Lista 7

⑨ Sejam $F_1, \dots, F_n$ os n primeiros números de Fermat.

Mostre que existe um inteiro N tq $F_i \mid (N + i - 1)$

$\forall\, i = 1, \dots, n$.

Resolver o sistema de congruências

$$x \equiv 1 - i \pmod{F_i}, \quad i = 1, \dots, n.$$

Mostrar que $\text{mdc}(F_i, F_j) = 1$ se $i \neq j$ e aí é só usar o Teorema Chinês.

Para mostrar que $\text{mdc}(F_i, F_j) = 1$ se $i \neq j$, mostre que:

$$2^{2^{n+k}} + 1 = \left(2^{2^{n+k}} - 1\right) + 2 = \left[\left(2^{2^{n+k-1}}\right)^2 - 1\right] + 2$$

$$= \left(2^{2^{n+(k-1)}} - 1\right)\left(2^{2^{n+(k-1)}} + 1\right) + 2$$

$$= \dots = \left(2^{2^{n+1}} - 1\right) \dots \left(2^{2^{n+(k-1)}} + 1\right) + 2$$

$$= \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right)\left(2^{2^{n+1}} + 1\right) \dots \left(2^{2^{n+(k-1)}} + 1\right) + 2$$

$$\text{mdc}\left(2^{2^{n+k}} + 1,\ 2^{2^n} + 1\right) = \text{mdc}\left(2^{2^n} + 1,\ 2\right) = 1$$

Lista 7

5 (a) Mostrar que $\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$ tem solução $\iff$ $\text{mdc}(m,n) \mid b-a$.

($\Rightarrow$) $\exists\, x_0$ tq $m \mid x_0 - a$ e $m \mid x_0 - b$ $\Rightarrow$ $\text{mdc}(m,n) \mid x_0 - a$ e

e $\text{mdc}(m,n) \mid x_0 - b$ $\Rightarrow$ $\text{mdc}(m,n) \mid (x_0 - a) - (x_0 - b) = b - a$

($\Leftarrow$) $x \equiv a \pmod m \Rightarrow x = a + ny$

$x \equiv b \pmod n \Rightarrow a + ny \equiv b \pmod n$

$\Rightarrow ny \equiv b - a \pmod n$.

Se $\text{mdc}(m,n) \mid b-a$, então

$ny \equiv b - a \pmod m$ tem solução.

$d = \text{mdc}(m,n)$

$n_1 = \frac{n}{d}$ $\quad m_1 = \frac{m}{d}$ $\quad \frac{b-a}{d} = c$

$n_1 y \equiv c_1 \ (m_1)$

$y \equiv y_0 \ (m_1)$ e as soluções são

$y = y_0 + m_1 t$, $t \in \mathbb{Z}$.

$$x = a + n y = a + n(y_0 + m_1 t), \quad t \in \mathbb{Z}$$

$$x = (a + n y_0) + (n m_1) t, \quad t \in \mathbb{Z}.$$

$$\text{e } n m_1 = \frac{nm}{d} = \text{mmc}(m,n).$$

Mostrar que todas soluções são congruentes mod (mmc(m,n))

Vimos que as soluções são da forma

$$x = x_0 + \text{mmc}(m,n)\, t, \quad t \in \mathbb{Z} \quad \text{e}$$

então elas são congruentes módulo mmc(m,n). ∎

Exercícios

Lista 5

15. Mostrar que $F_5 = 2^{2^5} + 1 \equiv 0 \pmod{641}$.

$$641 = 2^4 + 5^4 = 2^6 \times 10 + 1 = 2^7 \times 5 + 1$$

$$2^4 \equiv -5^4 \pmod{641} \quad (*)$$

$$2^7 \times 5 \equiv -1 \pmod{641} \quad (**)$$

Partindo de (**)

$$(2^7 \times 5)^4 \equiv (-1)^4 \pmod{641}$$

$$\Rightarrow 2^{28} \times 5^4 \equiv 1 \pmod{641}$$

Usando (*) agora

$$2^{28} \times (+2^4) \equiv -1 \pmod{641} \Rightarrow 2^{32} + 1 \equiv 0 \pmod{641}. \blacksquare$$

19. Quais são todos os inteiros m com a propriedade:

"Para todo inteiro a, $a^2 \equiv 0 \pmod{m} \Rightarrow a \equiv 0 \pmod{m}$".

RESPOSTA: m livre de $\square$'s.

