Crittografia ed Aritmetica Modulare
LABORATORIO del VI incontro
– con Soluzioni –

PLS - CAM

Padova, 21 novembre 2014

Ricordiamo dapprima i tre importanti risultati della prima sezione:

Teorema 1.1 (PICCOLO TEOREMA DI FERMAT)**.** *Sia p un intero primo e sia $\overline{0} \neq \overline{a} \in \mathbb{Z}_p$. Allora*

$$\overline{a}^{\,p-1} = \overline{1} \quad in \quad \mathbb{Z}_p.$$

Corollario1.2. *Sia p un intero primo e sia $a \in \mathbb{Z}$. Allora*

$$a^p \equiv a \mod p.$$

Teorema 1.3 (TEOREMA DI EULERO-FERMAT)**.** *Sia n un arbitrario intero positivo e sia $\overline{a}$ invertibile in $\mathbb{Z}_n$. Allora $\overline{a}^{\,\varphi(n)} = \overline{1}$ in $\mathbb{Z}_n$.*

ATTIVITÀ 1.4. *Alcune semplici riflessioni sui precedenti risultati.*

- *Il Piccolo Teorema di Fermat è un immediato corollario del Teorema di Eulero-Fermat. Infatti ...*
- *Il* Corollario 1.2 *è di fatto del tutto equivalente al* Teorema 1.1. *Assumete come ipotesi l'enunciato di* 1.2 *e fornite una dimostrazione di* 1.1.

Svolgimento. i) Se nel Teorema di Eulero-Fermat scegliamo quale intero n un primo p, allora la condizione che $\overline{a}$ sia invertibile in $\mathbb{Z}_n$ si traduce esattamente nella condizione che $\overline{a} \neq \overline{0} \in \mathbb{Z}_p$, e vale l'identità $\varphi(n) = p - 1$.

ii) Se $\overline{a} \neq \overline{0} \in \mathbb{Z}_p$, cioè se p non divide a, allora dall'ipotesi che p divida $a^p - a = a(a^{p-1} - 1)$ segue subito che p divide $(a^{p-1} - 1)$, essendo p primo. Dunque $\overline{a}^{p-1} = \overline{1}$ in $\mathbb{Z}_p$. ∎

HOMEWORK 1.5. *Seguendo la stessa linea dimostrativa del* Piccolo Teorema di Fermat*, con $\varphi(n)$ in luogo di $p-1$, si dimostri il* Teorema di Eulero-Fermat.

Svolgimento. Siano $\overline{u_1}, \ldots, \overline{u_{\varphi(n)}}$ le distinte classi invertibili in $\mathbb{Z}_n$. Consideriamo il sottoinsieme di $\mathbb{Z}_n$

$$\left\{\overline{u_1 a}, \overline{u_2 a}, \ldots, \overline{u_{\varphi(n)} a}\right\}. \qquad (*)$$

Poiché $\overline{a}$ è invertibile in $\mathbb{Z}_n$, questi elementi sono tra loro distinti. Infatti se $\overline{u_i a} = \overline{u_j a}$, moltiplicando per $\overline{a}^{-1}$ otteniamo che $\overline{u_i} = \overline{u_j}$, ed allora anche $i = j$. Inoltre ciascuno di questi elementi è invertibile in $\mathbb{Z}_n$, poiché è prodotto di due invertibili. Ne segue che l'insieme (*) coincide con

$$\left\{\overline{u_1}, \overline{u_2}, \ldots, \overline{u_{\varphi(n)}}\right\},$$

ed allora vi è uguaglianza del prodotto degli elementi, cioè

$$\overline{u_1 u_2 \ldots u_{\varphi(n)}}\ \overline{a}^{\,\varphi(n)} = \overline{u_1 u_2 \ldots u_{\varphi(n)}} \qquad (**)$$

Ora $\overline{u_1 u_2 \ldots u_{\varphi(n)}}$ è una classe invertibile in $\mathbb{Z}_n$, in quanto prodotto di classi invertibili. Così moltiplicando entrambi i membri dell'uguaglianza (**) per l'inverso di $\overline{u_1 u_2 \ldots u_{\varphi(n)}}$ si ottiene $\overline{a}^{\,\varphi(n)} = \overline{1}$, che è la tesi. ∎

Ricordiamo ora la fondamentale applicazione dei precedenti risultati al metodo RSA:

Corollario 2.1. *Sia $n = p_1\, p_2\, \ldots, p_t$, con p_i interi primi* **distinti**. *Siano e, f interi positivi tali che $ef \equiv 1 \mod \varphi(n)$. Allora*

$$\overline{a}^{\,ef} = \overline{a} \quad in \quad \mathbb{Z}_n$$

qualunque sia $\overline{a} \in \mathbb{Z}_n$.

