Πρόταση: Έστω $\alpha \in \mathbb{Z}$ ΣΥΝΘΕΤΟΣ. Τότε $\alpha \nmid (\alpha-1)!+1$

Απόδειξη: Έστω ότι $\alpha \mid (\alpha-1)!+1$ κ' $\alpha = rs$ με $2 \leq r,s$

Έχουμε $r \leq \alpha-1$ (για $s \geq 2$, άρα $r = \frac{\alpha}{s} < \alpha$)

Συνεπώς $r \mid (\alpha-1)!$, γιατί είναι ένας από τους παράγοντες

Αφού $r \mid \alpha$, από (*), $r \mid (\alpha-1)!+1$

Συνεπώς, $\left\{ \begin{array}{l} r \mid (\alpha-1)! \\ r \mid (\alpha-1)!+1 \end{array} \right. \xRightarrow{\text{ΑΦΑΙΡΕΣΗ}} r \mid 1$, αντίφαση

Π.χ. $\alpha=4$, $(\alpha-1)!+1 = 3!+1 = 7$ κ' $4 \nmid 7$

$\alpha = 6$ $(6-1)!+1 = 5!+1 = 121$ κ' $6 \nmid 121$, γιατί $2 \nmid 121$

ΠΡΟΤΑΣΗ: Έστω $\alpha \in \mathbb{Z}$ πρώτος. Τότε $\alpha \mid (\alpha-1)!+1$

Απόδειξη: Αφού α πρώτος, $U(\mathbb{Z}/\alpha) = \{[1]_\alpha, [2]_\alpha, [3]_\alpha, \dots, [\alpha-1]_\alpha\}$

ΙΣΧΥΡΙΣΜΟΣ: Έστω $c \in \mathbb{Z}$ με $1 \leq c \leq \alpha-1$ κ' $[c]_\alpha^{-1} = [c]_\alpha$

Τότε $c=1$ ή $c=\alpha-1$

Απόδειξη: $([c]_\alpha)^{-1} = [c]_\alpha \Rightarrow ([c]_\alpha)^2 = [1]_\alpha \Rightarrow [c^2]_\alpha = [1]_\alpha \Rightarrow$

$[c^2-1]_\alpha = [0]$

$\Rightarrow \alpha \mid c^2-1 \Rightarrow \alpha \mid (c-1)(c+1) \xRightarrow[\text{κ' } 1 \leq c \leq \alpha-1]{\alpha \text{ πρώτος}} c=1$ ή $c=p-1$

Θεωρούμε το γινόμενο.

$$A = [2]_a[3]_a[4]_a \cdots [a-2]_a \in U(\mathbb{Z}/a)$$

<u>Ισχυρισμός 2</u>: $A = [1]_a$

<u>Απόδειξη</u>: Έχουμε $([2]_a)^{-1} \in \{[3]_a, \dots, [a-1]_a\}$ από τον Ισχυρισμό 1. Άρα αφαιρώντας το $[2]_a$ κ' το $([2]_a)^{-1}$ από το σύνολο έχουμε ξανά γινόμενο ίσο με A. Συνεχίζουμε με επαγωγή.

Συνεπώς, $[(a-1)!]_a = [1]_a A [a-1]_a \overset{\text{Ισχ 2}}{=\!=\!=} [1]_a[1]_a[a-1]_a = [a-1]_a = [-1]_a$

Συνεπώς, $[(a-1)!]_a = [-1]_a \Rightarrow a \mid (a-1)! + 1$, άρα $(a-1)! \equiv -1 \mod a$

<u>Πόρισμα</u>: (Θεώρημα Wilson). Έστω $a \geq 2$. Τότε a πρώτος ανν $(a-1)! \equiv -1 \mod a$

<u>Απόδειξη</u>: Άμεσο από τις δύο προηγούμενες προτάσεις.

