9/12/2016

i) $\varphi(m) = \varphi(m \cdot n)$ με $n > 1 \Rightarrow n = 2$ και m περιττός

$n = 2$, m περιττός $\Rightarrow (2, m) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(n) \cdot \varphi(m) = 1\,\varphi(m)$

n περιττός $\Rightarrow \varphi(n) > 1$

$n = p_1^{k_1} \dots p_\ell^{k_\ell}$ $\quad p_1 < p_2 < \dots < p_\ell$ περιττός πρώτος

$m = q_1^{r_1} \dots q_t^{r_t}$ $\quad q_1 < q_2 < \dots < q_t$ πρώτοι

$n = p_1^{k_1} \dots p_\ell^{k_\ell} \dots S_1^{x_1} \dots S_y^{x_y}$ p_i και S_j πρώτοι

$m = q_1^{r_1} \dots q_t^{r_t} S_1^{x_1'} \dots S_y^{x_y'}$

q_i πρώτα διαφορετικοί από p_i και S_j

$(n, m) = 1 = S_1^{\min(x_1, x_1')} \cdot S_2^{\min(x_2, x_2')} \dots S_y^{(x_y, x_y')}$

$\phi(m) = \cancel{q_1^{r_1 - 1} \dots q_t^{r_t - 1}} S_1^{x_1' - 1} \dots S_y^{x_y' - 1} \cancel{(q_1 - 1) \dots (q_t - 1)(S_1 - 1) \dots (S_y - 1)}$ $(+)$

$\phi(mn) = \varphi(p_1^{k_1} \dots p_\ell^{k_\ell} q_1^{r_1} \dots q_t^{r_t} S_1^{x_1 + x_1'} \dots S_y^{x_y + x_y'})$

$= p_1^{k_1 - 1} \dots p_\ell^{k_\ell - 1} \cancel{q_1^{r_1 - 1} \dots q_t^{r_t - 1}} S_1^{x_1 + x_1' - 1} \dots S_y^{x_y + x_y' - 1}$

$= (p_1 - 1) \dots (p_\ell - 1) \cancel{(q_1 - 1) \dots (q_t - 1)(S_1 - 1) \dots (S_y - 1)}$ $(++)$

$(+) = (++) \Rightarrow p_1^{k_1 - 1} \dots p_\ell^{k_\ell - 1} S_1^{x_1} \dots S_y^{x_y} (p_1 - 1) \dots (p_\ell - 1) = 1$

$k_1 = 1, \dots, k_\ell = 1 \quad x_1 = 0 = \dots = x_y$

$p_1 < p_2 < \dots < p_\ell$ πρώτοι $\quad p_1 - 1 = 1 \Rightarrow p_1 = 2$

άρα $2 < p_2 \Rightarrow 2 - 1 < p_2 - 1$

$\Rightarrow 1 < p_2 - 1 < p_3 - 1 < \dots$

Αρα, $n = 2^{1}$

$m = 2^k q_1^{r_1} \dots q_\ell^{r_\ell}$

$\phi(2m) = \varphi(m)$

$2 < q_1 < \dots < q_\ell$ περιττοί

$\varphi(2^{k+1} q_1^{r_1} \dots q_\ell^{r_\ell}) = 2^k q_1^{r_1 - 1} \dots q_\ell^{r_\ell - 1}(q_1 - 1) \dots (q_\ell - 1)$

$\phi(m) = 2^{k-1} q_1^{r_1-1} \dots q_\ell^{r_\ell - 1}(q_1 - 1) \dots (q_\ell - 1)$

Πρέπει να δείξω ότι $2^k = 2^{k-1} \Rightarrow m$ είναι περιττός και $n = 2$

Άσκηση 9

$$\frac{1}{5}a^5 + \frac{1}{3}a^3 + \frac{7}{15}a \in \mathbb{Z}$$

$$\frac{1}{15}(3a^5 + 5a^3 + 7a) \in \mathbb{Z} \Leftrightarrow$$

$\Leftrightarrow$ $3a^5 + 5a^3 + 7a$ είναι πολλαπλάσιο του 15

$3a^5 + 5a^3 + 7a \equiv 0 \bmod 15$

$(5,3) = 1$ $\quad a^5 \equiv a \bmod 5 \Rightarrow 3a^5 \equiv 3a \bmod 15$ (+)

$5a^3 \equiv 5a \bmod 15$ (++)

