Exercícios da Lista 5

23(b) Determinar um quadrado perfeito $(aabb)_{10}$.

$N = a\times10^3 + a\times10^2 + b\times10 + b$

$N = 11\times(a\times10^2 + b)$. Para que N seja um □ perfeito, $11 \mid a10^3 + b$

$\Rightarrow a + b \equiv 0 \pmod{11}$.

$b \neq 2, 3, 7$ e 8

Testar:

$b = 0$, mas daí, $a\times10^2$ não é divisível por 11.

$b = 1$ $\quad aa11$ $\quad 11 \mid a01 \Rightarrow a + 1 \equiv 0 \pmod{11}$, só que $0 \leq a \leq 9$, nesta $\quad a = 7$

$b = 4$ $\quad aa44$ $\quad 11 \mid a04 \Rightarrow a + 4 \equiv 0 \pmod{11}$

7744 é um □, $7744 = 11^2 \times 64$

$b = 5$ $\quad aa55$, $11 \mid a05$ $\quad a + 5 \equiv 0 \pmod{11} \Rightarrow a = 6$

$11 \mid 605$ $\quad 605 = 11\times55$ e 55 não é um □.

$b = 6$ $\quad aa66$ $\quad a = 5$ $\quad 506 = 11\times46$ e 46 não é □.

$b = 9$ $\quad aa99$ $\quad a = 2$ $\quad 209 = 11\times19$ e 19 não é um □

O único quadrado é 7744

LISTA 5

24: $N = a\times10^2 + b\times10 + c$, $a\neq0$ $\quad 0\leq a,b,c\leq 9$

$11 \mid N \iff \frac{N}{11} = a^2+b^2+c^2$

Escreva $\frac{N}{11} = x\times10 + y$, $x\neq0$

$(x\times10+y)\times(10+1) = x\times10^2 + x\times10 + y\times10 + y$

$= x\times10^2 + (x+y)\times10 + y = N$

Caso (1) $x+y\leq 9 \Rightarrow x=a \quad b=x+y \quad y=c$

$\frac{N}{11} = x^2 + (x+y)^2 + y^2 = 2x^2+2xy+2y^2 = 2(x^2+xy+y^2)$

Para que existam x, y tais que $2(x^2+xy+y^2) = \frac{N}{11} = x\times10+y$

$2x^2+2xy+2y^2-10x-y=0$

$= 2y^2 + (2x-1)y + (2x^2-10x) = 0$

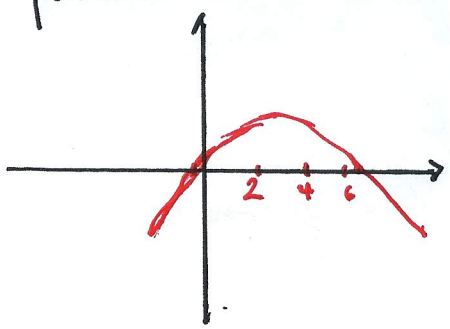
Para existir y tal que y seja solução de (*), é preciso determinar x tal que

$\Delta = (2x-1)^2 - 8(2x^2-10x) \geq 0$

$= 4x^2 - 4x + 1 - 16x^2 + 80x \geq 0$

$= -12x^2 + 76x + 1 > 0$

Essa parábola é assim:



Os inteiros nesse intervalo são

0, 1, 2, 3, 4, 5, 6

$x = 0 \Rightarrow \Delta = 1$

$2y^2 - y = 0$

$y(2y-1) = 0 \qquad y = 0$ *

$x = 1 \Rightarrow \Delta = -12 + 76 + 1 = 65$.

