The Euler-Fermat theorem and RSA cryptography

Lorenzo Rota

March 20, 2019

Abstract

Fermat's little theorem states that for any prime integer and non-multiple integer of the prime, the integer raised to the power of the prime - 1 in the prime modulo has a remainder of 1. Euler's theorem is a generalisation that takes two integers which are relatively prime, and considers the totient of the modulo as the exponent. This consequently led to a functioning design of the RSA cryptography algorithm. In this paper, both theorems and the correctness of the algorithm will be proved in an elegant manner.

1 Introduction

Fermat's little theorem, as the name suggests, was thought to have originally been discovered by Fermat, and later proven by Euler. The idea of the theorem is that one can find two integers: an integer which is prime, call it p, and an integer which is not a multiple of p, call it a. Taking the exponent $p-1$ of the base a is said to always have the remainder of 1 when dividing it by the prime number p. A simple and useful application of Fermat's little theorem, is indicating whether a number is a probable prime (as in some cases, the remainder will still be 1 for non-primes).

Euler discovered a stronger notion of the same theorem, which generalises over all numbers which are relatively prime. This is known as Euler's totient theorem, which is a fundamentally used in the RSA crypto-system.

In order to formalise both theorems and demonstrate its application, it is crucial to first define the basic notions of modular congruence. First let us define divisibility of two integers as follows:

Definition 1.1. *For any $n, m \in \mathbb{Z} \setminus \{0\}$, n is said to be divisible by m, denoted $m|n$, if and only if $mk = n$, for some constant $k \in \mathbb{Z} \setminus \{0\}$*

Next, we define what it means for two integers to be relatively prime:

Definition 1.2. *For any $n, m \in \mathbb{Z} \setminus \{0\}$, m and n are relatively prime, denoted $m \perp n$ or $n \perp m$, if and only if the gcd$(m, n) = 1$*

It is also important to note that $\gcd(m, n) = 1 \iff m \not\equiv 0 \pmod{n}$ $\iff m \nmid n$. The middle equivalence utilises the notion of modular congruence, which we can define as follows:

Definition 1.3. *Let $x, y, z \in \mathbb{Z}$. We can define modular congruence as $x \equiv y \ (mod\ z)$, if and only if $z|(x - y)$*

Here it is clear that for x to be equivalent to $y \pmod{z}$, the difference must be divisible by z. This is then also equivalent to $x \pmod{z} = y \pmod{z}$. We can now formalise Fermat's little theorem as follows:

Theorem 1.4 (Fermat's little theorem)**.** *For any $a \in \mathbb{Z}$, which is relatively prime with the prime number p, then $a^{p-1} \equiv 1 \ (mod\ p)$*

Expanding on the brief introduction, a stronger notion of Fermat's theorem is the Euler theorem, which considers two relatively prime integers that are not necessarily prime themselves. This requires the use of the so-called totient function:

Definition 1.5. *The Euler totient function $\varphi(n)$, is the number of positive integers less than or equal to n, which are relatively prime to n.*

The Totient function can also be defined as the cardinality of a set of relatively prime integers $\leq$ n: $\varphi(n) := |\{a \in \mathbb{Z} : 1 \leq a \leq n,\ \gcd(a, n) = 1\}|$. The theorem is thus stated as follows:

Theorem 1.6 (Euler's theorem)**.** *For any $a, n \in \mathbb{Z}^+$ and $n \geq 2$ which are relatively prime, then $a^{\varphi(n)} \equiv 1 \ (mod\ n)$*

In the next section both theorems will be proved and understood, but for now it is assumed that they are indeed true. Before elaborating on the importance of Euler's theorem in the RSA-cryptography algorithm, we first need to look at a property that arises from the totient function:

Proposition 1.7. *For $p, q \in \mathbb{Z}$ prime, then $\varphi(pq) = \varphi(p)\varphi(q)$*

The proof is simple, and goes as follows:

Proof. The composition pq can be expressed in terms of either the multiples of p or q:

