Θ.Α.

20/1/2016

Αν $n \geq 2$ και $a \in \mathbb{Z}$ και $(a,n)=1$, τότε:

$ord_n(a) = \min\{k \in \mathbb{N} / a^k \equiv 1 \pmod n\}$

a: πρωταρχική ρίζα $\bmod n \Leftrightarrow ord_n(a) = \varphi(n)$

$2^{74.207.281} - 1$ Άγνωστος πρώτος αριθμός

↓ Mersenne

GIMPS

Έχει 22.338.618 ψηφία. 7/1/2016

Υπάρχουν πρωταρχικές ρίζες $\bmod n \Leftrightarrow n = 2, 4, p^m, 2p^m$, όπου p: περιττός πρώτος και τότε υπάρχουν $\varphi(\varphi(n))$ πρωταρχικές ρίζες $\bmod n$, οι οποίες είναι: a^k, όπου a: πρωταρχική ρίζα $\bmod n$ $(k, \varphi(n)) = 1$

ΠΑΡΑΔΕΙΓΜΑ: $p=7$: πρώτος $\Rightarrow$ υπάρχουν πρωταρχικές ρίζες $\bmod 7$, οι οποίες είναι σε πλήθος $\varphi(\varphi(7)) = \varphi(6) = 2$. Θεωρούμε ένα αναγκαίο σύνολο σπαθιών $\bmod 7$: $\{1, 2, 3, 4, 5, 6\}$

① $ord_7(1) = 1$, ② $ord_7(2) =$;

$2^1 = 2 \not\equiv 1 \pmod 7$

$2^2 = 4 \not\equiv 1 \pmod 7$

$2^3 = 8 \equiv 1 \pmod 7$

Άρα $ord_7(2) = 3 \neq 6 = \varphi(7)$

Άρα το 2 δεν είναι πρωταρχική ρίζα $\bmod 7$

③ $ord_7(3) =$;

$3^1 = 3 \not\equiv 1 \pmod 7$

$3^2 = 9 \equiv 2 \not\equiv 1 \pmod 7$

$3^3 \equiv 27 \equiv 6 \not\equiv 1 \pmod 7$

$3^4 \equiv 18 \equiv 4 \pmod 7$

$3^5 = 12 \equiv 5 \pmod 7$

$3^6 \equiv (-1)^2 \equiv 1 \pmod 7$

Άρα $ord_7(3) = 6 = \varphi(7)$

$\Rightarrow 3$: πρωταρχική ρίζα $\bmod 7$

$ord_n(a) \mid \varphi(n)$

Αν a: πρωταρχική ρίζα $\bmod n$, τότε: $U(\mathbb{Z}_n) = \{[1]_n, [a]_n, \ldots, [a^{\varphi(n)-1}]_n\}$

Η δεύτερη πρωταρχική ρίζα $\bmod 7$ θα είναι η 3^k, όπου $(k, \varphi(7)) = 1 \Rightarrow (k,6) = 1 \Rightarrow$

$\Rightarrow k = 5$, $3^k = 3^5 = \underbrace{3 \cdot 3}_{9} \cdot \underbrace{3 \cdot 3}_{9} \cdot 3 \equiv 9 \cdot 9 \cdot 3 = 2 \cdot 2 \cdot 3 = 4 \cdot 3 = 12 \equiv (5) \bmod 7$

Ένα ανάγλυφο σύστημα υπολοίπων είναι $\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ (2, 6, 4, 5, 1)

$$\text{ord}_n(a^k) = \frac{\text{ord}_n(a)}{(k, \text{ord}_n(a))} = \frac{\varphi(n)}{(k, \varphi(n))}$$

ΑΣΚΗΣΗ: $n = 11$: πρώτος $\Rightarrow$ υπάρχουν πρωταρχικές ρίζες mod 11, οπότε σε πλήθος είναι $\varphi(\varphi(11)) = \varphi(10) = \varphi(2 \cdot 5) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$

Ανάγλυφο σύστημα υπολοίπων mod 11 : $= \{1, 2, 3, \ldots, 10\}$

$2^1 = 2 \not\equiv 1 \pmod{11}$

$2^2 = 4 \not\equiv 1 \pmod{11}$

$2^3 = 8 \not\equiv 1 \pmod{11}$

$2^4 = 16 \equiv 5 \pmod{11}$

$2^5 = 10 \equiv -1 \pmod{11}$

$\vdots$

$2^{10} = (-1)^2 \equiv 1 \pmod{11}$

Τότε $\text{ord}_{11}(2) = 10 = \varphi(11) \Rightarrow 2$: πρωταρχική ρίζα mod 11

$\rightarrow \{2^k \mid k = 1, \ldots, 10\}$

Θα είναι: 2^k, όταν $(k, \varphi(11)) = 1 \Rightarrow (k, 10) = 1$

$\Rightarrow k = 1, 3, 7, 9$

- $k = 1 \Rightarrow 2^1 = 2$
- $k = 3 \Rightarrow 2^3 = 8$
- $k = 7 \Rightarrow 2^7 = 7$
- $k = 9 \Rightarrow 2^9 = 6$

