(85) Resolva o sistema

$$x \equiv 24 \pmod{25}$$
$$x \equiv 9 \pmod{10}$$
$$x \equiv 13 \pmod{14}$$

Temos que $x = 25a + 24$, daí

$$25a + 24 \equiv 9 \mod 10$$
$$\Rightarrow 5a \equiv 5 \mod 10$$
$$\Rightarrow a \equiv 1 \mod 10$$

Portanto, $a = 10b + 1 \Rightarrow x = 250b + 49$

$$250b + 49 \equiv 13 \mod 14$$
$$\Rightarrow 12b \equiv 6 \mod 14$$
$$\Rightarrow -2b \equiv 6 \mod 14$$
$$\Rightarrow b \equiv 11 \mod 14 \text{ ou } b \equiv 4 \mod 14$$

Daí, $b = 14c + 11$ ou $b = 14c + 4$, quebrando em 2 casos

1) $b = 14c + 11 \Rightarrow x = 3500c + 2799$

Voltando a mod $x \overset{\equiv 2799}{\equiv} 349 \pmod{350}$

2) $b = 14c + 4 \Rightarrow x = 3500c + 1049$

Voltando a mod: $x \equiv 1049 \equiv 349 \pmod{350}$

(86) Determine a ordem de 2 modulo m, para
(a) $m = 7$
(b) $m = 7^2$
(c) $m = 7^3$

(a) $\text{ord}_7(2) = 3$

(b) $\text{ord}_{7^2}(2) = 3 \cdot 7$

(c) $\text{ord}_{7^3}(2) = 3 \cdot 7^2$

~~Ex~~ ~~Exemplo~~ Isso pode ser generalizado como se a ordem de 2 modulo p ~~Ep~~ primo é q, então a ordem de 2 modulo p^2 é $p \cdot q$.
Porém existem 2 contraexemplos para a generalização que são os primos de Wieferich. ($p = 1093$ e $p = 3511$)
~~Ep.~~ os primos de Wieferich são infinitos mas só conhecemos 2 deles até hoje.

(89) Escreva os polinomios ciclotônicos $\Phi_n(x)$ para n igual a 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 15, 105.

$\Phi_1(x) = x - 1$

$\Phi_2(x) = x + 1$

$\Phi_3(x) = x^2 + x + 1$

$\Phi_4(x) = x^2 + 1$

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

$\cancel{\Phi_6(x)} = x^6 - 1 = (x^3-1)(x^3+1) = \underbrace{(x-1)}_{\Phi_1}\underbrace{(x+1)}_{\Phi_2}\underbrace{(x^2+x+1)}_{\Phi_3}\underbrace{(x^2-x+1)}_{\Phi_6}$

$\Phi_6(x) = x^2 - x + 1$

$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\Phi_8(x) = x^4 + 1$

$\Phi_9(x) = x^6 + x^3 + 1$

$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$

$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + \dots + x + 1$

Lema: $x^n - 1 = \prod_{d|n} \Phi_d$

$\Phi_{12}(x) = x^4 - x^2 + 1$

$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$

$$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^{9} - x^{8} - 2x^{7} - x^{6} - x^{5} + x^{2} + x + 1.$$

(95) Prove que $\Phi_{2n}(x) = \Phi_n(-x)$, para n inteiro ímpar maior que 1.

Para $n > 1$

$$\prod_{d|2n} \Phi_d(x) = x^{2n} - 1 = (x^n - 1)(x^n + 1)$$
$$= -(x^n - 1)((-x)^n - 1)$$
$$= -\prod_{d|n} \Phi_d(x)\Phi_d(-x)$$

Vamos mostrar por indução em $n = 3, 5, 7, 9, \ldots$ Para $n = 3$:

$$\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = -\Phi_1(x)\Phi_3(x)\Phi_1(-x)\Phi_3(-x)$$

$$\Rightarrow \Phi_2(x)\Phi_6(x) = -\Phi_1(-x)\Phi_3(-x)$$

Note que, $\Phi_2(x) = -\Phi_1(-x)$. Logo $\Phi_6(x) = \Phi_3(-x)$. Para o caso geral note que os divisores de $2n$ aparecem em pares $(d, 2d)$, para $\forall d|n$.

