Τάξη του a mod n

$ord_n(a) = s$ = ο μικρότερος φυσικός ώστε:

$[a]_n^s = [1]_n$

Γνωρίζουμε ότι $[a]_n^{\varphi(n)} = [1]_n$, $(a,n)=1$

Όταν $ord_n(a) = \varphi(n)$, τότε η κλάση $[a]_n$ καλείται πρωταρχική ρίζα mod n

$\mathbb{Z}_7^*$: $2 \to 2^2 = 4 \to 2^3 = 2 \cdot 2^2 = 2 \cdot 4 = 8 \equiv 1 \mod 7$

$ord_7(2) = 3$

$3 \to 3^2 = 9 \equiv 2 \mod 7 \to 3^3 = 3^2 \cdot 3 \equiv 2 \cdot 3 \mod 7 \equiv$
$\equiv 6 \mod 7 \to$
$\to 3^4 = 3^3 \cdot 3 \equiv 6 \cdot 3 \mod 7 \equiv 6 \cdot 3 \mod 7 \equiv 18 \mod 7 \equiv$
$\equiv 4 \mod 7 \to 3^5 = 3^4 \cdot 3 \equiv 4 \cdot 3 \mod 7 \equiv 12 \mod 7 \equiv$
$\equiv 5 \mod 7 \to 3^6 = 3^5 \cdot 3 \equiv 5 \cdot 3 \mod 7 \equiv 15 \mod 7 \equiv$
$\equiv 1 \mod 7$

Άρα, $ord_7(3) = 6$.

Επομένως, $[3]_7$ πρωταρχική ρίζα

$$\mathbb{Z}_7^* = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$$
$$\{[3]_7^6, [3]_7^2, [3]_7^1, [3]_7^4, [3]_7^5, [3]_7^3\}$$

πχ

$$[4]_7 \cdot [6]_7 = [3]_7^4 \cdot [3]_7^3 = [3]_7^{4+3} = [3]_7^{7 \mod (ord_7 3)} =$$
$$= [7]_7^{7 \mod 6} = [3]_7^1$$

ΦΥΛΛΟ #5

1) p πρώτος $\overset{ΝΔΟ}{\Longrightarrow}$ $p+10$, $p+14$ πρώτοι

$p=3 \rightarrow p+10=13$ και $p+14=17$ ισχύει

Απορ.

$p>3 \rightarrow \begin{cases} p=3k+1 \rightarrow p+10 = 3k+1=10 \ \& \ p+14=\cancel{3(k+5)} \\ p=3k+2 \rightarrow p+10 = 3k+2+10 = 3(k+4) \leftarrow \text{Απορ.} \end{cases}$

Άρα, είναι μόνο το 3

2) $(m,n)=d \overset{ΝΔΟ}{\Longrightarrow} \varphi(mn)\varphi(d) = d\,\varphi(m)\,\varphi(n)$

$d = p_1^{k_1} \cdots p_\ell^{k_\ell}$

$m = p_1^{k_1'} \cdots p_\ell^{k_\ell'} \cdot q_1^{m_1} \cdots q_r^{m_r}, \quad k_i \le k_i'$

$n = p_1^{k_1''} \cdots p_\ell^{k_\ell''} \cdot t_1^{m_1'} \cdots t_{r'}^{m_{r'}'}, \quad k_i \le k_i''$, $q_i \neq t_i$ πρώτοι

$k_i = \min(k_i', k_i'')$

$\varphi(d) = p_1^{k_1-1} \cdots p_\ell^{k_\ell-1}(p_1-1)\cdots(p_\ell-1)$

$\varphi(mn) = \varphi(p_1^{k_1'+k_1''} + \cdots + p_\ell^{k_\ell'+k_\ell''} \cdot q_1^{m} \cdots q_r^{m_r} \cdot t_1^{m_1'} \cdots t_{r'}^{m_{r'}'}) =$

