Un interessante risvolto applicativo del piccolo Teorema di Fermat: il metodo di crittografia RSA

Consideriamo due numeri primi distinti p e q, e prendiamo un numero e che sia primo con $(p-1)(q-1)$. Sappiamo dunque che e è invertibile modulo $(p-1)(q-1)$, e chiamiamo d un suo inverso.

La seguente semplice proposizione è il cuore del metodo di crittografia che vogliamo descrivere:

Proposizione 0.1. *Dati p, q, e, d come sopra, per ogni numero m con $0 \leq m < pq$ vale*

$$(m^e)^d \equiv m \quad (pq)$$

Dimostrazione. Osserviamo che per il teorema cinese del resto l'equazione

$$x \equiv m \quad (pq)$$

è equivalente al sistema

$$\begin{cases} x & \equiv & m & (p) \\ x & \equiv & m & (q) \end{cases}$$

Dunque ci basta dimostrare che $(m^e)^d$ è una soluzione del sistema.

Verifichiamo che $(m^e)^d$ è soluzione della prima equazione (per la seconda equazione si procederà in maniera del tutto analoga), ossia verifichiamo che è vera la congruenza:

$$(m^e)^d \equiv m \quad (p)$$

Ora, se $p|m$ la congruenza appena scritta diventa $0 \equiv 0 \quad (p)$ che è vera.

Se invece $p \nmid m$ allora possiamo applicare il piccolo teorema di Fermat. Infatti per costruzione

$$ed \equiv 1 \qquad ((p-1)(q-1))$$

dunque possiamo scrivere

$$ed = 1 + k(p-1)(q-1)$$

per un certo intero k.

Allora

$$(m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} = m \cdot (m^{p-1})^{k(q-1)} \equiv m \cdot 1^{k(q-1)} \equiv m \quad (p)$$

dove abbiamo usato il piccolo teorema di Fermat per dire che $m^{p-1} \equiv 1 \quad (p)$.

□

Nel 1977 Ronald Rivest, Adi Shamir e Leonard Adleman inventarono un metodo (detto RSA dalle iniziali dei loro cognomi) per scambiarsi messaggi criptati il cui funzionamento può essere schematicamente riassunto nel seguente modo.[1]

Supponiamo che A voglia inviare un messaggio segreto a B (non occorre pensare a chissà quali contesti di spionaggio e controspionaggio, A per esempio potremmo essere noi mentre digitiamo il codice della nostra carta di credito per fare un acquisto online).

Innanzitutto B ha scelto due numeri primi distinti p e q molto grandi (attualmente si scelgono numeri di circa trecento cifre: osserviamo che la ricerca di numeri primi grandi è un problema matematico di per sé interessante, che ha dunque anche una importante applicazione).

Visto che conosce p e q, B conosce anche $p-1$ e $q-1$ e può dunque facilmente scegliere e e d con le caratteristiche illustrate in questo paragrafo.

[1] Per coloro che sono interessati ad una introduzione divulgativa (non tecnica) alla storia della crittografia fin dalle origini, segnalo il libro di S. Singh *Codici e Segreti*.

A questo punto B consegna ad A i numeri pq ed e. Anzi, li può addirittura rendere pubblici, in modo che altri possano inviargli messaggi crittati, non solo A.

Quando A vuole inviare un messaggio, questo messaggio può essere facilmente codificato da un numero m con $0 < m < pq$ (se è un messaggio numerico è già un numero, se è un messaggio con lettere, si può certo trovare un modo di associare ad ogni lettera un numero, dunque il messaggio finale risulterà un numero m, magari molto grande, ottenuto scrivendo uno accanto all'altro tutti i numeri che rappresentano le lettere).[2]

A questo punto A non invia il numero m, ma calcola m^e modulo pq e invia dunque un numero c con $0 < c < pq$ e $c \equiv m^e \quad (pq)$.

Dunque B riceve il messaggio c. Per decodificarlo calcolerà c^d modulo pq e, per la Proposizione 0.1, ritroverà il messaggio originale m.

Come mai questo sistema è efficace? Ricordiamo che solo B conosce il numero d, e il punto è proprio questo. Il numero d è stato ricavato da e e dalla conoscenza dei numeri $p-1$ e $q-1$, mentre sono pubblici solo i numeri e e il **prodotto** pq. Per ricavare $p-1$ e $q-1$ conoscendo il prodotto pq bisognerebbe saper fattorizzare pq, e questa è una operazione che, al giorno d'oggi, con numeri così grandi, non è possibile eseguire in tempo utile. E non esiste per il momento neppure nessun altro metodo che permetta, dato un numero c che sappiamo essere congruo modulo pq ad una potenza e-esima di un certo numero ignoto, di ritrovare in tempo utile questo numero ignoto.[3]

In questa breve dispensina abbiamo dato una prima descrizione schematica del metodo RSA, senza discutere le molte accortezze tecniche che occorre usare nella pratica e i molti possibili approfondimenti, che non competono a questo corso ma ad un corso di crittografia. Ad ogni modo, una volta che viene applicato con tutte le accortezze del caso, il metodo RSA è ritenuto molto affidabile.

Abbiamo fatto solo un primo accenno alle complesse problematiche della crittografia, ma è interessante sapere che un teorema di aritmetica elementare, semplice ma profondo, come il piccolo teorema di Fermat, ha ripercussioni applicative così importanti.

[2]Ricordiamo che pq è molto grande, dunque c'è spazio per codificare anche messaggi molto lunghi. Altrimenti A dovrà spezzare il suo messaggio e inviare vari numeri m_1, m_2 etc...

[3]Se siete curiosi potete dare un'occhiata all'articolo di Rivest e Kaliski *RSA problem*, https://people.csail.mit.edu/rivest/RivestKaliski-RSAProblem.pdf