Kolejna seria grup skończonych.

Dla $n \geq 2$ wiemy, że "$\cdot_n$" jest działaniem łącznym i przemiennym na $\mathbb{Z}_n$, które ma element neutralny 1.
Ale np. 0 nie ma elementu odwrotnego względem "$\cdot_n$".
Również np. 2 ——— " ——— "4".

Definiujemy: $\mathbb{Z}_n^* := \{k \in \mathbb{Z}_n \mid \underbrace{NWD(k,n) = 1}_{k \text{ i } n \text{ względnie pierwsze}}\}$

ĆW.
(i) $\cdot_n$ jest działaniem $\mathbb{Z}_n^*$ (tj. $(\mathbb{Z}_n^*, \cdot_n)$ jest grupą przemienną.

Jeśli p pierwsza, to $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$ i $|\mathbb{Z}_p^*| = p-1$.

Mała Tw. Fermata
Załóżmy, że $a \in \mathbb{Z}$, p jest liczbą pierwszą i $p \nmid a$.
Wtedy $a^{p-1} \equiv 1 \pmod p$

Dowód
Niech $r := r_p(a)$. Wtedy mamy $a^{p-1} \equiv r^{p-1} \pmod p$.
Czyli możemy przyjąć, że $a = r \in \mathbb{Z}_p$.
$p \nmid a \Rightarrow a \neq 0 \Rightarrow a \in \mathbb{Z}_p^*$.
$|\mathbb{Z}_p^*| = p-1 \xRightarrow{\text{Twierdzenie}} \underbrace{a \cdot_p \dots \cdot_p a}_{p-1 \text{ razy}} = 1$ w $\mathbb{Z}_p^*$ (bo a^{p-1} w $\mathbb{Z}_p^*$)
$\underbrace{a^{p-1}}_{\text{w } \mathbb{Z}} \equiv \underbrace{a \cdot_p \dots \cdot_p a}_{p-1 \text{ razy}} \pmod p \equiv 1 \pmod p$.

Uwaga
Dzięki MTF można łatwo liczyć następujące typu: $r_p(n^m)$, gdzie p to liczba pierwsza i $n, m \in \mathbb{Z}$, bo
n możemy zastąpić przez $r_p(n)$ (tu nic nie urzywamy)
m ——— " ——— $r_{p-1}(m)$ (urzywamy MTF)

Przykład
$r_{17}(172^{165}) = r_{17}(2^5)$, bo $r_{17}(172) = 2$, $r_{16}(165) = 5$
$r_{17}(2^5) = r_{17}(32) = 15$.

TW. Wilsona
Jeśli p jest liczbą pierwszą, to $(p-1)! \equiv (-1) \pmod p$.
Potrzebujemy dwóch lematów.

Lemat 1
Niech $(A, +)$ (notacja oddytywna!) będzie skończoną grupą przemienną, $A = \{a_1, \dots, a_n\}$ i niech $a_1, \dots, a_k \in A$ to będą wszystkie elementy $\sqrt{2}$ A takie, że $a+a=0$ (czyli $ord(a) \leq 2$). Wtedy:

$$\underbrace{a_1 + \dots + a_n}_{\text{suma wszystkich elementów } A} = \underbrace{a_1 + \dots + a_k}_{\text{suma elementów rzędu} \leq 2}$$

Dowód
$\forall a \in A$ mamy $a + a = 0 \iff a = -a$ (elem. odwrotny do a)
Liczymy $a_1 + \dots + a_n = \underbrace{a_1 + \dots + a_k}_{\text{rząd} \leq 2} + \underbrace{a_{k+1} + \dots + a_n}_{\text{rząd} > 2}$
Wtedy $a_{k+1} + \dots + a_n = 0$, bo $\forall a \in \{a_{k+1}, \dots, a_n\}$ $a \neq -a$, czyli w tej $\nearrow$ sumie wszystkie elementy „kasują się nawzajem".

Lemat 2
Niech $p \geq 3$ będzie liczbą pierwszą. Wtedy element $p-1 \in \mathbb{Z}_p^*$ jest jedynym elementem rzędu 2 w grupie $\mathbb{Z}_p^*$.

Dowód
$p \geq 3 \Rightarrow p-1 \neq 1 \Rightarrow ord_{\mathbb{Z}_p^*}(p-1) \geq 2$.
$(p-1) \cdot_p (p-1) = r_p((p-1)^2) = r_p(p^2 - 2p + 1) = 1$ ok
Czyli $ord_{\mathbb{Z}_p^*}(p-1) = 2$. Pokazujemy teraz jedyność.
Weźmy $a \in \mathbb{Z}_p^*$: $ord_{\mathbb{Z}_p^*}(a) = 2$ CEL: $a \overset{?}{=} p-1$.
Wtedy $a \neq 1$ i $r_p(a^2) = a \cdot_p a = 1$, tzn.
$p \mid a^2 - 1 = (a-1)(a+1)$
Ale $a \geq 2 \Rightarrow 1 \leq a-1 < p \Rightarrow p \nmid a-1$.
$p \mid (a-1)(a+1)$, p: pierwsza, $p \nmid a-1$ $\Rightarrow p \mid a+1$. Ale $1 \leq a+1 \leq p$, $p \mid a+1$
$\Downarrow$
$p = a+1 \Rightarrow a = p-1$

Dowód tw Wilsona
Mamy pokazać, że $(p-1)! \equiv -1 \pmod p$
Oczywiście, dla $p=2$ to prawda, więc bez $p \geq 3$
$(p-1)! \equiv \underbrace{1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)}_{\text{produkt wszystkich wszystkich elementów w grupie przemiennej } \mathbb{Z}_p^*} \pmod p$
jedyny element rzędu 2 w $\mathbb{Z}_p^*$
Lemat 1, Lemat 2 $\Rightarrow (p-1)! \equiv p-1 \pmod p \equiv -1 \pmod p$

Uwaga
(1) Prawdziwa (i łatwa do pokazania) jest też implikacja kotra przeciwna do tej w tw Wilsona":
$(n-1)! \equiv -1 \pmod n \Rightarrow n$ jest pierwsza.

(2) Implikacja do tej w MTF nie jest prawdziwa. Tzn. jeśli sformułujemy MTF jako:
p: pierwsza $\Rightarrow \forall a \in \mathbb{Z}$ $a^p \equiv a \pmod p$,
to „$\Leftarrow$" nie jest prawdziwa, tzn. istnieją liczby złożone n takie że $\forall a \in \mathbb{Z}$ $a^n \equiv a \pmod n$
Nazywają się one Liczbami Carmichaela.
Najmniejszą L.C. jest 561. Dopiero w 1994 r. pokazano, że jest ∞ wiele L.C.