$= p_1^{k_1'+k_1''-1} \cdots p_\ell^{k_\ell'+k_\ell''-1} \cdot q_1^{m_1-1} \cdots q_r^{m_r-1} \cdot t_1^{m_1'-1} \cdots t_{r'}^{m_{r'}'-1} \cdot$

$\cdot (p_1-1)\cdots(p_\ell-1)(q_1-1)\cdots(q_r-1)(t_1-1)\cdots(t_{r'}-1)$

$\varphi(m) = p_1^{k_1'-1} \cdots p_\ell^{k_\ell'-1} \cdot q_1^{m_1-1} \cdots q_r^{m_r-1}(p_1-1)\cdots(p_\ell-1)(q_1-1)\cdots(q_r-1)$

$\varphi(n) = p_1^{k_1''-1} \cdots p_\ell^{k_\ell''-1} \cdot t_1^{m_1'-1} \cdots t_{r'}^{m_{r'}'-1}(p_1-1)\cdots(p_\ell-1)\cdot(t_1-1)\cdots(t_{r'}-1)$

- $\varphi(mn)\varphi(d) = p_i^{k_i'+k_i''-1+k_i-1} \cdot (p_i-1)^2 \cdot q_i^{m_i-1}(q_i-1) \cdot t_i^{m_i'-1}(t_i-1)$

- $d\,\varphi(m)\cdot\varphi(n) = p_i^{k_i} \cdot p_i^{k_i'-1}(p_i-1) \cdot p_i^{k_i''-1}(p_i-1) =$
  $= p^{k_i+k_i'-1+k_i''-1} \cdot (p_i-1)^2 = q_i^{m_i-1}(q_i-1)$

το ίδιο για το $t_i^{m_i'-1}$

3) $\varphi(m^2) = \varphi(m\cdot m) \xRightarrow[(m,m)=m]{(2)} \varphi(m^2)\cancel{\varphi(m)} = m(\varphi(m))^{\cancel{2}} \Leftrightarrow$

$\Rightarrow \varphi(m^2) = m\cdot\varphi(m).$

4) α. $\varphi(n)=\frac{1}{2}n$

$n=2^k\cdot m$, m: περιττός
$\varphi(n)=\varphi(2^k\cdot m)$ #
$(2^k, m)=1$
$\varphi(2^k\cdot m)\cdot\varphi(1) = 1\cdot\varphi(2^k)\cdot\varphi(m)$
$\frac{1}{2}2^k m = \varphi(2^k)\cdot\varphi(m)$
$2^{k-1}m = 2^{k-1}(2-1)\varphi(m)$
$\varphi(m)=m$
m περιττός $\Rightarrow \varphi(m)<m$ με $\varphi(m)=m=1$

Δεν ισχύει για n περιττός
Για $n=2^k\cdot m$
$\varphi(2)=\varphi(2^1\cdot 1)=\frac{1}{2}\cdot 2=1$
$\varphi(2^k)=2^{k-1}(2-1)=2^k\frac{1}{2}$ Άρα για $n=2^k$

β. $\varphi(n)=2n$ Δεν ισχύει όμως $\varphi(n)=\varphi(2n)$
γιατί δεν μπορούμε να έχουμε περίρους διαιρέτες
από n.
$\varphi(n)=\varphi(2n)$
$n=2^k m$, m: περιττός
$\varphi(n)=\varphi(2^k m) \Rightarrow \varphi(2^k m)\varphi(1)=1\cdot\varphi(2^k)\cdot\varphi(m)$
$2n=2^{k+1}m \Rightarrow \varphi(2n)=\varphi(2^{k+1}m)=\varphi(2^{k+1})\cdot\varphi(m)$
Πρέπει, $\varphi(2^k)\cdot\varphi(m)=\varphi(2^{k+1})\cdot\varphi(m)$
Άρα, $\varphi(2^k)=\varphi(2^{k+1}) \Rightarrow 2^{k-1}\cdot(2-1)=2^k(2-1)$
• Άρα, για $k\geq 1$ έχουμε $1=2$ Άτοπο
Πρέπει το n να είναι περιττός
• Για $k=0$, $\varphi(2m)=\cancel{\varphi(2)^1}\cdot\varphi(m)=\varphi(m)$ m: περιττός

