2/3/2017

Χαρακτηριστικά Σύγχρονης Κρυπτογραφίας:

1. βασίζεται σε **τυπικούς ορισμούς**: ορίζουμε τι θέλουμε να κάνουμε ώστε να ξέρουμε αν το έχουμε πετύχει. Π.χ.: ένα πρωτόκολλο ονομάζεται **ασφαλές** αν αφού δούμε το κρυπτογραφημένο μήνυμα, δεν λαμβάνουμε καμία πληροφορία σε σχέση με την πληροφορία που είχαμε πριν το δούμε.
2. βασίζεται σε **σαφείς υποθέσεις**: Μια σαφής υπόδεση είναι ότι το πρόβλημα που θέλουμε να λύσουμε είναι δύσκολο.
3. περιλαμβάνει **μαθηματικές αποδείξεις**

Θεωρία Αριθμών:

Περιλαμβάνει μόνο ακεραίους (Z).

Βασική πράξη είναι η Διαίρεση: $\boxed{d \mid a}$ ο d διαιρεί τον a, δηλαδή $a=k\cdot d,\ k\in Z$

Πρώτος Αριθμός: είναι ένας αριθμός που οι μόνοι διαιρέτες του είναι το 1 και ο εαυτός του.

Σύνθετος αριθμός: είναι ένας αριθμός που έχει επιπλέον διαιρέτες.

Οι πρώτοι αριθμοί είναι άπειροι

Απόδειξη:

Έστω ότι οι πρώτοι αριθμοί είναι k σε πλήθος.

$$\text{πρώτοι}=\{p_1, p_2, p_3, \dots, p_k\}$$

Τους πολλαπλασιάζουμε μεταξύ τους:

$$n=\prod_{i=1}^{k} p_i$$

Ύστερα προσθέτουμε 1 στο αποτέλεσμα. Έτσι σε κάθε περίπτωση, ο n θα διαιρείται από το 1, και τον εαυτό του, αλλά σε κάθε διαίρεση με πρώτο θα έχουμε υπόλοιπο 1. **Άτοπο** επειδή κάθε αριθμός μπορεί να γραφτεί ως γινόμενο πρώτων. (βλ. παρακάτω)

Θεώρημα της Διαίρεσης

Για κάθε a, n με n>0 υπάρχουν μοναδικά q και r ώστε $\boxed{a=q\cdot n+r \quad 0\le r\le n-1}$

Το πηλίκο είναι $\lfloor a|n \rfloor$ και το υπόλοιπο r = amodn εξασφαλίζει τη μοναδικότητα.

Όλοι οι αριθμοί που διαιρούν το a και αφήνουν το ίδιο υπόλοιπο r ανήκουν στην ίδια οικογένεια, ή αλλιώς ανήκουν στην ίδια **κλάση ισοδυναμίας modn.** Αυτό γράφεται ως:

$$[a]_n=\{kn+r, k\in Z\}$$

Γιατί είναι χρήσιμη αυτή η έννοια;

Έστω ένας αριθμός n και σύνολο Z_n που περιλαμβάνει όλες τις κλάσεις ισοδυναμίας που μπορεί να προκύψουν αν διαιρέσουμε το n.

Δηλαδή $Z_n=\{[0]_n,[1]_n,\dots,[n-1]_n\}$ ή αλλιώς $Z_n=\{0,1,\dots,n-1\}$

Ισοδυναμία

$$a \bmod n = b \bmod n \Rightarrow a \equiv b$$

Έστω α_1 και α_2 και το σύμβολο * αντιπροσωπεύει τις πράξεις { +, -, x}. Δεν περιλαμβάνεται η διαίρεση γιατί δεν είναι καλά ορισμένη στο σύνολο των ακεραίων. Τότε έχουμε:

$(\alpha_1*\alpha_2)\text{mod}n=[(\alpha_1\text{mod}n)*(\alpha_2\text{mod}n)]\text{mod}n$

Με αυτό τον τρόπο μπορούμε να απλοποιούμε τις πράξεις.