Então seja $d_1, d_2, \ldots, d_k$ os divisores de n, onde $d_1 = 1$ e $d_k = n$ (ordem crescente).

$$\prod_{d|2n} \Phi d(x) = \cancel{\Phi_{d_1}\Phi_{d_2}} \Phi_{d_1}\Phi_{2d_1}\Phi_{d_2}\Phi_{2d_2}\cdots\Phi_{d_k}\Phi_{2k}$$

$$= -\Phi_{d_1}\Phi_{d_2}\cdots\Phi_{d_k}\cdot\Phi_{d_1}(-x)\Phi_{d_2}(-x)\cdots\Phi_{d_k}(-x)$$

$$\Rightarrow \Phi_{2d_1}(x)\cdot\Phi_{2d_2}(x)\ldots\Phi_{2d_k}(x) = -\Phi_{d_1}(-x)\Phi_{d_2}(-x)\ldots\Phi_{d_k}(-x)$$

Como $\Phi_2(x) = -\Phi_1(-x)$

$$\Phi_{2d_2}(x)\cdot\Phi_{2d_3}(x)\ldots\Phi_{2d_k}(x) = \Phi_{d_2}(-x)\ldots\Phi_{d_k}(-x)$$

Como (d_k) é crescente por hipótese de indução $\Phi_{2d}(x) = \Phi_d(-x)$

(98) Prove que se 4^n+2^n+1 é primo, então n é potencia de 3.

Primeiro seja $f(x) = x^{2n}+x^n+1 = \dfrac{x^{3n}-1}{x^n-1}$

$$= \frac{\prod_{d|3n} \phi_{3n}(x)}{\prod_{\delta|n} \phi_n(x)}$$

$$= \prod_{d|C} \phi_{3^{t+1}d}(x)$$

onde $n = 3^t \cdot C$, t.q. $3 \nmid C$. Suponha "n" não potencia de 3, então $C>1$.

<u>Afirmação</u>: $|\Phi_n(2)| \geq 1$

<u>Prova</u>: $|\Phi_n(2)| = \left|\prod_{mdc(n,k)=1} (2-\omega_n^k)\right| \geq 1$

cada termo é ≥ 1

Logo, se $f(2)$ é primo n é potencia de 3.

(99) Prove que não há números primos na sequência infinita

$$10001,\ 100010001,\ 1000100010001, \ldots$$

Note que $10001 = 73.173$. Agora para $n \geq 3$ o problema é equivalente a provar que

$$1 + 10^4 + 10^8 + \cdots + 10^{4n} \text{ <u>não</u> é primo}$$

Dessa forma $(m+1) \mid (n+1) \Rightarrow (1 + 10^4 + \cdots + 10^{4m}) \mid (1 + 10^4 + \cdots + 10^{4n})$
Basta então verificar quando $n+1$ é primo. Então

$$1 + 10^4 + \cdots + 10^{4n} = \Phi_{n+1}(10^4)$$

$$= \Phi_{n+1}(10) . \Phi_{4n+4}(10)$$

então não é primo pelo teorema:

Teorema: Se a, n são inteiros positivos e $\text{mdc}(a,n) = 1$, temos $\Phi_n(x^a) = \prod_{d \mid a} \Phi_{nd}(x)$.

(100) Encontre todas as soluções inteiras da equação

$$\frac{x^7-1}{x-1}=y^5-1$$

Para resolver a equação primeiro vamos provar que se x é um inteiro e p um primo tal que p divide $\frac{x^7-1}{x-1}$ então ou $p=7$ ou $p\equiv 1 \pmod 7$.

Prova: Pelo pequeno teorema de Fermat $x^{p-1}-1$ é divisível por p. Também pela hipótese x^7-1 é divisível por p. Agora suponha que 7 não divida $p-1$. Então $\operatorname{mdc}(p-1,7)=1$, então existe a e b tal que $7a+(p-1)b=1$. Consequentemente

$$x\equiv x^{7a+(p-1)b}\equiv (x^7)^a\cdot(x^{p-1})^b\equiv 1 \pmod p$$

e então

$$\frac{x^7-1}{x-1}=1+x+\dots+x^6\equiv 7 \pmod p.$$

Então temos que p divide 7, portanto $p=7$ deve ser válido se não tivermos $p\equiv 1 \pmod 7$, como afirmamos.

Mostramos agora que todo divisor positivo de $\frac{x^7-1}{x-1}$ sabemos que ou $d=0$ ou $d\equiv 1 \pmod 7$)

Assumindo (x,y) é uma solução para nosso problema, vamos supor que $y-1>0$ desde que $\frac{x^7-1}{x-1}\geq 1$, $\forall x\neq 1$. Então desde que $y-1$ divida $\frac{x^7-1}{x-1}=y^5-1$ temos $y\equiv 1 \pmod 7$ $y\equiv 2 \pmod 7$. Avaliando $1+y+y^2+y^3+y^4$ em ambos os casos possíveis temos contradição de fato que nosso possível divisor $1+y+y^2+y^3+y^4$ de $\frac{x^7-1}{x-1}$ é congruente a 0 ou 1 (mod 7).
Então não tem solução