γ. $n=2^k\cdot 3^\ell\cdot m$ $\left[\Rightarrow \varphi(m\cdot n)\,\varphi(m,n)=(m,n)\varphi(m)\cdot\varphi(n)\right]$
$(m,2)=1$, $(m,3)=1$ $\Big\}$ $\varphi(3n)=\varphi(2^k\cdot 3^{\ell+1}\cdot m)=\varphi(6n)=\varphi(2^{k+1}\cdot 3^{\ell+1}\cdot m)=$
$\Rightarrow \varphi(2^k)\cdot\varphi(3^{\ell+1})\cdot\varphi(m)=\varphi(2^{k+1})\cdot\varphi(3^{\ell+1})\varphi(m)$
$\Rightarrow \varphi(2^k)=\varphi(2^{k+1}) \Rightarrow 2^{k+1}(2-1)=2^k(2-1) \Rightarrow 1=2$
Άρα, $k=0$

$\varphi(2^2)\cdot\varphi(3^l)\cancel{\varphi(m)} = \varphi(2)\cdot\varphi(3^{l+1})\cancel{\varphi(m)} \Leftrightarrow$

$2\cdot\varphi(3^l) = \varphi(3^{l+1}) \Leftrightarrow$

$2\cdot 3^{l-1}\cancel{(3-1)} = 3^l\cancel{(3-1)} \Leftrightarrow 2=3$ Ατοπο

Αρα $l=0$

Μονος για $n=m$ ισχυει

5) $n = p_1^{k_1}\cdots p_l^{k_l}$

$\varphi(n) = 12 = 2^2\cdot 3$

- $n=p \Rightarrow \varphi(n) = p-1 = 12 \Rightarrow \boxed{n=13}$
- $n=p^2 \Rightarrow \varphi(p^2) = p(p-1) = 12 = 2^2\cdot 3$

  $p=3 \Rightarrow 3\cdot 2 = 6 \neq 12$

  $p=2 \Rightarrow 2\cdot 1 = 2 \neq 12$
- $n=p^3 \Rightarrow \varphi(p^3) = p^2(p-1) = 12 = 2^2\cdot 3$ Αδυνατη
- $n=p\cdot q \Rightarrow \varphi(pq) = \varphi(p)\cdot\varphi(q) = (p-1)(q-1) = 12 = 2^2\cdot 3$

  $p=2,\ q=13 \Rightarrow \varphi(2)\cdot\varphi(13) = 12$

  $p=3,\ q=7 \Rightarrow \varphi(3)\cdot\varphi(7) = 6\cdot 2 = 12$
- $n=p^2\cdot q \Rightarrow \varphi(p^2 q) = \varphi(p^2)\varphi(q) = 12 \Rightarrow$

  $\Rightarrow p(p-1)(q-1) = 12 \Rightarrow p=2$ και $p=7$
- $n = p^2\cdot q^2 \Rightarrow \varphi(n) = \varphi(p^2q^2) = p(p-1)q(q-1)$

Θελουμε $p(p-1)q(q-1) = 12 \Rightarrow p=2$ και $q=3$

αρα $\boxed{n=36}$

- $n=p^3 q \Rightarrow \varphi(n) = p^2(p-1)(q-1) = 12$ Αδυνατη
- $n=pqr \Rightarrow \varphi(n) = \varphi(q)\varphi(r)\varphi(p) = 12$

  $q=3,\ p=2,\ r=7 \Rightarrow n = 2\cdot 3\cdot 7 = 42$