Euler's Theorem and Application to Public Key Cryptography
Olivia Hartzell
orh2106

Preliminary Assumptions:
1). $gcd(a, b) = 1 \longrightarrow \exists m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

2). gcd(a,s) =1 and gcd(b,s) =1 $\longrightarrow$ gcd(ab, s) =1

3). define congruence mod n:
$a \equiv b \mod n$ if $n|(a - b)$, i.e. $\exists i \in \mathbb{Z}$ such that $ni = a - b$.

Let $\Phi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ be a function, where $\Phi(n)$ denotes the number of integers k, $0 \leq k < n$ which are relatively prime to n, i.e. gcd(n, k) =1.

Lemma 1: Let a, n be integers satisfying $n > 1$ and $gcd(a, n) = 1$. If r, s $\in \mathbb{Z}$, and $ar \equiv as \mod n$, then $r \equiv s \mod n$

Proof:
Since gcd(a, n)=1, $\exists m, k \in \mathbb{Z}$ such that $ma + kn = 1$ by assumption 1. Therefore, $\exists m$ such that $ma \equiv 1 \mod n$.
Consider $ar \equiv as \mod n$
$mar \equiv mas \mod n$
$(ma)r \equiv (ma)s \mod n$
$1r \equiv 1s \mod n$
Therefore, $r \equiv s \mod n$.

Lemma 2: Let a, n be integers satisfying $n > 1$ and gcd(a, n)=1. Then, there exist exactly $\Phi(n)$ distinct integers $m_1, m_2, ..., m_{\phi}(n)$ such that:
i) $0 \leq m_i < n$ and gcd(m_i, n) =1, $\forall_i$ =1, ..., $\phi(n)$.

ii) $\exists c \in \mathbb{Z}$ such that $\prod_{i=1}^{\phi(n)} m_i c \equiv 1 \mod$ n.

iii) $am_i \not\equiv am_j \mod n$ for $i \not\equiv j$.

Proof:
By definition of Φ : there exist exactly $\phi(n)$ distinct integers satisfying i). By assumption 2, gcd$(a, s) = 1$, and gcd$(b, s) = 1$, implies gcd$(ab, s) = 1$. Then, gcd$(\prod_{i=1}^{\phi(n)} m_i, n) = 1$.
Therefore, $\exists c, l \in \mathbb{Z}$ such that $c(\prod_{i=1}^{\phi(n)})m_i + nl = 1$, and $\prod_{i=1}^{\phi(n)} m_i c \equiv 1 \mod n$. Therefore, ii) holds.
Since $m_1, .., m_{\phi}(n)$ are all distinct and $gcd(a, n) = 1$, if $i \neq j$,
then $m_i \not\equiv m_j \mod n$. Therefore, $am_i \not\equiv am_j \mod n$ for $i \not\equiv j$.

Euler's Theorem: let $a, n \in \mathbb{Z}, n > 1$. If $gcd(a, n) = 1$:

$$a^{\phi(n)} \equiv 1 \mod n$$

(Note: if n is prime, $\phi(n) = n - 1 \Longrightarrow a^{n-1} \equiv 1 \mod n$)

Proof:
$m_1, ..., m_{\phi(n)}$ are distinct integers, thus $am_1, ..., am_{\phi(n)}$ are distinct integers mod n, and $gcd(m_i, n) = 1 \forall i$.

Since there are $\phi(n)$ integers,

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} m_i = \prod_{i=1}^{\phi(n)} (am_i)$$

We want to find: $\prod_{i=1}^{\phi(n)}(am_i)$

There must exist integers $s_1, ..., s_{\phi(n)}$ such that $s_i \equiv m_i a \mod n$ where $0 \leq s_i < n$.
We know $gcd(a, n) = 1$ and $gcd(m_i, n) = 1$, therefore $gcd(am_i, n) = 1$ (by assumption 2) and thus, $gcd(s_i, n) = 1$.
There are $\phi(n)$ distinct integers relatively prime to n, so $s_1, ..., s_{\phi(n)}$ is a possible re-ordering of $m_1, ..., m_{\phi(n)}$, in which case:

$$\prod_{i=1}^{\phi(n)}(am_i) \equiv \prod_{i=1}^{\phi(n)}(s_i) \equiv \prod_{i=1}^{\phi(n)}(m_i) \mod n$$

.

Therefore,

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)}(m_i) \equiv \prod_{i=1}^{\phi(n)}(m_i) \mod n$$

.

by Lemma 2, $\exists c \in \mathbb{Z}$ such that

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)}(m_i)c \equiv \prod_{i=1}^{\phi(n)}(m_i)c \equiv 1 \mod n$$

.

Therefore,

$$a^{\phi(n)} \equiv 1 \mod n$$

.

Application to Public Key Cryptography
The main idea: Oftentimes, we want to send secure messages, which are easy for the intended receiver to decode, but are difficult for others to decode (i.e. we may wish to send our credit card number over the internet).

Suppose our message is translated into a positive integer m. The receiver chooses a number n, which is the product of two prime numbers, say p_1, p_2.

The receiver chooses an integer e, such that $\gcd(e, \phi(n)) = 1$. The sender then sends $m^e \mod n$. n and e are both public.

Claim: Given $\phi(n)$, one can find a d such that $(m^e)^d \equiv \mathrm{m} \mod n$. Therefore, if given $\phi(n)$, m^e, n, one can uncover m, the message of interest.

Proof:

if $\gcd(m, n) = 1$, then $m^{\phi(n)} \equiv 1 \mod n$, by Euler's Theorem.
Also, since $gcd(e, \phi(n)) = 1$, $\exists k, l \in \mathbb{Z}$ such that $ke + l\phi(n) = 1$ (by assumption 1). These integers can be found by Euclid's Algorithm.
Therefore,

$$m^{ke} \equiv m^{1-l\phi(n)} \mod n$$

$$m^{ke} \equiv m(m^{\phi(n)^{-l}}) \mod n$$

$$m^{ke} \equiv m \mod n$$

Let d be the smallest integer such that $d \equiv k \mod \phi(n)$. Then, $ke \equiv 1 \mod \phi(n) \longrightarrow de \equiv 1 \mod \phi(n)$.
Then, by the above, $m^{de} \equiv m \mod n$.

The key step in this method is to choose an n which is the product of two primes p_1, p_2 such that it is easy for the receiver to compute $\phi(n)$, but not easy for anyone else.

For any $n = p_1 p_2$, Every integer $z < n$ is relatively prime to n, except for:

$$cp_1, \forall 1 \leq c \leq p_2 - 1$$

$$kp_2, \forall 1 \leq k \leq p_1 - 1$$

So, $\Phi(p_1 p_2) = (p_1 p_2 - 1) - (p_2 - 1) - (p_1 - 1)$ Therefore, $\Phi(n) = (p_1 - 1)(p_2 - 1)$

If one chooses n to be sufficiently large, (currently standard practice utilizes each prime at about 300 digits long), it is impossible for outsiders to factor n and compute $\phi(n)$, but easy for the receiver to compute.

1