Crittografia ed Aritmetica Modulare
– VI incontro –

PLS - CAM

Padova, 21 novembre 2014

1 Il Piccolo Teorema di Fermat

Come si è osservato nella ATTIVITÀ 1.2. del IV incontro, in generale il comportamento delle potenze intere delle classi resto modulo n è piuttosto irregolare. Fa eccezione il caso in cui n sia un intero primo.

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

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

Dimostrazione. Consideriamo il sottoinsieme di $\mathbb{Z}_p$

$$\{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}. \qquad (*)$$

Poiché $\overline{a}$ è invertibile in $\mathbb{Z}_p$, questi elementi sono tra loro distinti. Infatti se $\overline{ia} = \overline{ja}$, moltiplicando per $\overline{a}^{-1}$ otteniamo che $\overline{i} = \overline{j}$, ed allora anche $i = j$, poiché $0 < i, j < p$. Inoltre nessuno di questi elementi è $\overline{0}$, poiché se fosse $\overline{ia} = \overline{0}$ avremmo che $p|ia$, dunque $p|a$ oppure $p|i$, che è assurdo, essendo $\overline{a} \neq \overline{0}$ e $0 < i < p$. Ne segue che l'insieme (*) coincide con

$$\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\},$$

ed allora vi è uguaglianza del prodotto degli elementi, cioè

$$\overline{a}^{p-1}\overline{(p-1)!} = \overline{(p-1)!}. \qquad (**)$$

Ora $(p-1)!$ è un intero non divisibile per p (essendo p primo), e dunque la classe $\overline{(p-1)!}$ è non nulla, quindi invertibile in $\mathbb{Z}_p$. Moltiplicando entrambi

i membri dell'uguaglianza (**) per l'inverso di $\overline{(p-1)!}$ si ottiene $\overline{a}^{p-1} = \overline{1}$, che è la tesi. ∎

Corollario 1.2. *Sia p un intero primo e sia $a \in \mathbb{Z}$. Allora*

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

Dimostrazione. Se p non divide a, allora dal Teorema 1.1 otteniamo che $p|a^{p-1} - 1$. Così $p|a(a^{p-1} - 1) = a^p - a$. Se invece $p|a$, allora anche $p|a^p - a$. ∎

In realtà vale un risultato più generale di 1.1 che attesta la regolarità del comportamento di alcune potenze intere di classi resto modulo n. Seguendo una argomentazione del tutto analoga a quella utilizzata nella dimostrazione di 1.1 si può infatti dimostrare il celebre

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*.*

HOMEWORK 1.5. *Seguendo la stessa linea dimostrativa del* Teorema 1.1*, con $\varphi(n)$ in luogo di $p-1$, si dimostri il* Teorema 1.3*.*

2 Applicazioni al metodo RSA

Il Piccolo Teorema di Fermat ha una importante conseguenza

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

Dimostrazione. Si tratta di dimostrare che $n|a^{ef} - a$. Poiché stiamo assumendo che n sia il prodotto di primi p_i, $i = 1, \ldots, t$, a due a due distinti, la tesi equivale a dimostrare che ciascuno dei p_i divide $a^{ef} - a$. Ciò è certamente vero se p_i divide a. Assumiamo dunque che p_i non divida a. In virtù del Teorema 1.1 abbiamo perciò che $a^{(p_i-1)} \equiv 1 \mod p_i$. Inoltre, dal Teorema 3.1. del IV incontro abbiamo che $\varphi(n) = (p_1 - 1)(p_2 - 1) \ldots (p_t - 1)$, dunque le ipotesi assicurano che per ogni $i = 1, \ldots, t$ risulta $p_i - 1 | ef - 1$, cioè esiste $k_i \in \mathbb{Z}$ tale che $ef - 1 = (p_i - 1)k_i$. Otteniamo allora

$$a^{ef-1} \equiv a^{(p_i-1)k_i} \equiv 1^{k_i} \equiv 1 \mod p_i,$$

cosicché $a^{ef} \equiv a\, a^{ef-1} \equiv a\, 1 \equiv a \mod p_i$, come voluto. ∎

Quanto appena visto ha una diretta applicazione crittografica:

Corollario 2.2 (METODO CRITTOGRAFICO RSA - Rivest, Shamir, Adleman - 1978)**.**

- *Ogni utente (= ente utilizzatore di sistema crittografico RSA) si procura due numeri primi distinti p e q molto grandi (circa 300 cifre ciascuno), calcola $n = pq$ e $\varphi(n) = (p-1)(q-1)$. Terrà segreti p, q e $\varphi(n)$.*
- *L'utente sceglie poi in modo casuale un intero $1 < e < \varphi(n)$ che sia coprimo con $\varphi(n)$: per far ciò si avvale dell'algoritmo di Euclide esteso, che gli fornisce inoltre un intero f (da tenere segreto!) tale che $ef \equiv 1 \mod \varphi(n)$.*
- *L'utente fornisce pubblicamente la sua chiave (n, e).*
- *Chiunque voglia comunicare con lui, traduce il messaggio da trasmettere in una successione di elementi di $\mathbb{Z}_n$ (vedremo nella prossima sezione come, in dettaglio). Trasforma quindi ogni elemento $\overline{X}$ di questa successione nell'elemento crittato $\overline{X}^e$, e trasmette questi ultimi all'utente.*
- *L'utente riceve la successione di elementi crittati, e decritta ciascun $\overline{X}^e$ tramite "elevazione alla f", cioè calcola $(\overline{X}^e)^f = \overline{X}^{ef} = \overline{X}$ in $\mathbb{Z}_n$ (cfr.* Corollario 2.1*). In tal modo è in grado di risalire immediatamente al messaggio originale.*
- *Chiunque sia in condizione di "ascoltare" la trasmissione dei dati cifrati $\overline{X}^e$, pur conoscendo la chiave pubblica (n, e), non riesce a risalire ai dati d'origine $\overline{X}$. Infatti per far ciò dovrebbe essere in grado di determinare f,*

che è la classe inversa di e modulo $\varphi(n)$. Dovrebbe necessariamente calcolarsi $\varphi(n)$ o, equivalentemente, p e q (vedi la Osservazione 3.4. *del IV incontro), a partire da n, ma non riesce a farlo in un "tempo macchina finito", a causa della complessità algoritmica.*

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?

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.*

L'attività 2.4 è lontana da una reale applicazione di RSA per almeno due motivi. Innanzi tutto $n = 21 = 3 \cdot 7$ è prodotto di due primi troppo piccoli per essere considerati sicuri! Inoltre la codifica monoalfabetica non è proponibile, perché, come abbiamo visto nel I incontro, essa è facilmente espugnabile con metodi basati sull'analisi di frequenza.

Come si trasforma, allora, in modo sicuro, un testo da trasmettere come successione di elementi di $\mathbb{Z}_n$? Questo è l'argomento della prossima sezione.

3 Scrittura m-aria di un intero

Supponiamo che $n = pq$, con p e q primi distinti molto grandi. Supponiamo poi che i messaggi da cifrare e decifrare siano scritti in un alfabeto con m caratteri (ad esempio $m = 21$ se è sufficiente l'alfabeto italiano senza spaziature, oppure $m = 256$ se vogliamo utilizzare il codice ASCII).

Consideriamo ora una stringa

$$x_k x_{k-1} \dots x_0 \qquad (*)$$

di $k+1$ caratteri o, meglio, di numeri compresi tra 0 e $m-1$ (infatti ogni carattere x_i della stringa è scritto nell'alfabeto con m caratteri, dunque è un elemento di $\mathbb{Z}_m$). Tale stringa può essere "letta" come un intero positivo X dato da

$$X = x_k m^k + x_{k-1} m^{k-1} + \dots + x_1 m^1 + x_0 m^0. \qquad (**)$$

Se $m = 10$, ad esempio, ciò costituisce l'usuale scrittura decimale di X.

In generale, si dice che (*) rappresenta la **scrittura m-aria di X**, ed i coefficienti $x_0, x_1, \dots, x_k$ sono detti le **cifre di X in base m**.

Questa corrispondenza tra stringhe (*) di elementi di $\mathbb{Z}_m$ ed interi positivi (**) è biiettiva. Infatti ad ogni numero intero positivo X possiamo a sua volta associare una stringa (*) in modo tale che valga (**), cioè tale per cui (*) costituisca esattamente la scrittura m-aria di X. Procediamo nel modo seguente. Consideriamo dapprima la divisione di X per m, ottenendo quoziente X_0 e resto x_0; successivamente eseguiamo la divisione di X_0 per m, ottenendo quoziente X_1 e resto x_1. Procediamo iterativamente in questo modo, sino ad ottenere quoziente $X_k = 0$. La successione $x_0, x_1, \dots, x_k$ di resti così ottenuta soddisfa all'identità (**), dunque essi costituiscono esattamente le cifre di X in base m.

In definitiva, il testo del messaggio intero (od una sua parte cospicua, se il messaggio è troppo lungo) può interpretarsi come una stringa che rappresenta la scrittura m-aria di un intero positivo X, con $0 \le X < n$ (ricordiamoci che n è molto grande!). Dunque l'intero messaggio è biiettivamente trasformato in una (od in qualche) classe resto $\overline{X}$ modulo n. A questo punto $\overline{X}$ viene crittografata in $\overline{Y} = \overline{X}^e$ tramite RSA, così come descritto nel Corollario 2.2.

L'utente riceve il messaggio in codice, lo decritta tramite $\overline{X} = \overline{Y}^{\,f}$, ed infine riottiene il messaggio originale in chiaro, attraverso la scrittura m-aria di X.

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 $\overline{X} \in \mathbb{Z}_n$?*