$a^3 \equiv a \bmod 3$

άρα ο $3a^5 + 5a^3 + 7a$ διαιρείται με το 15

$\varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$

$3a^5 + 5a^3 \overset{(+)}{\underset{(++)}{\equiv}} (3a + 5a) \bmod 15$

$3a^5 + 5a^3 + 7a \equiv (3a + 5a + 7a) \bmod 15 \equiv 15a \bmod 15 \equiv 0 \bmod 15$

ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Ασκησεις #6 ΤΜΗΜΑ ΠΕΡΙΤΤΩΝ

1) Να βρεθουν: $ord_{11}(2)$, $ord_{17}(3)$, $ord_{11}(8^{2015})$

2) Βρειτε τους φυσικους n ωστε $7^n \equiv 4 \bmod 17$

3) Για n περιττο, δειξτε οτι $2^n + 3^n \not\equiv 0 \bmod 17$

4) Εστω p και q διαφορετικοι περιττοι πρωτοι και a ακεραι
με $(a, pq) = 1$. Δειξτε οτι $a^{\frac{\varphi(pq)}{2}} \equiv 1 \bmod pq$

5) Να λυθουν οι εξισωσεις

$3x \equiv 7 \bmod 17$ $\qquad$ $8x \equiv 3 \bmod 11$

6) Να λυθει το συστημα στους ακεραιους

$$\begin{aligned} 5x &\equiv 3 \bmod 7 \\ 4x &\equiv 2 \bmod 5 \\ x &\equiv 2 \bmod 3 \end{aligned}$$

7) Να βρεθει ο φυσικος n ωστε α) $\varphi(n) = \frac{1}{2} n$

β) $\varphi(n) = \varphi(2n)$

γ) $\varphi(n) = 2n$

Άσκηση 2: $n = ;$ $\quad 7^n \equiv 4 \bmod 17$

$7 = 3^k \qquad 3 \quad 9 \quad \overset{-7}{10} \quad -4 \quad -12 \equiv 5 \quad 15 \equiv -2 \quad -6 \quad -1$

$\qquad\qquad -3 \quad -9 \quad \underset{11}{7} \quad \underset{12}{4} \quad -5 \quad 2 \quad 6 \quad 1$

$7 \equiv 3^{11} \bmod 17 \Rightarrow 7^n \equiv 11^n \bmod 17$

$4 \equiv 3^{12} \bmod 17$

$7^n \equiv 3^{11} \equiv 4 \equiv 3^{12} \bmod 17$

$3^{11n} \equiv 3^{12} \bmod 17$

$ord_{17}(3) = 16$

$11n \equiv 12 \bmod 16$

$-5n \equiv 12 \bmod 16$

$-3 \cdot 15n \equiv 3 \cdot 12 \bmod 16$

$n \equiv 4 \bmod 16$

Ασκήσεις #6

Α 1) Να βρεθούν : 1) $ord_{11}(2)$, 2) $ord_{17}(3)$, 3) $ord_{11}(8^{2015})$

1) $ord_{11}(2)$

$(11,2)=1$

Πιθανές: 2, 5, 10

$\varphi(11)=10$

Ψάχνει $s<10$ με $s|10$ ώστε $ord_{11}(2)=s$

$s|10 \Rightarrow s=1,2,5,10$

$2^4=16\equiv 5 \mod 11$

$2^5=32\equiv -1 \mod 11$

$(2^5)^2\equiv(-1)^2 \mod 11 \Rightarrow \boxed{2^{10}\equiv 1 \mod 11}$

άρα $ord_{11}(2)=10$ πρωταρχική το 2

2) $ord_{17}(3)$

$(17,3)=1$

Πιθανές = 2, 4, 8, 16

$\varphi(17)=16$

$3^2=9$

$3^3=27\equiv 10 \mod 17$

$3^4=81\equiv 13 \mod 17\equiv -4 \mod 17$

$(3^4)^2\equiv(-4)^2 \mod 17 \Rightarrow 3^8\equiv 16 \mod 17 \Rightarrow \boxed{3^8\equiv(-1) \mod 17}$

$(3^8)^2\equiv(-1)^2 \mod 17$

$3^{16}\equiv 1 \mod 17$

άρα $ord_{17}(3)=16$ πρωταρχική το 3

3) $ord_{11}(8^{2015})=ord_{11}(2^{3\cdot 2015})=2$