ATTIVITÀ 2.3. *Siamo sicuri che a messaggi distinti corrispondano versioni cifrate distinte? In altre parole, l'applicazione*

$$\mathbb{Z}_n \to \mathbb{Z}_n, \quad \overline{X} \mapsto \overline{X}^{\,e}$$

è iniettiva?

Svolgimento. L'applicazione è iniettiva, poiché se $\overline{X}, \overline{Y} \in \mathbb{Z}_n$ sono tali per cui le loro cifrature $\overline{X}^{\,e} = \overline{Y}^{\,e}$ coincidono, allora applicando l'elevazione ad f si vede che, grazie al Corollario 2.1,

$$\overline{X} = \overline{X}^{\,ef} = \left(\overline{X}^{\,e}\right)^f = \left(\overline{Y}^{\,e}\right)^f = \overline{Y}^{\,ef} = \overline{Y}$$

∎

ATTIVITÀ 2.4. *Proviamo ad applicare il metodo descritto nel* Corollario RSA *ad un caso estremamente semplice. Supponiamo di voler cifrare/decifrare in modo monoalfabetico (cioè carattere per carattere) un testo privo di spazi, associando ad ogni lettera dell'alfabeto italiano la sua posizione d'ordine.*

- *I caratteri sono identificati con una classe di* $\mathbb{Z}_n$*, con* $n = 21$*.*
- *In questo caso* $\varphi(n) = \varphi(21) = \varphi(3 \cdot 7) = 2 \cdot 6 = 12$*. Si scelga* $1 < e < 12$ *con* $(12, e) = 1$*. Sia* $1 < f < 12$ *tale che* $ef \equiv 1 \mod 12$ *(NB: qui accade sempre che* $e = f$ *!)*
- *Si scelga un testo italiano privo di spazi, e lo si codifichi carattere per carattere applicando* $\overline{X} \mapsto \overline{X}^{\,e}$*.*
- *Si applichi* $\overline{Y} \mapsto \overline{Y}^{\,f}$ *ai caratteri del testo in codice per riottenere il testo in chiaro.*

Svolgimento. In $\mathbb{Z}_{12}$ le classi invertibili $\neq \overline{1}$ sono $\overline{5}$, $\overline{7}$ e $\overline{11}$, e ciascuna di queste coincide con la propria inversa. Converrà scegliere $e = f = 5$ ed un testo breve, ad esempio "MARIO", che diviene la "$\overline{11}\ \overline{1}\ \overline{16}\ \overline{9}\ \overline{13}$". Applicando l'elevazione ad $e = 5$ in $\mathbb{Z}_{21}$ si ottiene il codice cifrato

$$\overline{11}^{\,5}\ \overline{1}^{\,5}\ \overline{16}^{\,5}\ \overline{9}^{\,5}\ \overline{13}^{\,5} = \overline{2}\ \overline{1}\ \overline{4}\ \overline{18}\ \overline{13}$$

che corrisponde alla parola "BADTO". Per decifrare, dovremo elevare alla $f = 5$, riottenendo quindi in $\mathbb{Z}_{21}$

$$\overline{2}^{\,5}\ \overline{1}^{\,5}\ \overline{4}^{\,5}\ \overline{18}^{\,5}\ \overline{13}^{\,5} = \overline{11}\ \overline{1}\ \overline{16}\ \overline{9}\ \overline{13}$$

cioè, nuovamente, "MARIO". ∎

ATTIVITÀ 3.1. *Supponiamo che siano assegnati sia* n *(= intero prodotto di due primi) che* m *(= numero dei caratteri dell'alfabeto). Qual è la massima lunghezza* l *(= numero dei caratteri) di una stringa che possa interpretarsi in modo univoco come scrittura* m*-aria di una classe* $\overline{X} \in \mathbb{Z}_n$ *?* (Sugg.: con l cifre in $\mathbb{Z}_m$ si riescono a rappresentare esattamente m^l numeri interi ...)

Supponiamo ad esempio che n *sia un numero con* 500 *cifre decimali e che abbiamo scelto di rappresentare i caratteri del nostro alfabeto attraverso il loro codice ASCII (cioè* $m = 256$*). Qual è allora la massima lunghezza di un testo traducibile in un'unica classe* $\overline{X} \in \mathbb{Z}_n$*?*

Svolgimento. Per avere univocità di rappresentazione in $\mathbb{Z}_n$ occorre sincerarsi che $0 \leq X < n$, e dunque che $m^l < n$. Pertanto se n e m sono assegnati, si ottiene per l la condizione

$$l < \log_m n.$$

Ed allora se n è un numero dell'ordine di 10^{500} e $m = 256$, otteniamo una massima lunghezza di testo rappresentabile in modo univoco quale elemento di $\mathbb{Z}_n$ pari a

$$l = \log_{256} 10^{500} = 500/\log_{10} 256 \cong 207,62.$$

cioè circa 207 caratteri. ∎