then $\varphi(n) = (p-1)(q-1)$.*

Proof: How many integers are less than n and relatively prime to n? Well, the integers $p, 2p, 3p, \ldots, (q-1)p$ don't count (they share a common factor with n). The integers $q, 2q, 3q, \ldots, (p-1)q$ don't count, either. However, these are the only exceptions, and these two lists of exceptions are disjoint, so when we eliminate these exceptions from the $n-1$ positive integers less than n, what remains is what we want. Finally, the first list contains $q-1$ exceptions, and the second list contains $p-1$ exceptions. Therefore, there are $n-1-(p-1)-(q-1) = pq-p-q+1 = (p-1)(q-1)$ positive integers less than and relatively prime to n. □

At this point, it is natural to conjecture that the Euler totient function will lead the way to a generalization of Fermat's little theorem. And indeed, we can prove the following result:

Theorem 12.3: *(Euler's Theorem.)* $x^{\varphi(n)} \equiv 1 \pmod{n}$ *for all x satisfying* $\gcd(x,n) = 1$.

Proof: The proof will be just like that of Fermat's little theorem. Consider the set Φ of positive integers less than n and relatively prime to n. If we pick each of the elements of Φ by x, we get another set $\Phi_x = \{ix \bmod n : i \in \Phi\}$. Note that all the elements of Φ_x are distinct (since x is invertible) and relatively prime to n, hence $\Phi = \Phi_x$. Therefore, the products $\prod_{i \in \Phi} i$ and $\prod_{i \in \Phi_x} i$ are equal modulo n. But $\prod_{i \in \Phi_x} i \equiv x^{|\Phi|} \prod_{i \in \Phi} i \pmod{n}$, hence $x^{|\Phi|} \equiv 1 \pmod{n}$. Finally, noting that $|\Phi| = \varphi(n)$, the theorem follows. □

You can check that Fermat's little theorem is a special case of Euler's theorem.

RSA

Finally, using Euler's theorem, I will give a proof that RSA works correctly (i.e., decrypting a RSA-encrypted message gives you back the original message).

We let $n = pq$ be the product of two primes and e be a number with $\gcd(e, \varphi(n)) = 1$, so that the RSA public key is given by the pair (n, e). Recall that the encryption of a message m is defined as follows:

$$e(m) \equiv m^e \pmod{n}.$$

Similarly, the decryption of a ciphertext c is defined as:

$$d(c) \equiv c^d \pmod{n}$$

where $d \equiv e^{-1} \pmod{\varphi(n)}$. We will prove that decryption is the inverse of encryption, This will ensure that the receiver can recover the original encrypted message using his private key, as should be the case for a good encryption scheme.

Theorem 12.4: $d(e(m)) \equiv m \pmod{n}$ *whenever* $\gcd(m,n) = 1$.

Proof: Recall that $e \equiv d^{-1} \pmod{\varphi(n)}$, so $ed \equiv 1 \pmod{\varphi(n)}$, or in other words, $ed - 1$ is a multiple of $\varphi(n)$; say, $k\varphi(n)$. Then we can calculate:

$$d(e(m)) \equiv (m^e)^d \equiv m^{ed} \equiv m^{1+k\varphi(n)} \equiv m \cdot (m^{\varphi(n)})^k \equiv m \cdot 1^k \equiv m \pmod{n}$$

where here we have used Euler's theorem to conclude that $m^{\varphi(n)} \equiv 1 \pmod{n}$. $\square$