Codici Correttori e Crittografia: Pseudoprimi di Fermat, Funzione λ e Numeri di Carmichael

Vittorio Valent

9 aprile 2017

Introduzione

In crittografia è fondamentale la ricerca di numeri *primi* a molte cifre: la grande maggioranza della crittografia a chiave pubblica (PKC) si basa infatti sulla difficoltà di fattorizzare *semiprimi* molto grandi, cioè numeri che sono il prodotto di due soli fattori primi. Numerosi problemi legati alla crittografia sono facilmente risolvibili nella teoria (come ad esempio fattorizzazione o la risoluzione di equazioni quadratiche modulari), ma essi diventano difficilmente computabili in tempi ragionevoli quando i numeri in considerazione sono dell'ordine di 300 cifre decimali (1024 bit). Il problema della fattorizzazione è quindi complesso da risolvere nella pratica e gli algoritmi per scomporre numeri grandi in fattori primi sono molto lenti.Per quanto riguarda i numeri primi, esistono invece diversi test per verificare la primalità di un numero: uno dei più semplici è il test di Fermat.

1 Test di Fermat e Pseudoprimi di Fermat

Teorema (Piccolo Teorema di Fermat)**.** *Sia $p \in \mathbb{Z}$ primo, allora per ogni $a \in \mathbb{Z}_p$ si ha che $a^p \equiv a \ (mod\ p)$ o, equivalentemente, per ogni $a \in \mathbb{Z}_p^*$, ossia per ogni a tale che $(a, p) = 1$, si ha che $a^{p-1} \equiv 1 \ (mod\ p)$.*

Grazie a questo teorema possiamo definire un test di primalità, detto *Test di Fermat*, il quale prende un numero n e verifica se, dato un $a \in \mathbb{Z}_n^*$, $a^{n-1} \equiv 1 \ (mod\ n)$. Se il test è negativo si ha che n è certamente composto. Se il test risulta positivo allora diciamo che n è *probabilmente primo di Fermat in base a*. I numeri probabilmente primi di Fermat in base a di dividono a

loro volta in due categorie: i numeri che sono effettivamente primi e i numeri composti che passano ugualmente il test. Questi ultimi si dicono *pseudoprimi di Fermat in base a*.

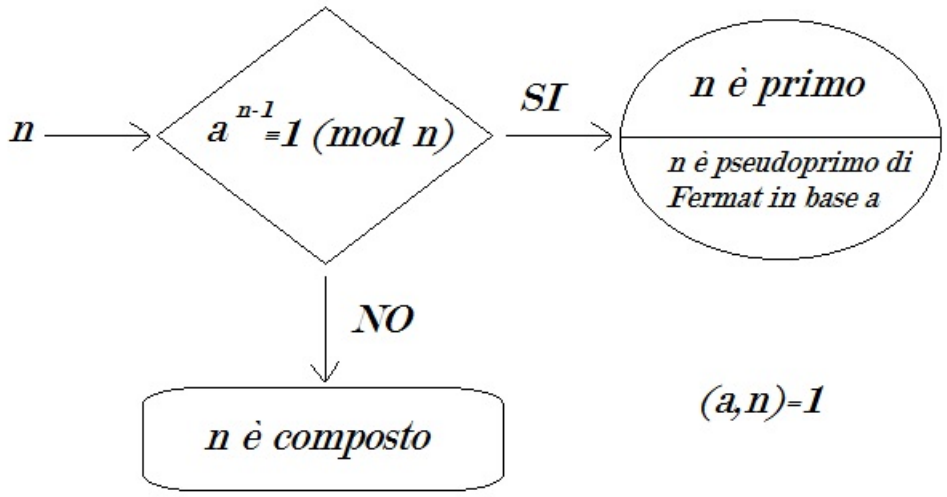

Figura 1: Test di Fermat

2 Funzione λ di Carmichael

Definizione. Sia $n \in \mathbb{N} \setminus \{0\}$ e sia $n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$ la sua scomposizione in fattori primi. Si definisce la funzione $\lambda(n)$ di Carmichael nel seguente modo:

$$\begin{cases} \lambda : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{Z} \\ \lambda : n \longmapsto mcm\{\varphi(p_i^{e_i})\} \end{cases}$$

dove mcm indica il minimo comune multiplo in $\mathbb{Z}$ e φ denota la funzione di Eulero che a ogni n associa il numero degli interi compresi tra 1 e n coprimi con n.