π.χ. $a = 7$

$U(\mathbb{Z}/7) = \{[1]_7, [2]_7, \dots, [6]_7\}$

Έχουμε $([2]_7)^{-1} = [4]_7$, $([3]_7)^{-1} = [5]_7$

$([1]_7)^{-1} = [1]_7$, $([6]_7)^{-1} = ([-1]_7)^{-1} = [-1]_7 = [6]_7$

κ' το A της απόδειξης.

$$A = [2]_7[3]_7[4]_7[5]_7 = ([2]_7[4]_7)([3]_7[5]_7) = ([2]_7([2]_7)^{-1})([3]_7([3]_7)^{-1}) = [1]_7[1]_7 = [1]_7$$

Θ. Wilson: Αν $a \in \mathbb{Z}$, $a \geq 2$. τότε α πρώτος αν $(a-1)! \equiv -1 \mod a$ ισοδύναμα αν $[(a-1)!]_a = [-1]_a$

Π.χ Υπολογίζε το υπόλοιπο της Ευκλείδειας Διαίρεσης του $27!$ με το 31.

Παρατήρηση: Έστω α, n ακέραιοι με $n \geq 2$ κ' r ακέραιος ώστε $[a]_n = [r]_n$ κ' $0 \leq r \leq n-1$. Τότε το r είναι το υπόλοιπο της Ευκλείδειας Διαίρεσης του α με το n. Ο λόγος είναι ότι αν r' το υπόλοιπο, έχουμε $[a]_n = [r']_n$, $0 \leq r \leq n-1$ κ' $0 \leq r' \leq n-1$, έπεται $r = r'$.

Συνέχεια πχ: Βήμα 1ο: 31 πρώτος, γιατί $\sqrt{31} = 5$ κ' κάτι κ' οι πρώτοι ≤ 6, δηλαδή 2, 3, 5 δεν διαιρούν το 31. Άρα από Πρόταση, 31 πρώτος

Βήμα 2ο: Από Θ. Wilson $[(30)!]_{31} = [-1]_{31}$

$\Rightarrow [30]_{31}[29]_{31}[28]_{31}[27!]_{31} = [-1]_{31}$

$\Rightarrow [-1]_{31}[-2]_{31}[-3]_{31}[27!]_{31} = [-1]_{31}$

$\Rightarrow [-6]_{31}[27!]_{31} = [-1]_{31}$

$\Rightarrow [25]_{31}[27!]_{31} = [-1]_{31}$. $(*)$

Βήμα 3ο: Αφού 31 πρώτος, $\text{ΜΚΔ}(25,31) = 1$, άρα το $[25]_{31}$ αντιστρέφεται στο $\mathbb{Z}/_{31}$. Υπολ. με Ευκλ. ~~Διαίρεση~~ Αλγ. το $([25]_{31})^{-1}$.

$31 = 1 \cdot 25 + 6$

$25 = 4 \cdot 6 + 1$

$6 = 6 \cdot 1 + 0$

Έχουμε $1 = 25 - 4 \cdot 6 = 25 - 4(31 - 1 \cdot 25)$

Συνεπώς $[1]_{31} = [5]_{31}[25]_{31} - [4]_{31}[31]_{31}$

Συνεπώς $([25]_{31})^{-1} = [5]_{31}$

Πολλαπλ. την $(*)$ με $([25]_{31})^{-1}$ έχουμε

$([25]_{31})^{-1}[25]_{31}[27!]_{31} = ([25]_{31})^{-1}[-1]_{31} \Rightarrow$

$\Rightarrow [1]_{31}[27!]_{31} = [5]_{31}[-1]_{31} \Rightarrow [27!]_{31} = [-5]_{31} = [26]_{31}$

Συνεπώς, από την Παρατήρηση, το υπόλοιπο της Ευκλ. Διαιρ. του $27!$ με το 31 είναι ίσο με 26, γιατί $0 \leq 26 \leq 30$