(i) $p,\ 2p,\ \ldots,\ (q-1)p,\ qp$

(ii) $q,\ 2q,\ \ldots,\ (p-1)q,\ pq$

From this, we know that there are exactly $p+q-1$ multiples of pq, where we exclude the last multiple of itself as we only want to count it once. From the definition of $\varphi(pq)$, we count the number of positive integers $\leq pq$ which are relatively prime to pq, thus:
$\varphi(pq) = pq - (p+q-1) = (p-1)(q-1) = \varphi(p)\varphi(q)$ □

RSA cryptography works through the means of public and private key distribution (usually of a particular size). The algorithm can be outlined as follows:
Generating the keys (Receiver):

- Let $n := pq$ where $p, q \in \mathbb{Z}^+$ prime
- Let $e \in \mathbb{Z}^+$ be odd, such that e and $\varphi(n)$ are relatively prime
- Find $d \in \mathbb{Z}$, such that $ed \equiv 1 \pmod{\varphi(n)}$
- Let `public-key` $:= (e, n)$ and `private-key` $:= (d, n)$

Encryption (Sender): uses `public-key`

- Let the message to be encrypted be $M \in \mathbb{Z}$ and ensure $2 \leq M \leq n$.
- Let $M' :\equiv M^e \pmod{n}$ be the newly encrypted message

Decryption (Receiver): uses `private-key`

- Compute $(M')^d \equiv M^{ed} \pmod{n}$
- Since $M^{ed} \equiv M \pmod{n}$, the original message M is retrieved

This results in the following theorem, which will be proved in the next section:

Theorem 1.8 (RSA)**.** *Let $n := pq$ where $p, q \in \mathbb{Z}^+$ are prime. For some $e \in \mathbb{Z}^+$. $\exists d \in \mathbb{Z}$ such that $ed \equiv 1 \pmod{\varphi(n)}$, then $M^{ed} \equiv M \pmod{n}$*

2 Proof of the Euler-Fermat theorem and correctness of the RSA algorithm

We will first prove Fermat's little theorem (Theorem 1.4) with the use of two properties:

Property 2.1 (Addition/Multiplication)**.** *For $a, b, x, y \in \mathbb{Z}$, if $a \equiv b$ and $x \equiv y$, then $a \pm x \equiv b \pm y$ and $ax \equiv by$*

Property 2.2 (Cancellation)**.** *For $a, b, x, y, m \in \mathbb{Z}$, if $ax \equiv by$, $a \equiv b$ and a, m are relatively prime, then $x \equiv y \pmod{m}$*

The second property can be proven as follows:

$$\begin{aligned}
& ax - by \equiv 0 \pmod{m} && \\
\iff\ & a(x-y) \equiv 0 \pmod{m} && (a \equiv b) \\
\iff\ & a(x-y) = km && (k \in \mathbb{Z}) \\
\implies\ & x - y = km && (\gcd(a, m) = 1) \\
\iff\ & x \equiv y \pmod{m} &&
\end{aligned}$$

Fermat's little theorem can then be proved as follows:

Proof. Consider the set of residues of $a \pmod{p}$ to be defined as $S := \{0, 1, 2, \ldots, (p-1)\}$, which contains p multiples of a. Since each residue forms an equivalence class when $ax \pmod{p} = ay \pmod{p} \implies ax \equiv ay \pmod{p} \implies x \equiv y \pmod{p}$ as $\gcd(a, p) = 1$ by the cancellation property. This allows us to choose any two integers from the same residue class, and by the multiplicative property we can multiply between elements from all the residue classes (excluding 0):

$$\begin{aligned}
& as \equiv s \pmod{p} && (s \in S) \\
\implies\ & (a) \cdot (2a) \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p} && \text{(Property 2.1)} \\
\implies\ & a^{p-1}(p-1)! \equiv (p-1)! \pmod{p} && \\
\implies\ & a^{p-1} \equiv 1 \pmod{p} && \text{(Property 2.2)}
\end{aligned}$$