Dem: ($\Rightarrow$)

Se p é primo e $a^2 \equiv 0 \pmod{p}$, então $p \mid a^2 \Rightarrow p \mid a \Rightarrow a \equiv 0 \pmod{p}$.

Se m é livre de quadrados $\Rightarrow m = p_1 p_2 \cdots p_k$, $p_i \neq p_j$ se $i \neq j$

e p_i primo $\forall i = 1, \ldots, k$.

Se $a^2 \equiv 0 \pmod{m} \Rightarrow m \mid a^2 \Rightarrow p_i \mid a^2 \ \forall i \Rightarrow p_i \mid a \ \forall i$

$\Rightarrow m \mid a$ pois $\text{mdc}(p_1, \ldots, p_k) = 1$.

($\Leftarrow$) Se $\exists\, p$ primo tal que $p^2 \mid m \Rightarrow m = p^2 x$, $x \in \mathbb{Z}$

Seja $a = px$ $px \not\equiv 0 \pmod{m}$, mas $a^2 \equiv 0 \pmod{m}$.

30: $p \neq 2$ e $p \neq 5$

$\text{mdc}(p, 10) = 1$ $\quad 10^{n(p-1)} \equiv 1 \pmod{p} \quad \forall n$.

$10^{n(p-1)} - 1 = (9 \ldots\ldots 9)_{10} \quad \forall n$.

41: Sejam p e q primos gêmeos, isto é, p primo e $p+2 = q$ é primo. Mostrar que $p+q \equiv 0 \pmod{12}$. $\quad k \geq 1$

Se $p = 4k+1$ e $q = 4k+3$

$\Rightarrow p+q \equiv 2+4k+4 \equiv 0 \pmod{4}$

$p = 4k+3$ e $q = 4k+3+2$

$p+q = 8k+6+2 = 8(k+1) \Rightarrow 4 \mid p+q$.

Se $p \equiv 1 \pmod 3$ e $p+2 \equiv 0 \pmod 3 \Rightarrow 3 \mid p+2$ e $p+2$ não é primo

Se $p = 3k+1$, $q = 3k+2+2 = 3(k+1)+1$

$\Rightarrow p+q = 3k+2+3(k+1)+1 \Rightarrow 3 \mid p+q$.

Logo $12 \mid p+q$.

46. Mostre que o dígito das dezenas de qualquer potência de 3 é par.

$3 \equiv 3 \pmod{10}$
$3^2 \equiv 9 \pmod{10}$
$3^3 \equiv 7 \pmod{10}$
$3^4 \equiv 1 \pmod{10}$

$3^4 \equiv 1 \pmod{10}$

$3^n \equiv 3^{4q+r}$, $0 \leq r < 4$

$3^n \equiv 3^r (3^4)^q \pmod{10} \equiv 3^r \pmod{10}$.

. As potências de 3 são congruentes a $1, 3, 7, 9 \pmod{10}$.

Mostrar que para todo $n > 0$, o algarismo da dezena de uma potência de 3 é par.

$3 \equiv 03 \pmod{10}$
$3^2 \equiv 09 \pmod{10}$
$3^3 \equiv 27 \pmod{10}$

Por indução em n.

$n = 1$ ✓

Suponha que $k \geq 1$ e que

$3^k \equiv 10a + b \pmod{100}$, onde

a é par, $0 \leq a \leq 9$

Mostrar que

$3^{k+1} \equiv 10x + y \pmod{100}$, onde x é par, $0 \le x \le 9$.

$3^{k+1} \equiv 3(10a+b) \equiv 10 \times 3a + 3b \pmod{100}$

Se $3a > 10$, como a é par, $3a$ é par.

Logo $3a = r\,10 + s$ onde s é par, $0 \le s \le 9$

$r = 0, 1, 2$

$3^{k+1} = 10(\underbrace{10r+s}_{3a}) + 3b \equiv 10s + 3b \pmod{100}$.

$b = 1, 3, 7, 9$

Se $b = 1, 3$ então $3^{k+1} \equiv 10s + 3$ ou $3^{k+1} \equiv 10s + 9 \pmod{100}$,

e o algarismo da dezena não muda.

Se $b = 7, 9$ $3b = 21$ ou $3b = 27$

Assim, $3^{k+1} \equiv 10s + 21 \pmod{100}$ ou $3^{k+1} \equiv 10s + 27 \pmod{100}$

$\equiv 10(\underbrace{s+2}_{\text{par}}) + 1 \pmod{100}$

$\equiv 10(\underbrace{s+2}_{\text{par}}) + 7 \pmod{100}$

47 Mostrar que para todo n ímpar o número

$$S_n = 2^{2n}(2^{2n+1} - 1)$$ termina em 28.