Υπενθύμιση: Αν $a, b \in \mathbb{Z}$ με $n \geq 2$ κ' $[a]_n, [b]_n \in U(\mathbb{Z}/n)$, τότε κ' $[ab]_n \in U(\mathbb{Z}/n)$. Εύκολα επαληθεύεται $([ab]_n)^{-1} = ([a]_n)^{-1}([b]_n)^{-1}$

Θεώρημα: (Fermat-Euler). Έστω $n \geq 1$ κ' $a \in \mathbb{Z}$ με $\text{ΜΚΔ}(a,n)=1$.
Τότε $a^{\phi(n)} \equiv 1 \mod n$

Απόδειξη: Έστω $\{x_1, \dots, x_{\phi(n)}\}$ ένα περιορισμένο σύστημα υπολοίπων mod n.
Δηλαδή $U(\mathbb{Z}/n) = \{[x_1]_n, [x_2]_n, \dots, [x_{\phi(n)}]_n\}$

Αφού $\text{ΜΚΔ}(a,n)=1$, από πρόταση κ' το $\{ax_1, ax_2, \dots, ax_{\phi(n)}\}$ είναι περιορισμένο σύστημα υπολ. mod n. Επομένως, $\exists$ συνάρτηση $\sigma: \{1, \dots, \phi(n)\} \to \{1, \dots, \phi(n)\}$ με σ 1-1 κ' επί, ώστε $[ax_i]_n = [x_{\sigma(i)}]_n$ $\forall i$ με $1 \leq i \leq n$.
Πολλαπλασιάζοντας για $1 \leq i \leq n$, έπεται $[ax_1]_n[ax_2]_n \cdots [ax_{\phi(n)}]_n =$
$= [x_1]_n[x_2]_n \cdots [x_{\phi(n)}]_n$.

$\Rightarrow [a]_n[x_1]_n[a]_n[x_2]_n = [x_1x_2 \cdots x_{\phi(n)}]_n \Rightarrow ([a]_n)^{\phi(n)}[x_1x_2 \cdots x_{\phi(n)}]_n =$
$[x_1x_2 \cdots x_{\phi(n)}]_n$. (*)

Από πρόταση το $[x_1x_2 \cdots x_{\phi(n)}]_n$ είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}/n$, σαν γινόμενο αντιστρεψίμων. Συνεπώς, $\exists$ ακέραιος B με $([x_1 \cdots x_{\phi(n)}]_n)^{-1} = [B]_n$
Πολλαπλασιάζοντας την (*) με $[B]_n$ έχουμε:

$([a]_n)^{\phi(n)}([x_1 \cdots x_{\phi(n)}]_n)[B]_n = [x_1x_2 \cdots x_{\phi(n)}]_n[B]_n \Rightarrow$
$\Rightarrow ([a]_n)^{\phi(n)} = [1]_n$

$\leftrightarrow$

$n \geq 2$, $\text{ΜΚΔ}(a,n)=1 \Rightarrow a^{\phi(n)} \equiv 1 \mod n$

π.χ. $n=3, a=2$ $\quad \phi(n) = \phi(3) = 3(1-\frac{1}{3}) = 2$ κ' $([2]_3)^{\phi(3)} = ([2]_3)^2 =$
$= [4]_3 = [1]_3$

π.χ. $n=5$ τότε $\phi(5)=4$ κ' $([1]_5)^4 = [1]_5$, $([2]_5)^4 = [2^4]_5 = [16]_5 = [1]_5$
$([3]_5)^4 = ([3]_5^2)^2 = ([4]_5)^2 = [16]_5 = [1]_5$
$([4]_5)^4 = ([-1]_5)^4 = [(-1)^4]_5 = [1]_5$

π.χ. $n=8$. Τότε $U(\mathbb{Z}/8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ κ' $\phi(8)=\phi(2^3) =$
$= 2^3(1-\frac{1}{2}) = 4$.

$$([1]_8)^4 = [1^4]_8 = [1]_8$$
$$([3]_8)^4 = ([3^2]_8)^2 = ([1]_8)^2 = [1]_8$$
$$([5]_8)^4 = ([-3]_8)^4 = ([-3]_8)^4 = ([(-3)^2]_8)^2 = ([1]_8)^2 = [1]_8$$
$$([7]_8)^4 = ([-1]_8)^4 = [(-1)^4]_8 = [1]_8.$$

π.χ. Ν.δ.ο. $5^{321} \equiv 5 \bmod 561$.