$\sqrt{\Delta}$ não é inteiro

$x = 2 \qquad \Delta = -48 + 152 + 1 = 105$

$\sqrt{\Delta}$ não é inteiro

$x = 3 \qquad \Delta = -108 + 228 + 1 = 121$

A equação é $2y^2 + 5y - 12 = 0$

$y = \dfrac{-5 \pm 11}{4} = \begin{matrix} 6/4 \\ -4 \end{matrix}$ NÃO É INTEIRO

$x = 4 \qquad \Delta = -16 \times 12 + 76 \times 4 + 1$

$= -192 + 304 + 1 = 112$

$\sqrt{\Delta}$ não é inteiro

$x = 5 \qquad \Delta = -12 \times 25 + 76 \times 5 + 1$

$= -300 + 380 + 1 = 81$

$\sqrt{\Delta} = 9$

A equação é $2y^2 + 9y + (2.25 - 50) = 0$

$y = 0$ ou $y = -9/2$

Com $y = 0$ e $x = 5$

$50 - 50 = \frac{N}{11}$ e $N = 550$

$\frac{N}{11} = 5^2 + 5^2 = 50$

$x = 6$

$\Delta = -12 \times 36 + 76 \times 6 + 1 = 25$

A equação é $2y^2 + 11y + 12 = 0$

$y = \frac{-11 \pm 5}{4} = -6/4 < 0$ → $-16/4$

A única solução foi $N = 550$

Caso (2) $x + y \geq 10$ $x + y - 10 \geq 0$

$x \times 10^2 + (x + y - 10) \times 10 + 10^2 + y = N$

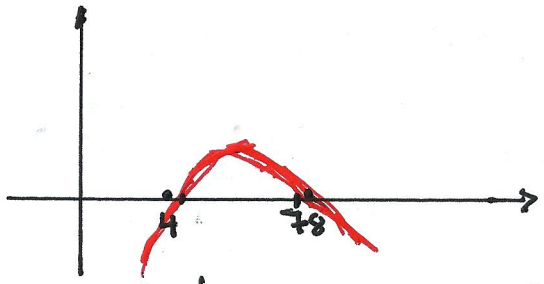
$(x+1)10^2 + (x+y-10) \times 10 + y = N = a10^2 + b10 + c$

$\frac{N}{11} = (x+1)^2 + (x+y-10)^2 + y^2$

$\Leftrightarrow 2y^2 + y(2x-21) + (2x^2 - 28x + 101) = 0$

Encontrar x para que $\Delta \geq 0$

$$\Delta = -12x^2 + 140x - 367$$



Temos que testar $x = 5, 6, 7$

$x = 5$ $\quad \Delta = -12 \times 25 + 700 - 367 = 13$

$\sqrt{\Delta} \notin \mathbb{Z}$

$x = 6$ $\quad \Delta = -12 \times 36 + 840 - 367 = 41$

$\sqrt{\Delta} \notin \mathbb{Z}$

$x = 7$ $\quad \Delta = -12 \times 49 + 140 \times 7 - 367 = 25$

A equação é

$2y^2 + y(14-21) + (98 - 28 \times 7 + 101) = 0$

$2y^2 - 7y + 3 = 0$

$\Delta = 49 - 24 = 25$

$y = \frac{7 \pm 5}{4} = \begin{cases} 3 \\ 1/2 \end{cases}$

$\boxed{y = 3}$

$N = 803 = 73 \times 11$

$64 + 9 = 73$

Lista 6

30. Mostre que para todo inteiro positivo a tem-se $a^{\varphi(n)+1} \equiv a \pmod{n}$ se, e somente se, n é livre de quadrados.

($\Rightarrow$) Suponha que $n = p^2$, p primo.

$\varphi(p^2) = p(p-1) \geq p$ $\qquad$ $\varphi(p^2)+1 \geq p+1 \geq 3$

$p-1 \geq 1$

Se $a = p$, $\quad a \not\equiv 0 \pmod{p}$

$a^{\varphi(p^2)+1} = p^{p(p-1)+1}$ e $p^2 \mid p^{p(p-1)+1}$.

Assim $\left.\begin{array}{l} p^{\varphi(p^2)+1} \equiv 0 \pmod{p^2} \\ p \not\equiv 0 \pmod{p^2} \end{array}\right\} \Rightarrow a^{\varphi(p^2)+1} \not\equiv a \pmod{p^2}$

para a todo a.

($\Leftarrow$) Se n é livre de quadrados, então $n = p_1 \cdots p_k$,

$p_i \neq p_j$ se $i \neq j$ e p_i primo.

$\varphi(n) = (p_1-1) \cdots (p_k-1)$

Seja $a \in \mathbb{Z}$

Se $p_i \nmid a$, $\quad a^{p_i-1} \equiv 1 \pmod{p_i} \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{p_i}$

$\Rightarrow a^{\varphi(n)+1} \equiv a \pmod{p_i}$

Se $p_i \mid a \Rightarrow a \equiv 0 \pmod{p_i}$

$\Rightarrow a^{\varphi(n)+1} \equiv 0 \pmod{p_i}$ e $a^{\varphi(n)+1} \equiv a \pmod{p_i}$.

Assim, para todo $i = 1, \dots, k$,

$a^{\varphi(n)+1} \equiv a \pmod{p_i}$.

Como $\text{mdc}(p_1, \dots, p_k) = 1$ temos que $a^{\varphi(n)+1} \equiv a \pmod{n}$, qualquer que seja $a \in \mathbb{Z}$.

