1) (x,y) ώστε $x+y=100$, $x,y\geq 0$ και $x=7a$, $y=11b$.

$7a+11b=100$.

$(7,11)=1 \mid 100 \Rightarrow$ έχει ακέραιες λύσεις.

$7(-3)+11\cdot(-2)=1$.

Λύσεις: $a=-3\cdot 100+11t$.

$b=+2\cdot 100-7t=+200-7t$

$x,y\geq 0 \Rightarrow -300+11t\geq 0 \nrightarrow 11t\geq 300 \nrightarrow t\geq \frac{300}{11}$ ή $t\geq 28$.

$+200-7t\geq 0 \quad 200\geq 7t \nrightarrow t\leq \frac{200}{7}$ ή $28\geq t$.

Μοναδική τιμή $t=28$ για να είναι x,y φυσικοί.

Άρα: $x=(-300+11\cdot 28)\cdot 7=\dots$

$y=(200-7\cdot 28)\cdot 11=\dots$

) $\left.\begin{matrix}3x+5y+7z=560\\ 9x+25y+49z=2920\end{matrix}\right\}$ Ακέραιες λύσεις.

$+25y+49z-3(3x+5y+7z)=2920-3\cdot 560 \Rightarrow$

$+28z=1240$

$+14z=620$

4) $=1 \mid 620 \nrightarrow$ έχει ακέραιες λύσεις

$5y + 14z = 1 \mid 620$ $\quad y = 3 \cdot 620 + 14t = 1860 + 14t$

$5 \cdot 3 + 14 \cdot (-1) = 1$ $\quad z = (-1) \cdot 620 - 5t = -620 - 5t$

Αντικατάσταση:

$3x + 5(1860 + 14t) + 7(-620 - 5t) = 560$

$3x + 9300 + 70t - 4340 - 35t = 560$

$3x + 35t = -4400$

$(3, 35) = 1 \mid -4400 \Rightarrow$ έχει ακέραιες λύσεις.

$3 \cdot 12 + 35 \cdot (-1) = 1$

$x = 12(-4400) + 35s$, $s \in \mathbb{Z}$

$t = (-1)(-4400) - 3s$

Αντικαθιστούμε το t στο y και z. Άρα η λύση εξαρτάται από το $s \in \mathbb{Z}$.

$\mathbb{Z}_{15} = \{[0], [1], \ldots, [14]\}$

$[a]$ αντιστρέψιμη: $\Leftrightarrow (a, 15) = 1$.

$\{[1], [2], [4], [7], [8], [11], [13], [14]\}$

Αντίστροφοι: $[a] \odot [b] = [0] = [15]$.

$[1]^{-1} = [1]$ και $[-1]^{-1} = [-1]$.

$[2]^{-1} = [a] \Leftrightarrow 2a = 1 \bmod 15$.

$[8] : 2 \cdot 8 = 1 \bmod 15$

$[4]^{-1} = [4]$

$[7]^{-1} = [13]$

$[11]^{-1} = [11]$

4) $\mathbb{Z}_{17} = \{[0], [\blacksquare], [3^1], \ldots, [3^{10}]\}$. $\varphi(17)$

③, $3^2 = 9$, $3^3 = 27 \bmod 17 = 10$, $3^4 = 3 \cdot 10 \bmod 17 = 13$, $3^5 = 3 \cdot 13 \bmod 17 = 39 \bmod 17 = 5 \bmod 17$

$3^6 = 3 \cdot 5 \bmod 17 = 15 \bmod 17$

$3^7 = 3 \cdot 15 \bmod 17 = 45 \bmod 17 = 11 \bmod 17$

$3^8 = 3 \cdot 11 \bmod 17 = 33 \bmod 17 = 16 \bmod 17$.

$3^9 = 3 \cdot 16 \bmod 17 = 48 \bmod 17 = 14 \bmod 17$.

$3^{10} = 3 \cdot 14 \bmod 17 = 42 \bmod 17 = 8 \bmod 17$.

$3^{11} = 3 \cdot 8 \bmod 17 = 24 \bmod 17 = 7 \bmod 17$.

$3^{12} = 3 \cdot 7 \bmod 17 = 21 \bmod 17 = 4 \bmod 17$.

$3^{13} = 3 \cdot 4 \bmod 17 = 12 \bmod 17$.

$3^{14} = 3 \cdot 12 \bmod 17 = 36 \bmod 17 = 2 \bmod 17$

$3^{15} = 3 \cdot 2 \bmod 17 = 6 \bmod 17$.

$3^{16} = 3 \cdot 6 \bmod 17 = 18 \bmod 17 = 1 \bmod 17$.

10) 3^{1000}

Ζητάμε $3^{1000} \bmod 100$

$3^{\varphi(100)} = 1 \bmod 100$.

$(3,100) = 1$.

$\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = 2\varphi(2) 5\varphi(5) = 40$

1000 με το $\varphi(100) = 40 \Rightarrow 1000 = 40 \cdot 25$.

$3^{1000} = (3^{40})^{25} \equiv 1^{25} \bmod 100 \equiv 1 \bmod 100$

Άρα τα δύο τελευταία είναι 0,1.

Wilson: $(n-1)! = -1 \bmod n$.

$x^2 + 1 = 0$. Η λύση είναι $\pm i$ φανταστικός

ΘΕΩΡΗΜΑ:
Έστω p περιττός πρώτος. Υπάρχει $a \in \mathbb{Z}$ με $a^2 = 1 \bmod p \iff p = 1 \bmod 4$ ή $p = 4k+1$.