Si ha inoltre che $\lambda(n)$ è l'esponente di $\mathbb{Z}_n^*$, cioè è il minimo comune multiplo dei periodi di ogni elemento di $\mathbb{Z}_n^*$, infatti $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{e_k}}^*$. Con p_i dispari si ha che $|Z_{p_i^{e_i}}| = \varphi(p_i^{e_i}) = p_i^{e_i} - p_i^{e_i-1} = p_i^{e_i-1}(p_i - 1)$, perciò $\lambda(n) = mcm\{\varphi(p_i^{e_i})\} = mcm\{p_i^{e_i-1}(p_i - 1)\}$. Se $n = 2^m$ si ha che $\lambda(n) = 2^{m-2}$, se $m = 1, 2$ allora $\lambda(n) = \varphi(n)$.

Osservazione. Se $n = pq$ con p e q primi, allora $\lambda(n) = mcm\{\varphi(p), \varphi(q)\} =$
$= mcm\{(p-1), (q-1)\} = \frac{(p-1)(q-1)}{(p-1,q-1)} = \frac{\varphi(n)}{(p-1,q-1)}$.

Proprietà. (della funzione di Carmichael)

1. Se $a|b$ allora $\lambda(a)|\lambda(b)$;
2. $\lambda(ab) = mcm\{\lambda(a), \lambda(b)\}$;
3. Se $k^m \equiv 1 \ (mod\ n)$ e $m \leqslant \lambda(n)$ allora $m|\lambda(n)$

3 Numeri di Carmichael

Definizione. Sia $n \in \mathbb{Z}$ composto. Se $a^{n-1} \equiv 1 \ (mod\ n)\ \forall a \in \mathbb{Z}_n^*$ diciamo che n è un **numero di Carmichael**.

Osservazione. Un numero di Carmichael è necessariamente dispari, infatti dato n pari si ha che $(n-1)^{n-1} \equiv (-1)^{n-1} \ (mod\ n) \equiv -1$ poiché $n-1$ è dispari. Supponendo $n \neq 2$ si ha che $(n-1)^{n-1} \equiv -1 \ (mod\ n) \neq 1$, allora, dato che $(n-1, n) = 1$, n non è un numero di Carmichael.

Teorema (di caratterizzazione dei numeri di Carmichael)**.** *Sia $n \in \mathbb{N}$, allora sono equivalenti:*

1. *n è un numero di Carmichael*
2. *$n = p_1 \cdot \ldots \cdot p_k$ e $\forall i \in \{1, \ldots, k\}$ $p_i | n-1$*
3. *$\lambda(n)|n-1$ dove λ è la funzione di Carmichael*

Dimostrazione. **1⇒2:** sia $n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$, n dispari ($p_i \neq 2\ \forall i$). Si ha che $\forall\ i\ \mathbb{Z}_{p_i^{e_i}}^*$ è ciclico, pertanto esiste, per ogni i, un $a_i \in \mathbb{Z}_{p_i^{e_i}}^*$ tale che $\langle a_i \rangle = \mathbb{Z}_{p_i^{e_i}}^*$. Inoltre $per_{\mathbb{Z}_{p_i^{e_i}}^*}(a_i) = \varphi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$. Per il Teorema Cinese dei Resti si ha che esiste a (unico $(mod\ n)$) tale che $a \equiv a_i \ (mod\ p_i^{e_i})\ \forall i$ e con $(a, n) = 1$. Per ipotesi $a^{n-1} \equiv 1 \ (mod\ n)\ \forall a \in \mathbb{Z}_n^*$. Poiché $n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$ per tutti gli i si ha che $p_i | n$. Allora $\forall i \in \{1, \ldots, k\}\ a^{n-1} \equiv 1 \ (mod\ p_i^{e_i})$ e di conseguenza $a_i^{n-1} \equiv 1 \ (mod\ p_i^{e_i})$, perciò $\forall i \in \{1, \ldots, k\}\ p_i^{e_i-1}(p_i - 1) | n-1$. Ma $p_i \nmid n-1$, pertanto deve essere che $p_i^{e_i-1} = 1 \Leftrightarrow e_i = 1\ \forall i \in \{1, \ldots, k\}$. Quindi $\forall i \in \{1, \ldots, k\}$ si ha che $n = p_1 \cdot \ldots \cdot p_k$ e $p_i | n-1$.

