16/3/2017

Πώς μπορούμε να χρησιμοποιήσουμε το κινέζικο θεώρημα των υπολοίπων;

Έστω ότι θέλουμε να υπολογίσουμε το $65 \cdot 57 \pmod{77}$
Το 77 γράφεται ως $7 \cdot 11$ άρα μπορούμε να γράψουμε το παραπάνω ως διάνυσμα:
65=[65mod7, 65mod11]=[2,10]
57=[57mod7, 57mod11]=[1,2]
Ύστερα πολλαπλασιάζουμε τα στοιχεία των διανυσμάτων ένα προς ένα:
$[2 \cdot 1 \bmod 7,\ 10 \cdot 2 \bmod 11] = [2,9]$ άρα $65 \cdot 57 \pmod{77} = [2,9]$
Έτσι έχουμε το σύστημα: $x \equiv 2 \pmod 7$, $x \equiv 9 \pmod{11}$ $\Rightarrow x \equiv 9 \pmod{77}$ Άρα η λύση είναι το 9.

Αβελιανή ομάδα
Λέγεται μια ομάδα που πληροί την ιδιότητα της αντιμεταθετικότητας.

Υποομάδα
Είναι ένα υποσύνολο μιας ομάδας το οποίο διατηρεί τις ιδιότητες που έχει η ομάδα.
Στην ουσία μας ενδιαφέρουν μόνο οι υποομάδες $(Z_n,+)$ και $(Z_n^*,*)$.

Πώς βρίσκουμε υποομάδες μιας ομάδας;

1. Μια ομάδα θα έχει τόσες υποομάδες όσα και τα στοιχεία της. Γράφουμε πρώτα το στοιχείο που ορίζει την ομάδα.
2. Το προσθέτουμε/πολλαπλασιάζουμε με τον εαυτό του μέχρι να γράψουμε όλα τα υπόλοιπα.

Παραδείγματα:
Υποομάδες της $(Z_8,+)$, $Z_8=\{0,1,2,3,4,5,6,7\}$
$\langle 0 \rangle_8 = \{0\}$
$\langle 1 \rangle_8 = \{1,2,3,4,5,6,7,0\}$
$\langle 2 \rangle_8 = \{2,4,6,0\}$
$\langle 3 \rangle_8 = \{3,6,1,4,7,2,5,0\}$
...
$\langle 7 \rangle_8 = \{7,6,5,4,3,2,1,0\}$

Παρατηρούμε ότι σταματάμε όταν συναντήσουμε το 0.

Υποομάδες της $(Z_8^*,*)$, $(Z_8^*,*)=\{1,3,5,7\}$
$\langle 1 \rangle_8 = \{1\}$
$\langle 3 \rangle_8 = \{3,1\}$
$\langle 5 \rangle_8 = \{5,1\}$
$\langle 7 \rangle_8 = \{7,1\}$

Παρατηρούμε ότι σταματάμε όταν συναντήσουμε το 1.

Παρατήρηση: Έχουμε βρει όλα τα στοιχεία μιας υποομάδας όταν βρούμε το ουδέτερο στοιχείο της.

Πώς λύνουμε προβλήματα εκθετών $\alpha^x \equiv b\, mod n$

Η θέση του στοιχείου στην υποομάδα είναι ο εκθέτης στον οποίο υψώνουμε το στοιχείο που ορίζει την ομάδα. Π.χ. $(Z_7^*,*)$: $<5>_7=\{5,4,6,2,3,1\}$ $5^x \equiv 2 (mod\, 7)$. Λόγω αυτού μπορούμε να λύσουμε τα προβλήματα εκθετών γρήγορα, επειδή ισχύει η ιδιότητα: $g^k=g^{k-1}g$ mod n. Αν δηλαδή γνωρίζουμε το προηγούμενο στοιχείο, μπορούμε εύκολα να βρούμε το επόμενο.

$(Z_7^*,*)$	1	2	3	4	5	6	7	8
$<2>_7$	2	4	1	2	4	1	2	4
$<3>_7$	3	2	6	4	5	1	3	2

Παρατηρούμε ότι μετά το ουδέτερο στοιχείο παρουσιάζεται περιοδικότητα.