ΑΣΚΗΣΗ: Να δειχθεί ότι: $2016 \mid \varphi(a^{9016} - 1)$, όταν a: έτος γέννησης σας

Γενικότερα θα δείξουμε ότι: $\forall n, a \in \mathbb{N} : n \mid \varphi(a^n - 1)$

$\text{ord}_{a-1}^{n}(a) = n$

① $(a, a^n - 1) = d$, τότε: $d \mid a \Rightarrow d \mid a^n, \forall n \geq 1$ / $d \mid a^n - 1 \not\Rightarrow d \mid 1$ $\Rightarrow d = 1$

Άρα ορίζεται n $\text{ord}_{a-1}^{n}(a)$

② Προφανώς $a^n - 1 \mid a^n - 1 \Rightarrow a^n - 1 \equiv 0 \pmod{(a^n - 1)} \Rightarrow a^n \equiv 1 \pmod{(a^n - 1)}$

③

Έχουν $k \in \mathbb{N} : 1 \le k < n$ και $a^k \equiv 1 \pmod{(a^n-1)} \Rightarrow a^n-1 \mid a^k-1 \Rightarrow$

$\Rightarrow a^n-1 \le a^k-1 \Rightarrow a^n \le a^k$: ατοπο. διότι $k<n$ και $a, k \in \mathbb{N}$.

④ Άρα $\operatorname{ord}_{a^n-1}(a) = n$ Άρα: $n \mid \varphi(a^n-1)$

Κρυπτογραφία:

Πρώτο απλό κρυπτογράφημα ① Julius Ceasar ($100 \pi.x$ - $44 \pi.x$)

Α	Β	Γ	Δ	Ε	...	Ω
↓	↓	↓	↓	↓		↓
0	1	2	3	4		23

Κλειδί: a, b έχουν

$(a, 24) = 1$

$0 \le b \le 23$ (a,b) : κλειδί

Ρ: ένα γράμμα ως αλφάβητο

$C \equiv aP + b \pmod{24}$

(Η)

$aP \equiv C - b \pmod{24} \Rightarrow P = a'(c-b) \bmod 24$

$(a, 24) = 1 \Rightarrow \exists [a]'_{24}$

Παράδειγμα: $a = 5$, $b = 3$ $\quad A \rightsquigarrow 0$

$P = 5(0-3) \pmod{24} = -15 \pmod{24} = 9 \pmod{24} \rightsquigarrow K$

ΑΔΖ | ΚΣΩΗ | ΥΧΨ | ΝΥΔ

κλειδί: $(a,b) = (5,3)$

Κ

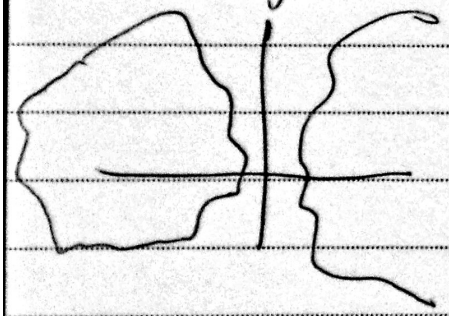
② Κρυπτογραφία Δημόσιου Κλειδιού
Κρυπτοσύστημα RSA (1978)
Βασίζεται σε κλειδιά της μορφής (e,n), όπου $e,n \in \mathbb{N}$ $(e,\varphi(n))=1$
και $n=p\cdot q$ όπου p,q πρώτοι αριθμοί μη πλήθος ψηφίων >500

Ρ: αρχείο σε αλφάβητο
↳ $E(C) \equiv P^e_{(\mathrm{mod}\, n)}$

$[d]_{\varphi(n)} = [e]^{-1}_{\varphi(n)}$

$D(C) = C^d = (P^e)^d \equiv P_{(\mathrm{mod}\, n)}$
Το δεύτερο κλειδί είναι το (d,n)

③ Κρυπτογραφία Ελλειπτικές Καμπύλες $\{(x,y) \in \mathbb{R}^2 / y^2 = x^3 + ax + b\}$



Για τις εξετάσεις: ① Στοιχειώδη θεωρία διαιρετότητας, πρώτοι αριθμοί, ΜΚΔ, ΕΚΠ
Ευκλ. Διαιρ. + Ευκλ. - Αλγ.
② Διοφαντικές εξισώσεις
③ Αριθμητικές συναρτήσεις Βασικές ιδιότητες (Τύπος αντιστροφής Möbius)
④ Βασικά θεωρήματα ισοτιμιών (Euler, Fermat, Wilson Επίλυση γραμμικών ισοτιμιών)
⑤ Σύστημα Γραμμ. Ισοτιμιών
⑥ Τάξεις στοιχείων
⑦ Ριζοπρωτικές ρίζες