Eventually going to do Public Key Cryptography

For us to get there, we have to learn some number theory.

Fundamental Theorem of Arithmetic states that each positive integer has a unique prime factorization. Prime numbers are positive integers greater than 1 that are only divisible by 1 and themselves.

\[ 35 = 5 \times 7 \]
\[ 48 = 2^4 \times 3 \]
\[ 74 = 2 \times 37 \]

In general, for any integer, we can express its prime factorization as \( \prod_{p_i \in \text{Primes}} p_i^{a_i} \).

(1) Fermat’s Theorem
(2) Values that share no common factor with an integer \( n \).
(3) Euler’s Theorem
(4) Prime number testing

Fermat’s Theorem: For any prime number \( p \) and integer \( a \) such that \( \gcd(a, p) = 1 \), \( a^{p-1} = 1 \mod p \)

For example, let \( a = 5 \), \( p = 7 \), then \( 5^6 = 1 \mod 7 \)

\( p = 101 \), \( a = 47 \), \( 47^{100} = 1 \mod p \)

Consider the set of values \( \{1, 2, 3, \ldots, p-1\} \). Call this set \( S \).

Create a new set of values \( \{1, 2a, 3a, 4a, \ldots, (p-1)a\} \) Call this set \( T \).

\( A = 5 \) and \( p = 7 \)

\( S = \{1,2,3,4,5,6\} \)

\( T = \{5,10,15,20,25,30\} \)

If we were to reduce all the values in \( T \mod p \) (mod 7 for this case), then the set \( T \) would equal the set \( S \).

\( T' = \{5, 3, 1, 6, 4, 2\} \) (This is the same set of values as \( S \!\! \) !)

How many possible mods are there mod \( p \)? \( p \) possible mods, \( 1 \) of which is \( 0 \).

The set \( S \) contains ALL possible mods except \( 0 \).

If we can prove that none of the mods in set \( T \) are 0 and that none of the mods in set \( T \) equal each other, then we have proven that the set \( T \), when modded by \( p \) is the same as the set \( S \).

First, let’s prove that \( T \) doesn’t contain a value equal to 0 mod \( p \).
The values in $T$ are $a$, $2a$, $3a$, ..., $(p-1)a$. None of these numbers has a factor of $p$ because $\gcd(a, p) = 1$ and the other factors are $1, 2, 3, ..., p-1$, so there is no multiple of $p$ in this list either.

Now, we must show that no two values in the set $T$ are equivalent to one other mod $p$:

$$\{a, 2a, 3a, \ldots, (p-1)a\}$$

Proof by contradiction: Assume the opposite that two values in the set are equivalent mod $p$. Let these values be $a_i$ and $a_j$, where $0 < i, j < p$, $i \neq j$, since we picked distinct values in the list.

$$a_i = a_j \pmod{p}$$

$$a_i - a_j = 0 \pmod{p}$$

$$a(i-j) = 0 \pmod{p}$$

if something is $0 \pmod{p}$, then $p$ divides evenly into it.

So, $p \mid (a(i-j))$.

Does $p \mid a$ or does $p$ even share any common factors with $a$? NO – it was given that $\gcd(a, p) = 1$

So this means that $p \mid (i-j)$. But this is impossible because $0 < |i - j| < p-1$. We’ve reached a contradiction, which means our initial assumption was incorrect. But if that was incorrect, we can conclude that no two values on the list are equivalent mod $p$.

So, if sets $S$ and $T$ are equal sets under mod $p$, then if we were to take the product of the values in both sets, they HAVE TO BE equivalent mod $p$!

$$\prod_{i=1}^{p-1} a_i \equiv \prod_{i=1}^{p-1} i \pmod{p}$$

$$\prod_{i=1}^{p-1} a_i - \prod_{i=1}^{p-1} i \equiv 0 \pmod{p}$$

$$a^{p-1} \prod_{i=1}^{p-1} i - \prod_{i=1}^{p-1} i \equiv 0 \pmod{p}$$

$$(a^{p-1} - 1) \prod_{i=1}^{p-1} i \equiv 0 \pmod{p}$$

$$(a^{p-1} - 1)(p-1)! \equiv 0 \pmod{p}$$

Since $p$ is prime, this means that either $p \mid (a^{p-1} - 1)$, or $p \mid (p-1)!$. 

p | (p − 1)! is false because p is prime and can’t divide into any integer smaller than p, but (p-1)!, when prime factorized only has integers smaller than p.

So if that’s false, what has to be true?

p | (a^{p-1} − 1)

\[ a^{p-1} − 1 \equiv 0 \pmod{p} \]

\[ a^{p-1} \equiv 1 \pmod{p} \]

**One big lesson:** there is cyclic behavior in modular exponentiation whenever we calculate our mod with a prime, that cycle length is guaranteed to be p-1, or less.

Euler wondered, can we get a similar formula for all integers?

2^{14} \mod 15, you might not get 1…but what if there was a different exponent for which this would work?

Euler’s goal: if \gcd(a, n) = 1, and n is any integer, what power do I have to raise a to, in order to obtain 1 \mod n, a^2 = 1 \pmod{n}. What is ??

Try making these sets for let’s say n=9, a=5

S = {1,2,3,4,5,6,7,8}, these two numbers share a common factor with 9

T = {5,10,15,20,25,30,35,40}, these share a common factor with 9

What made this proof work for Fermat is that the two sets S and T were equivalent sets mod p. But now, if we share a common factor, proving this equivalence becomes harder…Maybe two numbers in the set could be the same…

Euler said…let’s take these numbers out:

If n = 9, a=5, don’t put anything in the set S that shares a common factor with 9:

S = \{1,2,4,5,7,8\}

T = \{5,10,20,25,35,40\} = \{5,1,2,7,8,4\}

N=20, S = \{1,3,7,9,11,13,17,19\} a = 9

T = \{9, 3*9, 7*9, 9*9, 11*9, 13*9, 17*9, 19*9\} = \{9, 7, 3, 1, 19, 17, 13, 11\}

Euler then wanted to show that these new sets S and T, when considered mod n were the same sets.

So, Euler had to give a name to his new set S. He defined S as follows:
Let S be the set of all integers in between 1 and n-1, that share no common factors with n. This set is called a reduced residue set mod n.

Natural question: How many values does this set have, in terms of n?

The answer to this question was discovered by Euler, and the answer is called the Euler Phi Function. Thus, \( \phi(n) \) = the number of integers in the set \{1,2,3,…..,n-1\} that do NOT share a common factor with n.

We know for primes p, \( \phi(p) = p - 1 \).

How about for an integer \( n = pq \), where p and q are both primes?

Example n = 5 x 7 = 35

\[
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
8 & 9 & 10 & 11 & 12 & 13 & 14 \\
15 & 16 & 17 & 18 & 19 & 20 & 24 \\
22 & 23 & 24 & 25 & 26 & 27 & 28 \\
29 & 30 & 31 & 32 & 33 & 34 & 35 \\
\end{array}
\]

But I want to cross out all the numbers that have a factor of 5 or 7.

In this example, we see that there is precisely one multiple of 5 per column.

If this observation is true in general, then the number of values we cross off would be \( p + q - 1 \).

\[
\phi(pq) = pq - (p + q - 1) = pq - p - q + 1 = (p - 1)(q - 1)
\]

This turns out to be true and we’ll prove it next time.