Θεώρημα Fermat

$Για\ κάθε\ \alpha \in \mathbb{Z}_p *\ ισχύει\ ότι\ \ a^{p-1} \equiv 1 (mod n)\ \ όπου\ p\ είναι\ πρώτος.$

Υπενθύμιση:

Θεώρημα Euler

$Για\ κάθε\ \alpha \in \mathbb{Z}_n *\ \ a^{\Phi(n)} \equiv 1 (mod n)\quad όπου\ \Phi(n)=|Z_n *|$

Χρησιμοποιώντας τα θεωρήματα αυτά μπορούμε να λύσουμε προβλήματα του τύπου:

$3^{98765432101}$ mod101

$\Phi(101)=101 \cdot (1-\frac{1}{101})=100$ άρα από το θεώρημα του Euler, $3^{100} \equiv 1 (mod\, 101)$ Έτσι έχουμε $3^{98765432101}$ mod101 = $3^{100\lambda+1}$mod101 = $3^{100\lambda}$3mod101. Αλλά $3^{100} \equiv 1\, mod\, 101$ άρα η προηγούμενη σχέση ισούται με 3mod101=3

Γεννήτορας - Generator

Λέγεται ένας αριθμός που μπορεί στην υποομάδα του να αναπαράγει όλα τα στοιχεία της ομάδας στην οποία ανήκει.

Ιδιότητα:

$g^x \equiv g^y\, mod n \Leftrightarrow x \equiv y (mod \Phi(n))$ Η ιδιότητα αυτή μπορεί να ισχύει ακόμα και αν το g δεν είναι γεννήτορας.

Έστω ότι θέλουμε να λύσουμε: $3^{98765432199}$mod101=$3^{100\lambda+99}$mod101=3^{99}mod101

α^bmodn	3^{99}mod101

1. Γράφω το b σε δυαδική μορφή	99=1100011
2. temp=1	temp=1

3. Από MSB προς LSB
for (i=1 to n, i--){
temp=temp^2 modn
if bit=1
temp=temp amodn
}
return temp
	1mod101->3mod101->9mod101->27mod101->27^2mod101->27^4mod101...

One Way Function

Υπενθύμιση: Πρόβλημα Παραγοντοποίησης, Πρόβλημα Διακριτού Λογαρίθμου. Το κοινό τους γνώρισμα είναι ότι τα αντίστροφα προβλήματα λύνονται εύκολα.
Τα προβλήματα αυτά λέγονται **one way function**, αφού ισχύει ότι:

- f: X → Y
- αν γνωρίζω το x μπορώ εύκολα να βρω το y=f(x).
- για σχεδόν όλα τα y δεν μπορώ να βρω γρήγορα κάποιο x ώστε y=f(x).

Προσοχή!! Εύκολα και γρήγορα σημαίνει σε πολυωνυμικό χρόνο σε σχέση με την είσοδο.

Diffie-Hellman key exchange

Το πρόβλημα με τα πρωτόκολλα συμμετρικού κλειδιού είναι το πώς θα τα ανταλλάξουμε μέσα από ένα ανασφαλές κανάλι. Αυτή η μέθοδος ασύμμετρου κλειδιού αντιμετωπίζει αυτό το πρόβλημα.

Οι χρήστες συμφωνούν σε έναν τεράστιο πρώτο p και ένα γεννήτορα g του Z_p*.
Κάθε ζευγάρι χρηστών κάνει τα εξής:

A	B
Διαλέγει αυθαίρετα έναν αριθμό α από το Z_p*.	Διαλέγει αυθαίρετα έναν αριθμό β από το Z_p*.
Υπολογίζει το g^{α}modp	Υπολογίζει το g^{β}modp
Στέλνει το αποτέλεσμα στον B	Στέλνει το αποτέλεσμα στον A
Υπολογίζει το $(g^{\beta}\text{modp})^{\alpha}$	Υπολογίζει το $(g^{\alpha}\text{modp})^{\beta}$
Τελικό κλειδί είναι το $g^{\alpha\beta}$modp	

Για να αποκρυπτογραφήσουμε αυτό το πρωτόκολλο θα πρέπει να βρούμε το α ή το β. Για να τα βρούμε όμως γρήγορα θα πρέπει να μπορούμε να λύσουμε γρήγορα το πρόβλημα Διακριτού Λογαρίθμου, το οποίο είναι δύσκολο.