$\Leftarrow$ Έχουμε ότι $p = 4k+1$. Βρες a με $a^2 \equiv 1 \bmod p$. $p - 1 = 4k$.

$1, 2, \ldots, 2k, 2k+1, \ldots, 4k-1, 4k$.

$1 + 4k = p = 0 \bmod p \Leftrightarrow -1 = 4k \bmod p$.

$-2 = (4k-1) \bmod p$.

$2k + 2k + 1 = 0 \bmod p$. Άρα $2k+1 = -2k \bmod p$.

$1 \cdot 2 \cdot \ldots \cdot 2k \cdot (2k+1) \cdot \ldots \cdot (4k-1) \cdot 4k = (p-1)! \equiv -1 \bmod p$

$(-1) \cdot 2k \quad (-1) \cdot 2 \quad (-1) \cdot 1 = ((2k)!)^2 \cdot (-1)^{2k}$

$((2k!))^2 \equiv -1 \bmod p \Rightarrow a = 2k = \frac{4k}{2} = \frac{p-1}{2}$. Άρα $a = \frac{p-1}{2}$.

$\Rightarrow$ Υποθέσαμε ότι ∃a με $a^2 \equiv -1 \bmod p$. Θέσαμε $p = 4k+1$.

$(a,p) = 1 \Rightarrow a^{p-1} \equiv 1 \bmod p \Rightarrow \left(a^{\frac{p-1}{2}}\right)^2 = 1 \bmod p$. ή $(a^2)^{\frac{p-1}{2}} \equiv 1 \bmod p$.

Όμως $a^2 = -1 \bmod p$, άρα:

$(-1)^{\frac{p-1}{2}} = 1 \bmod p$.

Αν είχαμε $p = 4k+3 \Rightarrow \frac{p-1}{2} = \frac{4k+2}{2} = 2k+1$, περιττός.

Άρα τότε $(-1)^{2k+1} = -1 \bmod p \equiv 1 \bmod p$: ΑΔΥΝΑΤΟ.

Σαξη αντιδειγμα: κλάσης.

Euler: Αν $(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \bmod m$
(a, m: πρώτος)

π.χ. $p = 7$: $\varphi(p) = 6 \Rightarrow [a]_7^{\varphi(p)} = [a]_7^6 = [1]_7$.

$[4]_7 \rightarrow [4^2]_7 = [2]_7 \rightarrow [4^3]_7 = [4]_7 \cdot [2]_7 = [8]_7 = 1 \bmod 7$.

$4^3 = 1 \bmod 7$, αλλά από Euler : $4^6 = 1 \bmod 7$.

Δηλαδή ο $3 < \varphi(7) = 6$ ώστε να έχουμε $4^3 \equiv 1 \bmod 7$.

ΟΡΙΣΜΟΣ:
Έστω $n > 1$ και $a \in \mathbb{Z}^*$ με $(a,n) = 1$. Ονομάζουμε τάξη του a modulo n τον ελάχιστο φυσικό s ώστε $a^s \equiv 1 \bmod n$.
Γράφουμε $s = \text{ord}_n a$.

Παρατήρηση:
Γνωρίζουμε ότι $a^{\varphi(n)} \equiv 1 \bmod n$
Εδώ όμως ψάχνουμε τον μικρότερο με αυτή την ιδιότητα.

π.χ. Να βρεθεί η τάξη του 12 βάσει mod 55.

$(12, 55) = 1 \Rightarrow 12^{\varphi(55)} \equiv 1 \bmod 55$: Υπάρχει μικρότερος από $\varphi(55)$?. $= 40$

$12^2 \equiv 144 \equiv 34 \bmod 55$.
$12^3 \equiv 34 \cdot 12 \bmod 55 \equiv 23 \bmod 55$.
$12^4 \equiv 23 \cdot 12 \bmod 55 \equiv 1 \bmod 55$.
$\text{ord}_{55} 12 = 4$

π.χ. $p = 17$ $\text{ord}_{17} 3 = 16 = \varphi(17)$ και μάλιστα κάθε αντιστοιχεί μια κλάση στο $\mathbb{Z}_{17}$ ήταν δύναμη του 3.

ΟΡΙΣΜΟΣ:
Έστω $a \in \mathbb{Z}^*$ και $n > 1$ φυσικός με $(a,n) = 1$.
Αν $\text{ord}_n a = \varphi(n)$, τότε ο a καλείται πρωταρχική κλάση ή ρίζα mod n.

$x^{\varphi(p)} - 1 \equiv 0 \bmod p$.

π.χ. Το 3 στο mod 7 είναι πρωταρχική ρίζα διότι $ord_7 3 = 6$.

ΙΔΙΟΤΗΤΕΣ:

n φυσικός >1 και $a, b \in \mathbb{Z}^*$ με $(a,n)=1$.

1) $a \equiv b \bmod n \not\Rightarrow ord_n a = ord_n b$.

Προσοχή: $ord_7(2) = 3 = ord_7(4)$: $2 \neq 4 \bmod 7$.

2) $a^m \equiv a^{\hat{}} \bmod n \Leftrightarrow m \equiv n \bmod (ord_n a)$

3) Αν $a^m = 1 \bmod n \Leftrightarrow ord_n a \mid m$.

Άρα $ord_n(a)$ διαιρεί το $\varphi(n)$.