2⇒3: Se $n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$, allora $\lambda(n) = mcm\{\varphi(p_i)\} = mcm\{p-1\}$. Poichè $\forall i \in \{1, \ldots, k\}\ p_i | n-1$ si ha che $mcm\{p-1\} | n-1$, quindi $\lambda(n) | n-1$.

3⇒1: Sia a tale che $(a, n) = 1$. Per ipotesi $n - 1 = k\lambda(n)$, quindi $a^{n-1} = a^{k\lambda(n)} = (a^{\lambda(n)})^k \equiv 1 \ (mod\ n)$ ($\lambda(n)$ è l'esponente di $\mathbb{Z}_n^*$).
n è pertanto un numero di Carmichael. □

Corollario. *Un numero di Carmichael è prodotto di almeno 3 fattori primi, cioè non può essere un semiprimo.*

Dimostrazione. Sia $n = pq$ un numero di Carmichael, con $p < q$ primi. $q \equiv 1 \ (mod\ q-1) \Rightarrow pq \equiv p \ (mod\ q-1) \Rightarrow pq - 1 \equiv p - 1 \ (mod\ q-1) \Rightarrow n - 1 \equiv p - 1 \ (mod\ q-1)$. Poichè n è di Carmichael so che $q-1|n-1$, quindi $n - 1 \equiv 0 \ (mod\ q-1)$, quindi anche $p - 1 \equiv 0 \ (mod\ q-1)$ e pertanto $q - 1|p - 1 \Rightarrow q \leqslant p$. Ma questo è assurdo, avendo supposto $p < q$. □

Proposizione. *$n \in \mathbb{N}$ è di Carmichael se e solo se $\forall a \in \mathbb{Z}\ a^n \equiv a \ (mod\ n)$*

Dimostrazione. Se n è di Carmichael allora $n = p_1 \cdot \ldots \cdot p_k$ e $\forall i \in \{1, \ldots, k\}\ p_i | n - 1$. Sia $a \in \mathbb{Z}$ e sia i fissato. Si ha che $p_i | a$ oppure $p_i \nmid a$. Se $p_i | a$ allora $a \equiv 0 \ (mod\ p_i) \Rightarrow a^n \equiv 0 \ (mod\ p_i) \Rightarrow a^n \equiv a \ (mod\ p_i)$. Se $p_i \nmid a$ allora $(a, p_i) = 1$ e $ap - 1 \equiv 0 \ (mod\ p_i) \Rightarrow an - 1 \equiv 0 \ (mod\ p_i) \Rightarrow a^n \equiv a \ (mod\ p_i)$. Quindi per ogni i si ha che $p_i | a^n - a$, pertanto $mcm\{p_i\} | a^n - a \Rightarrow n | a^n - a \Rightarrow a^n \equiv a \ (mod\ n)$.

Viceversa sia $n \in \mathbb{N}$, a tale che $(a, n) = 1$, cioè $a \in \mathbb{Z}_n^*$. Poichè a è invertibile modulo n si ha che $a^n \equiv a \ (mod\ n) \Leftrightarrow a^{n-1} \equiv 1 \ (mod\ n)$. Allora n è di Carmichael.

□

Conclusioni

Si evince, da quanto detto sopra, che il Test di Fermat non offre una risposta matematicamente certa sulla primalità di un numero. Esso quindi, pur avendo il vantaggio di essere un test molto semplice e facilmente computabile, non è un test di primalità efficiente. Le falle del test di Fermat offrono però la possibilità di studiare i numeri di Carmichael e le loro affascinanti proprietà. Questo mostra che in matematica, nello specifico in crittografia, i problemi più semplici possono portare a soluzioni complesse e ad applicazioni pratiche efficaci.