Università' degli studi di Roma "Tor Vergata"
Teoria della sicurezza e crittografia
Lezione 07

Authors: Marcello Politi, Samir Salman, Angelo Silvestri

Novembre 2019

1 Teorema cinese del resto

Il teorema cinese del resto, così detto perchè il primo enunciato è dovuto a *Sun Zi* matematico cinese del III secolo d.C può essere enunciato come segue:

Dati due numeri primi tra di loro p e q, e due numeri interi qualsiasi a e b esiste sempre un x tale che:

$$x = a \bmod p$$
$$x = b \bmod q$$

Detto in altre parole: dati due numeri primi tra di loro p e q, e due numeri interi qualsiasi a e b esiste sempre un x che diviso per p dia resto a e diviso per q dia resto b. Di qui il nome di teorema del resto.

Questo teorema si estende anche a più di due numeri, e si può riformulare così: Dati n numeri primi tra di loro p1, p2 ... pn, ed n numeri qualsiasi a1, a2 ... an esiste sempre un x tale che:

$$x = a1 \bmod p1$$
$$x = a2 \bmod p2$$
$$\dots$$
$$x = an \bmod pn$$

2 Introduzione a Guile

Quando si lavora con numeri molto grandi è necessario usare soluzioni particolari per riuscire a manipolare correttamente tali numeri; a tal proposito vi sono

librerie dedicate, esempio la GMP Gnu Multiple Precision. L'idea è di utilizzare un nuovo ambiente adottando **Scheme** un linguaggio di programmazione funzionale, dialetto del **Lisp** List-Processing, di cui mantiene tutte le caratteristiche; prerequisito è installare **Docker**(consigliabile su linux distribuzione ubuntu).

Utilizzaremo la versione 3.0 di Scheme. ***Guile*** è una implementazione del linguaggio Scheme, quindi un interprete Scheme.

2.1 Tipi elementari, operatori principali

Tipi elementari: *Interi, caratteri, String*
Tipo strutturato più semplice: **cons**

car e **cdr** sono operazioni primitive che operano su liste concatenate composte da celle cons. Una cella cons è composta da due puntatori; l'operazione car estrae il primo puntatore e l'operazione cdr ne estrae il secondo.

Così, l'espressione (car (cons x y)) restituisce x e (cdr (cons x y)) restituisce y.

Quando le celle cons vengono usate per implementare liste singolarmente concatenate (piuttosto che alberi o altre strutture più complesse), l'operazione car restituisce il primo elemento della lista mentre cdr ne restituisce il resto. Per questo motivo queste operazioni vengono a volte chiamate first (primo) e rest (resto) o head (testa) e tail (coda).

Quote **'** torna l'identità ciuoè il parametro della funzione. Es: '(abc) restiruisce abc

Operatori condizionali: **cond**, la cond valuta n espressioni e termina la valutazione appena trova una condizione vera. Esempio:

(cond (test1 action1) (test2 action2) ... (testn actionn))