Κοινός Διαιρέτης

Αν d|α και d|b τότε $d|(ax+by),\ x,y\in Z$

Μέγιστος Κοινός Διαιρέτης

Ιδιότητες

- gcd(α,b)=gcd(b,α)
- gcd(α,kα)=α
- gcd(-α,b)=gcd(α,b)
- gcd(α,0)=α για $\alpha\neq 0$
- gcd(α,b)=min(αx_0+by_0)>0

Απόδειξη gcd(α,b)=min(αx_0+by_0)>0

Θα πρέπει να αποδείξουμε ότι:

$$1^{ος}\ τρόπος \begin{cases} 1.\ gcd(a,b)\geq min(\alpha x_0+by_0) \\ 2.\ gcd(a,b)\leq min(\alpha x_0+by_0) \end{cases}$$

Ξεκινάμε από το 2. Προκύπτει από την τελευταία ιδιότητα

Για το 1 έχουμε:

έστω s=min(αx_0+by_0)>0. Άρα υπάρχουν q, r : $\begin{array}{l} a=q\cdot s+r\Rightarrow \\ a=\lfloor a|s\rfloor\cdot s+(amods)\Rightarrow \\ amods=a-\lfloor a|s\rfloor\cdot s \end{array}$

Αλλά γνωρίζουμε ότι $0\leq amods<s \quad και \quad a(1-\lfloor a|s\rfloor x_0)-b(\lfloor a|s\rfloor)$

Από τα παραπάνω συμπεραίνουμε ότι amods θα είναι ένας ακέραιος στο [0,1), άρα θα είναι 0. Δηλαδή το s διαιρεί το α. Ομοίως και για το b, οπότε αποδεικνύεται και το 2.

2ος τρόπος

Θεώρημα Παραγοντοποίησης

Οποιοσδήποτε αριθμός μπορεί να γραφτεί ως γινόμενο πρώτων με μοναδικό τρόπο.

$Έστω \;\; n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} .... p_i^{e_i} \;\; πρώτοι, \; e_i \geq 1$

Γράφουμε τα a και b ως τα γινόμενα:

$\alpha = p_1^{e_1} \cdot p_1^{e_1} ... p_k^{e_k} \;\; και \;\; b = p_1^{f_1} \cdot p_2^{f_2} ... p_m^{f_m} \;\; με \, e_i, f_i \geq 0 \; και \; k < m$

Τότε έχουμε ότι $gcd(a,b) = p_1^{min(e_1, f_1)} \cdot p_2^{min(e_2, f_2)} .... p_k^{min(e_k, f_k)}$

Το πρόβλημα με αυτή την απόδειξη είναι ότι το πρόβλημα της παραγοντοποίησης είναι ένα πρόβλημα που δεν λύνεται σε πολυωνυμικό χρόνο σε σχέση με την είσοδο.

Αν ξέρουμε ότι ο n είναι σύνθετος, τότε ο ένας παράγοντάς του θα είναι σίγουρα μικρότερος ή ίσος του $\sqrt{n}$. Και πάλι όμως ο $\sqrt{n}$ δεν είναι πολυωνυμικός ως προς την είσοδο, οπότε το πρόβλημα παραμένει.

3ος τρόπος

Αλγόριθμος του Ευκλείδη

```
do
    gcd(a,b)=gcd(b,amodb)
while b>0
```

Η χειρότερη περίπτωση για τον αλγόριθμο αυτό είναι τα α και b ναι είναι συνεχόμενοι όροι της ακολουθίας Fibonacci, αλλά ακόμα και τότε έχει πολυωνυμική πολυπλοκότητα log(a+b)

Πρώτοι μεταξύ τους

Είναι δύο αριθμοί αν gcd(α,b)=1

Ο μέγιστος κοινός διαιρέτης μας ενδιαφέρει επειδή μέσω αυτού μπορούμε να ορίσουμε τη διαίρεση στους ακεραίους.