72. Recorrendo ao Pequeno Teorema de Fermat, mostre que:

(a) $a^{21} \equiv a \pmod{15}$, para todo o inteiro a;

(b) $a^{13} \equiv a \pmod{273}$, para todo o inteiro a;

(c) $a^{12} \equiv 1 \pmod{35}$, para todo o inteiro a tal que m.d.c.$(a, 35) = 1$.

Teorema: Se p é primo e $p \nmid a$ então $a^{p-1} \equiv 1 \pmod{p}$

↳ Pequeno Teorema de Fermat (PTF)

Corolário Se p é primo então $a^p \equiv a \pmod{p}$

a) $15 = 3 \times 5$. Vamos trabalhar por casos

- $3 \nmid a$ e $5 \nmid a$

Do PTF

$$a^2 \equiv 1 \pmod{3}$$
$$a^{20} \equiv 1^{10} \pmod{3}$$
$$a^{21} \equiv a \pmod{3}$$

$$a^4 \equiv 1 \pmod{5}$$
$$a^{20} \equiv 1^5 \pmod{5}$$
$$a^{21} \equiv a \pmod{5}$$

Resulta que $3 \mid a^{21} - a$ e $5 \mid a^{21} - a$

Como m.d.c $(3,5) = 1$ então $15 \mid a^{21} - a$

Portanto $a^{21} \equiv a \pmod{15}$

- $3 \mid a$ e $5 \nmid a$

  $5 \nmid a \Rightarrow a^{21} \equiv a \pmod{5}$ (raciocínio anterior)

  $3 \mid a \Rightarrow 3 \mid a^{21} - a$ (não necessita PTF)

  Como m.d.c $(3,5) = 1$ então $15 \mid a^{21} - a$

- $3 \nmid a$ e $5 \mid a$ análogo

- $3 \mid a$ e $5 \mid a$ análogo

b) Queremos ver que $a^{13} \equiv a \pmod{273}$

$273 = 3 \times 7 \times 13$

- $3 \mid a \Rightarrow 3 \mid a^{13} - a$

  $3 \nmid a$ aplique-se o PTF

  $a^{2} \equiv 1 \pmod{3} \Rightarrow a^{12} \equiv 1^{6} \pmod{3}$

  $\Rightarrow a^{13} \equiv a \pmod{3}$

  Em qualquer caso $a^{13} \equiv a \pmod{3}$

- $7 \mid a \Rightarrow 7 \mid a^{13} - a$

  $7 \nmid a \Rightarrow$ aplique-se o PTF

  $a^{6} \equiv 1 \pmod{7} \Rightarrow a^{12} \equiv 1^{2} \pmod{7}$

  $\Rightarrow a^{13} \equiv a \pmod{7}$

  Em qualquer caso $a^{13} \equiv a \pmod{7}$

- $13 \mid a \Rightarrow 13 \mid a^{13} - a$

  $13 \nmid a \Rightarrow a^{12} \equiv 1 \pmod{13} \Rightarrow a^{13} \equiv a \pmod{13}$

  Em qualquer caso $a^{13} \equiv a \pmod{13}$

Como 3, 7 e 13 são primos entre si dois a dois

e como $3 \mid a^{13} - a$, $7 \mid a^{13} - a$ e $13 \mid a^{15} - a$

então $3 \times 7 \times 13 \mid a^{13} - a$, ou seja, $a^{13} \equiv a \pmod{273}$

c) $a^{12} \equiv 1 \pmod{35}$ para todo a tal que $m.d.c(a,35)=1$

$35 = 5 \times 7$

Como $m.d.c(a,35) = 1$ então $5 \nmid a$
$7 \nmid a$

Podemos aplicar o PTF e temos

$a^4 \equiv 1 \pmod 5 \quad \Rightarrow \quad a^{12} \equiv 1^3 \pmod 5$

$\Rightarrow \quad a^{12} \equiv 1 \pmod 5$

$a^6 \equiv 1 \pmod 7 \quad \Rightarrow \quad a^{12} \equiv 1^2 \pmod 7$

$\Rightarrow \quad a^{12} \equiv 1 \pmod 7$

Como $a^{12} \equiv 1 \pmod 5$ e $a^{12} \equiv 1 \pmod 7$

então $a^{12} \equiv 1 \pmod{35}$.

73. Mostre que 60 divide $a^4 + 59$ se m.d.c.$(a, 30) = 1$.

$a^4 + 59 \equiv 0 \pmod{60} \iff a^4 \equiv -59 \pmod{60}$

$\iff a^4 \equiv 1 \pmod{60}$

Então provar que $60 \mid a^4 + 59$ é o mesmo que provar que $a^4 \equiv 1 \pmod{60}$

$60 = 2^2 \times 3 \times 5$

Como 3 é primo pelo PTF: $a^2 \equiv 1 \pmod 3$

$a^4 \equiv 1^2 \pmod 3$

$a^4 \equiv 1 \pmod 3$

Com 5 é primo então pelo PTF $a^4 \equiv 1 \pmod 5$

Note-se que $3 \nmid a$ e $5 \nmid a$ uma vez que m.d.c $(a, 30) = 1$

Note-se também que $2 \nmid a$ pelo mesmo motivo

Portanto $a \equiv 1 \pmod 2$, ou seja, a é ímpar

Logo na divisão por 4 os restos possíveis para a são: 1, 3

Temos então dois casos se $a \equiv 1 \pmod 4$ ou $a \equiv 3 \pmod 4$

Se $a \equiv 1 \pmod 4$ $\Rightarrow$ $a^4 \equiv 1 \pmod 4$

Se $a \equiv 3 \pmod 4$ $\Rightarrow$ $a^4 \equiv 3^4 \pmod 4$

$\Rightarrow a^4 \equiv 81 \pmod 4$

$\Rightarrow a^4 \equiv 1 \pmod 4$

Em qualquer das duas situações $a^4 \equiv 1 \pmod 4$

Temos que $4 \mid a^4 - 1$, $3 \mid a^4 - 1$ e $5 \mid a^4 - 1$

Como 4, 3 e 5 são primos entre si dois a dois então

$4 \times 3 \times 5 \mid a^4 - 1$, ou seja, $a^4 \equiv 1 \pmod{60}$.

Logo $a^4 \equiv -59 \pmod{60} \Leftrightarrow a^4 + 59 \equiv 0 \pmod{60}$

$\Leftrightarrow 60 \mid a^4 + 59$.

74. Se $a \in \mathbb{Z}$ é tal que $7 \nmid a$, prove que a^3+1 ou a^3-1 é divisível por 7.

Se $7 \nmid a$ então podemos aplicar o PTF $a^6 \equiv 1 \pmod 7$

$\iff a^6 - 1 \equiv 0 \pmod 7 \iff 7 \mid a^6 - 1$

$\iff 7 \mid (a^3-1)(a^3+1)$.

Como 7 é primo $7 \mid a^3 - 1$ ou $7 \mid a^3+1$.