31. Teorema de Lucas (1878)

(Esse resultado pode ser um teste para verificar se um número n é ou não primo.

Sejam a e m inteiros positivos com $\text{mdc}(a, m) = 1$. Suponha que $a^{m-1} \equiv 1 \pmod{m}$ e que $a^{k} \not\equiv 1 \pmod{m}$ $\forall$ k com $k < m-1$. Mostrar que m é primo.

Pela hipótese, temos que $\text{ord}_m(a) = m-1$, pois $m-1$ é o menor inteiro tq $a^{m-1} \equiv 1 \pmod{m}$.

Pelo Teorema de Euler, temos que $a^{\varphi(m)} \equiv 1 \pmod{m}$ (pois $\text{mdc}(a, m) = 1$). Então $m-1 \mid \varphi(m) \Rightarrow m-1 \leq \varphi(m)$.

Por outro lado, $\varphi(m) \leq m-1$ para todo m. Logo $\varphi(m) = m-1$

$\Rightarrow m$ é primo.

(32) Se n é um divisor positivo de $M_p = 2^p - 1$, p primo, então $n \equiv 1 \pmod{p}$.

Se $n \mid M_p \Rightarrow M_p \equiv 0 \pmod{n} \Rightarrow 2^p \equiv 1 \pmod{n}$.

$\Rightarrow \operatorname{ord}_n 2 = p$, pois p é primo.

Suponha que $n = q$, q é primo

$2^p \equiv 1 \pmod{q}$

$2^{q-1} \equiv 1 \pmod{q} \Rightarrow p \mid q-1 \Rightarrow q \equiv 1 \pmod{p}$.

Se $q \mid n$, q primo, $\Rightarrow q \equiv 1 \pmod{p}$

Logo, se $n = q_1^{r_1} \cdots q_k^{k_k}$ e $q_i \equiv 1 \pmod{p} \Rightarrow n \equiv 1 \pmod{p}$

32. Se $n>0$ é tq $n \mid M_p$. , $M_p = 2^p - 1$, p primo, então $n \equiv 1 \pmod p$.

(1) Notar que $\operatorname{ord}_n 2 = 1$. Se $\operatorname{ord}_n 2 = k$, então

$2^k \equiv 1 \pmod n$ e $k \mid p \Rightarrow k = 1$ ou $k = p$.

Se $k=1$, $2 \equiv 1 \pmod n \Rightarrow n \mid 1 \Rightarrow n = 1$ —

Logo $\operatorname{ord}_n 2 = p$.

Seja q primo tal que $q \mid n$.

$\Rightarrow 2^p \equiv 1 \pmod q$

$q \mid \underbrace{2^p - 1}_{\text{ímpar}} \Rightarrow q \neq 2 \Rightarrow \operatorname{mdc}(q,2) = 1 \Rightarrow$

$2^{q-1} \equiv 1 \pmod q \Rightarrow p \mid q-1 \Rightarrow q \equiv 1 \pmod p$

Assim, todo divisor primo de n é congruente a $1 \bmod p$.

$\Rightarrow n \equiv 1 \pmod p$.

(33) Mostre que se $d \mid F_n = 2^{2^n}+1$, então d é da forma

$$d = 2^{n+1}k + 1, \quad k \geq 0.$$

Note que $(2^{n+1}k_1 + 1)(2^{n+1}k_2 + 1)$

$$= 2^{n+1}k_1 2^{n+1}k_2 + 2^{n+1}k_1 + 2^{n+1}k_2 + 1$$

$$= 2^{n+1}\underbrace{\left(2^{n+1}k_1k_2 + k_1 + k_2\right)}_{k} + 1$$

Assim, basta provar para $d \mid F_n$, d primo.

Seja p primo tal que $p \mid F_n$. Então

$$2^{2^n} \equiv -1 \pmod p \Rightarrow \left(2^{2^n}\right)^2 \equiv 1 \pmod p$$

$$\Rightarrow 2^{2^{n+1}} \equiv 1 \pmod p \Rightarrow \operatorname{ord}_p 2 \mid 2^{n+1}.$$

pois $\operatorname{ord}_p 2 \nmid 2^n$, pois $2^{2^n} \equiv -1 \pmod p$

Logo $\operatorname{ord}_p 2 \equiv 2^{n+1}$.

Por outro lado, $2^{p-1} \equiv 1 \pmod p \Rightarrow \operatorname{ord}_p 2 \mid p-1$

$$\Rightarrow p-1 = 2^{n+1}k, \text{ para algum } k > 0$$

$$\Rightarrow p = 2^{n+1}k + 1.$$