Universita' degli studi di Roma "Tor Vergata"
Teoria della sicurezza e crittografia

Author: Marcello Politi, Samir Salman, Angelo Silvestri

Novembre 2019

1 Piccolo Teorema di Fermat

Il piccolo teorema di Fermat afferma che:

$$a^p \equiv a(mod\, p) \tag{1}$$

per ogni numero primo p e intero a

1.1 Proof

È da notare che basta provare:
$a^{p-1} \equiv 1 \pmod p$ per ogni intero a coprimo con p. Moltiplicando ambo i membri dell'ultima espressione per a si ottiene la versione esposta a inizio pagina del teorema. Se a non fosse primo con p allora $a^p \equiv 0 \equiv a \pmod p$ ed il teorema risulterebbe vero in ogni caso.

Sfrutteremo quindi la semplificazione sopra riportata. Si considerino i multipli di a che vanno da a stesso fino a $(p-1)a$.
Nessuno di questi multipli può dare resto 0 diviso per p perché né $p-1$ né a sono multipli interi di p. Inoltre non può esistere una coppia di questi multipli che sia congrua modulo p, perché, se fosse per esempio:
$ra \equiv sa \pmod p$
si avrebbe
$(r-s)a \equiv 0 \pmod p$

Ma questo è impossibile, perché allora p dovrebbe dividere uno dei due fattori. Ma a è primo con p, e $r-s$, essendo r ed s numeri naturali compresi tra 1 e p, è $(r-s) < p$.

Per cui i multipli considerati hanno un resto nella divisione per p differente per ciascuno di essi, e differente da 0. Siccome consideriamo $p-1$ multipli, tali multipli devono essere necessariamente congrui (modulo p) ai numeri $1, 2, 3, \ldots, p-1$ in un certo ordine. Ne segue, per il prodotto di tutti questi multipli:
$a(2a)(3a)...(p-1)a = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod p$

da cui, ponendo $K = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)$, si ha
$K(a^{p-1} - 1) \equiv 0 \pmod{p}$.

Dato che p è primo, l'unico modo affinché ciò avvenga è che o K o il secondo fattore sia divisibile per p. (con p primo le classi di modulo n costituiscono un dominio di integrità).
Ma K non è divisibile per p, perché non lo è nessuno dei suoi fattori; quindi deve essere:
$a^{p-1} - 1 \equiv 0 \pmod{p}$.