Βήμα 1ο: Υπολογισμός $\phi(561)$

Χρειαζόμαστε ανάλυση του 561 σε γινόμενο πρώτων.

Αφού $3 \mid (5+6+1) = 12 \Rightarrow 561$ πολ/σιο του 3

$$\begin{array}{r|l} 561 & 3 \\ 26 & 187 \\ 21 & \end{array}$$, άρα $561 = 3 \cdot 187$

Έχουμε $1-8+7=0$ που διαιρείται με το 11

Άρα $11 \mid 187$. Συνεπώς, $561 = 3 \cdot 11 \cdot 17$ πρωτογενής ανάλυση.

Συνεπώς, $\phi(561) = \phi(3 \cdot 11 \cdot 17) = 561(1-\frac{1}{3})(1-\frac{1}{11})(1-\frac{1}{17}) = 320$

Βήμα 2ο: Από Θ. Euler-Fermat, αφού $\text{ΜΚΔ}(5, 561) = 1$ έχουμε

$$([5]_{561})^{\phi(561)} = [1]_{561} \Rightarrow [5^{320}]_{561} = [1]_{561}$$

Πολλαπλ. με $[5]_{561}$, έχουμε $[5^{321}]_{561} = [5]_{561}$, συνεπώς

$$5^{321} \equiv 5 \bmod 561.$$

Πρόταση: Έστω $n \geq 2$ κ' $a \in \mathbb{Z}$ με $\text{ΜΚΔ}(a,n)=1$ κ' $k \geq 1$ ακέραιος. Θέτουμε r για το υπόλοιπο της Ευκλ. Διαιρ. του k με το $\phi(n)$. Τότε:

$$a^k \equiv a^r \bmod n$$

(Με τη σύμβαση αν $r=0$ τότε $a^r = 1$)

Απόδειξη: $\exists q \in \mathbb{Z}$ με $q \geq 0$ ώστε $k = q\phi(n) + r$

Συνεπώς, $[a^k]_n = [a^{q\phi(n)+r}]_n = [a^{q\phi(n)}]_n [a^r]_n =$

$= ([a^{\phi(n)}]_n)^q [a^r]_n = [a^r]_n$

γιατί $[a^{\phi(n)}]_n = [1]_n$ από Θ. Euler - Fermat.

Πχ Είδαμε $\phi(561) = 320$. Έστω $a \in \mathbb{Z}$ με $ΜΚΔ(a, 561) = 1$.
Έστω $q \in \mathbb{Z}$ με $q > 0$. Τότε

$$[a^{q \cdot 320}]_{561} = [1]_{561}.$$

κ' $[a^{q \cdot 320 + 1}]_{561} = [a]_{561}$

Παρατήρηση: Είδαμε $561 = 3 \cdot 11 \cdot 17$. Επομένως, $ΜΚΔ(a, 561) = 1$ αν
$3 \nmid a$ κ' $11 \nmid a$ κ' $17 \nmid a$.

Πιο γενικά, αν $n \geq 2$ με πρωτογενή ανάλυση
$n = p_1^{a_1} \cdots p_s^{a_s}$, όπου p πρώτος, $p_i \neq p_j$ για $i \neq j$ κ' $a_i > 0$ $\forall i$
Τότε $ΜΚΔ(b, n) = 1$ αν $p_1 \nmid b$ κ' $p_2 \nmid b$ κ' ... κ' $p_s \nmid b$