Monitoria:

Ex 8: Queremos que $18! \equiv -1 \pmod{437}$ (*)

Temos $437 = 19 \cdot 23$. Então, já sabemos que provar (*) é equiv. a provar que

$$437 \mid (18! + 1) \quad (**)$$

Na monitoria passada vimos que é suficiente provar que

$$19 \mid (18! + 1) \quad \text{e} \quad 23 \mid 18! + 1$$

Como 19 é primo, pelo teo. de Wilson,

$$(19-1)! \equiv -1 \pmod{19} \iff$$

$$18! + 1 \equiv 0 \pmod{19} \iff 19 \mid (18! + 1).$$

Temos também que 23 é primo. Então, novamente pelo teo. de Wilson:

$$(23-1)! \equiv -1 \pmod{23} \iff$$

$$22! \equiv -1 \pmod{23} \iff 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv -1 \pmod{23},$$

$\Leftrightarrow \quad 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv -1 \pmod{23}$.

Repare que $22 \equiv -1 \pmod{23}$, $21 \equiv -2 \pmod{23}$,

$20 \equiv -3 \pmod{23}$ e $19 \equiv -4 \pmod{23}$. Então,

$22 \cdot 21 \cdot 20 \cdot 19 \equiv 2 \cdot 3 \cdot 4 = 24 \pmod{23}$ e

$24 \equiv 1 \pmod{23}$.

Então, pelo exposto,

$22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv -1 \pmod{23} \Leftrightarrow$

$24 \cdot 18! \equiv -1 \pmod{23} \Leftrightarrow 18! \equiv -1 \pmod{23} \Leftrightarrow$

$23 \mid 18! + 1$.

Teorema de Euler: Sejam a e n inteiros com $n \geq 1$, tais que $mdc(a, n) = 1$. Então,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Definição: Para cada inteiro $n \geq 1$, indicaremos por $\phi(n)$ o número de inteiros positivos menores ou iguais a n tais que $mdc(x, n) = 1$, $1 \leq x \leq n$

obs: $\{1, \ldots, n-1\}$

Demonstração (Teorema de Euler)

Dado $n \geq 1$, considere o conj. de números entre 1 e $(n-1)$ que são rel. primos com n.

Vamos denotar esse conj como

$$A = \{x_1, \ldots, x_t\}$$

ie, $\text{mdc}(x_i, n) = 1$, $1 \leq x_i \leq n-1$

Agora, dado outro número a tal que $\text{mdc}(a, n) = 1$, consideremos o seguinte conj.

$B = \{x_1 a, \ldots, x_t a\}$

Como $x_i a$ é relativamente primo com n. (ex 5 (ii) - pág 69), o resto da divisão de $x_i a$ por n é um dos elementos de A.

De fato, note que pelo alg. de Divisão $x_i a = nq + r$, $0 \leq r < n$. Veja que $A \subseteq \{0, \ldots, n-1\}$. Considere que $r \notin A$, então $mdc(r, n) = d \neq 1$. Daí, $d \mid r$ e $d \mid n \Rightarrow$

$d \mid x$ e $d \mid n \Rightarrow d \mid x + nq = x_i a$. Logo

$mdc(x_i a, n) \geq d$, contradição.

Agora, como $x_i a \equiv x_j a \pmod{n} \iff$ $(i \neq j)$

$x_i \equiv x_j \pmod{n}$ e não podemos ter que

$x_i \equiv x_j \pmod{n}$, devemos ter que os elementos de B são congruentes aos elementos de A de modo biunívoco, ie, cada elemento de A é congruente a um único elemento de B.

Desse modo,

$$x_1 a \equiv x_{i_1} \pmod{n}$$

$$x_2 a \equiv x_{i_2} \pmod{n}$$

$$\vdots$$

$$x_t a \equiv x_{i_t} \pmod{n}$$

em que $x_{i_1}, \ldots, x_{i_t}$ são os elementos de A.

Com isso,

$$(x_1 \cdots x_t)\, a^t \equiv x_1 \cdots x_t \pmod{n}.$$

Como $mdc(x_i, n) = 1$ então,

$$mdc(x_1 \cdots x_t, n) = 1$$

Daí,

$$(x_1 \cdots x_t)\, a^t \equiv (x_1 \cdots x_t) \pmod{n} \Rightarrow$$

$$a^t \equiv 1 \pmod{n}$$

Observe que $A = \{x_1, \ldots, x_t\}$, tal que $1 \leq x_i \leq (n-1)$ e $mdc(x_i, n) = 1$. Percebe assim, que $t = \phi(n)$.