The last step is true because the factorial of $p - 1$ must be relatively prime to p as it contains no factors of p □

The proof of Euler's theorem (Theorem 1.6) works in a similar fashion, but first let us define the set of integers which are relatively prime to some integer n as: $U_n := \{a \pmod{n} : \gcd(a, n)\}$. Since this follows from the definition of $\varphi(n)$, we say that $|U_n| = \varphi(n)$. The proof then goes as follows:

Proof. Consider the set of residues of $a \pmod{n}$ to be defined as $S := \{u_1, u_2, \ldots, u_{\varphi(n)}\}$, where $u_i \in U_n$ and $1 \leq i \leq \varphi(n)$. Since u_i represents the residue class, and $\gcd(a, n) = 1$, we argue similarly that $x \equiv y \pmod{n}$ for numbers from the same residue class. Thus:

$$\begin{aligned} & as \equiv s \pmod{p} && (s \in S) \\ \implies & (au_1) \cdot (au_2) \cdot \ldots \cdot (au_{\varphi(n)}) \equiv u_1 \cdot u_2 \cdot \ldots \cdot u_{\varphi(n)} \pmod{n} && \text{(Property 2.1)} \\ \implies & a^{\varphi(n)}(u_1 \cdot u_2 \cdot \ldots \cdot u_{\varphi(n)}) \equiv u_1 \cdot u_2 \cdot \ldots \cdot u_{\varphi(n)} \pmod{n} && \\ \implies & a^{\varphi(n)} \equiv 1 \pmod{n} && \text{(Property 2.2)} \end{aligned}$$

The last step is clearly true, because all u_i are relatively prime to n, thus their product must also be relatively prime and therefore the cancellation property holds □

The last proof will prove the correctness of the RSA algorithm; in particular Theorem 1.8. This requires the use of the Chinese remainder theorem (for which the proof will be omitted)

Theorem 2.3. *Let $p, q \in \mathbb{Z}^+$ be relatively prime, and $x, y \in \mathbb{Z}$. Then there exists $M \in \mathbb{Z}$ such that:*

$$\begin{aligned} M &\equiv x \pmod{p} \\ M &\equiv y \pmod{q} \end{aligned}$$

where $M \pmod{pq}$ has a unique solution.

The proof that $M^{ed} \equiv M \pmod{n}$ goes as follows:

Proof. Since $n := pq$, and p, q are both prime, by Theorem 2.3 it suffices to show that $M^{ed} \equiv M \pmod{p}$ and $M^{ed} \equiv M \pmod{q}$. Since both p and q are prime, it will be shown for one prime number (i.e. p). If M is divisible by p, then it is trivially true since $M \equiv 0 \pmod{n}$. If M is relatively prime to p, consider the following: Since $ed \equiv 1 \pmod{\varphi(n)}$, then $\exists k \in \mathbb{Z}$ such that $ed - 1 = k\varphi(n)$, where $\varphi(n) = \varphi(p)\varphi(q)$:

$$\begin{aligned} M^{ed} &\equiv M^{1+k\varphi(p)\varphi(q)} \\ &\equiv M(M^{\varphi(p)})^{k\varphi(q)} \\ &\equiv M1^{k\varphi(q)} && \text{(Theorem 1.6)} \\ &\equiv M \pmod{p} \\ &\equiv M \pmod{n} && \text{(Theorem 2.3)} \end{aligned}$$

□

References

[1] Keith Conrad. *Euler's theorem*. URL: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/eulerthm.pdf.

[2] Andreas Klappenecker. *The RSA Public-Key Cryptosystem*. URL: http://faculty.cs.tamu.edu/klappi/csce222-s11/rsa.pdf.

[3] Donald Ervin Knuth. *The Art of Computer Programming, Vol. 1: Fundamental Algorithms*. 3rd. Addison-Wesley, 1968, pp. 39–41. ISBN: 9780201896831.

[4] Eric W. Weisstein. *Residue Class*. URL: http://mathworld.wolfram.com/ResidueClass.html.