Por indução em n.

$n = 1 \quad 2^2(2^3 - 1) = 28.$

Suponha verdadeiro para k^{n} ímpar, mostrar que vale para $k+2$.

H.I $S_k \equiv 28 \pmod{100}$ T: $S_{k+2} \equiv 28 \pmod{100}$

Vamos provar que $S_{k+2} \equiv S_k \pmod{100}$.

$$S_{k+2} - S_k = 2^{2(k+2)}(2^{2(k+2)+1} - 1) - 2^{2k}(2^{2k+1} - 1)$$

$$= 2^{2k}(2^4 \cdot 2^{2k+5} - 2^4 - 2^{2k+1} + 1)$$

$$= 2^{2k}[2^4 \cdot 2^4 \cdot 2^{2k+1} - 2^{2k+1} - 15]$$

$$= 2^{2k}[2^{2k+1}(256-1) - 15]$$

$$= 2^{2k}\left[2^{2k+1} \times 255 - 15\right] = \underbrace{2^{2k} \times 5}_{\text{já é divisível por 20}}\left[\underbrace{2^{2k+1} \times 51 - 3}_{\text{mostrar que é divisível por 5}}\right]$$

$$2^2 \equiv -1 \pmod 5$$

$$2^{2k} \equiv (-1)^k \pmod 5 \equiv -1 \pmod 5$$

↳ k é ímpar

$$2^{2k+1} \equiv -2 \pmod 5$$

$$51 \equiv 1 \pmod 5$$

$$\text{Logo, } 2^{2k+1} \times 51 - 3 \equiv -2 - 3 \pmod 5 \equiv 0 \pmod 5$$

Assim $S_{k+2} \equiv S_k \equiv 28 \pmod{100}$.

38: Mostrar que $2730 \mid n^{13} - n \quad \forall n \in \mathbb{Z}$

$2730 = 13 \times 7 \times 5 \times 3 \times 2$

$n^{13} \equiv n \pmod{13} \quad \forall n$

Se $mdc(n, 7) = 1$, $n^6 \equiv 1 \pmod 7$

$n^{12} \equiv 1 \pmod 7$

Se $7 \nmid n$ ou $7 \nmid n$, $n^{13} \equiv n \pmod 7$

Se $mdc(n, 5) = 1$, $n^4 \equiv 1 \pmod 5$

$\Rightarrow n^{12} \equiv 1 \pmod 5$

$\Rightarrow n^{13} \equiv n \pmod 5 \quad \forall n$.

Se $mdc(n, 3) = 1$

$n^2 \equiv 1 \pmod 3$

$\Rightarrow n^{12} \equiv 1 \pmod 3$

$n^{13} \equiv n \pmod 3$

$n^{13} \equiv n \pmod 2$ sempre!

Logo $2 \times 3 \times 5 \times 7 \times 13 \mid n^{13} - n \quad \forall n$.

13. Seja p primo ímpar. Mostrar que $((p-1)!)^{p^{n-1}} \equiv -1 \pmod{p^n}$

Temos que provar que $p^n \mid \left[((p-1)!)^{p^{n-1}} + 1\right] \quad \forall\, n \geq 1$.

Pelo Teorema de Wilson, temos que

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

Logo, $(p-1)! + 1 = k p$ para algum $k \in \mathbb{Z}$

$$\left((p-1)! + 1\right)^{p^{n-1}} = (kp)^{p^{n-1}} = k^{p^{n-1}} p^{p^{n-1}}.$$

Mostrar que para todo n, $p^n \mid p^{p^{n-1}}$.

(Mostrar por indução em n

$n = 1 \quad p \mid p^{p^0}$

Suponha $k \geq 1$ e que $p^k \mid p^{p^{(k-1)}}$. Mostrar que $p^{k+1} \mid p^{p^k}$.

$$\Rightarrow (p^k)^p \mid \left(p^{p^{k-1}}\right)^p = p^{p^k}$$

Mas $kp = (k-1)p + p \geq (k-1)2 + 2 \geq 2k \geq k+1$.)

Assim $\left((p-1)! + 1\right)^{p^n} \equiv 0 \pmod{p^{n+1}}$

Mas $((p-1)!)^{p^n} \equiv (-1)^{p^n} \pmod{p^{n+1}}$

Veja o Exercício 12 da Lista 4