Problema 7. (a) Ache todos os primos p tais que $\frac{7^{p-1}-1}{p}$ é um quadrado perfeito.

(b) Ache todos os primos p tais que $\frac{11^{p-1}-1}{p}$ é um quadrado perfeito.

Primeiro, por Fermat, $7^{p-1} \equiv 1 \pmod p$. Logo, $\frac{7^{p-1}-1}{p}$ é inteiro pra todo $p \neq 7$.
Vamos falar que $7^{p-1} - 1 = n^2 p$.
Olhando $\pmod 3$, sabemos que $7^{p-1} - 1 \equiv 0 \equiv n^2 p$. Para $p \neq 3$, n é múltiplo de 3. Desse modo, olhando $\pmod 9$, sabemos que $0 \equiv n^2 p \equiv 7^{p-1} - 1$. Como em $\pmod 9$, $7^1 \equiv 7$, $7^2 \equiv 4$, $7^3 \equiv 1$, temos que $p = 3k + 1$. Como p é primo, $p = 6k + 1$.
Conclusão. $p = 3$ ou $p = 6k + 1$.

- Se $p = 3$, temos que $\frac{7^2-1}{3} = 16$, que é quadrado perfeito.
- Se $p = 6k + 1$. Logo, $7^6 - 1 \mid 7^{6k} - 1 = 7^{p-1} - 1$.

  Isto é, $7^6 - 1 = (7^3 - 1)(7^3 + 1) = (7 - 1)(7^2 + 7 + 1)(7^3 + 1) = 6 \times 57 \times 344 = 2^4 \times 3^2 \times 19 \times 43$

  Sabemos que 6 divide n^2, logo 6 divide n. Seja $n = 6m$.

$$\begin{aligned} n^2 p &= 7^{6k} - 1 \\ &= (7^{3k} - 1)(7^{3k} + 1) \\ &= (7^k - 1)(7^{2k} + 7^k + 1)(7^k + 1)(7^{2k} - 7^k + 1) \end{aligned}$$

a. $(7^k - 1, 7^k + 1) = (7^k - 1, 2) = 2$
b. $(7^k - 1, 7^{2k} - 7^k + 1) = (7^k - 1, 1) = 1$
c. $(7^k - 1, 7^{2k} + 7^k + 1) = (7^k - 1, 2 \cdot 7^k + 1) = (7^k - 1, -3) = 3$
d. $(7^k + 1, 7^{2k} + 7^k + 1) = (7^k + 1, 1) = 1$
e. $(7^k + 1, 7^{2k} - 7^k + 1) = (7^k + 1, -2 \cdot 7^k + 1) = (7^k + 1, 3) = 1$
f. $(7^{2k} + 7^k + 1, 7^{2k} - 7^k + 1) = (7^{2k} + 7^k + 1, 2 \cdot 7^k) = 1$

$$m^2 p = \frac{(7^k - 1)}{6} \frac{(7^{2k} + 7^k + 1)}{3} \frac{(7^k + 1)}{2} (7^{2k} - 7^k + 1)$$

Caso I.

$$\begin{cases} 7^k - 1 = 6x^2 \\ 7^k + 1 = 2y^2 \end{cases}$$

$$\begin{cases} 7^k = 3x^2 + y^2 \\ 1 = y^2 - 3x^2 \end{cases}$$

A solução minimal é $(y_1, x_1) = (2, 1)$. Logo, (y_t, x_t) é tal que $y_t + \sqrt{3}x_t = \left(2 + \sqrt{3}\right)^t$. Logo:

$$y_t = \frac{(2 + \sqrt{3})^t + (2 - \sqrt{3})^t}{2}$$

$$x_t = \frac{(2 + \sqrt{3})^t - (2 - \sqrt{3})^t}{2\sqrt{3}}$$

Ambos y e x seguem a recorrência $a_n - 4a_{n-1} + a_{n-2} = 0$.

Problema 9. Prove que existem infinitos naturais n com as seguintes propriedades:

- n pode ser escrito como soma de dois quadrados, e;
- n pode ser escrito como soma de dois cubos, e;
- n não pode ser escrito como soma de duas potências sextas.

Sabemos que, $x^{12} \equiv 1$ ou $0 \pmod{13}$, para todo x. Consequentemente, $x^6 \equiv -1, 0$ ou $1 \pmod{13}$. Logo,

$$x^2 + y^2 \equiv -2, -1, 0, 1 \text{ ou } 2 \pmod{13}.$$

Lema 1. Se $n \equiv 3, 4, 5, 6, 7, 8, 9$ ou 10, então n não pode ser escrito como soma de potências sextas.

Lema 2 (Fermat's theorem on sums of two squares). n é soma de dois quadrados se, e somente se, $\nu_p(n)$ é par para todo $p = 4k + 3$ primo.

Queremos infinitos n tais que

$$n = a^2 + b^2 = c^3 + d^3.$$

Solução 1.
Seja p primo tal que $p \equiv 1 \pmod{4}$ e $p \equiv 6 \pmod{7}$. Por Dirichilet, existem infititos primos com essa propriedade.

- Sabemos que p^3 pode ser escrito como soma de quadrados, pelo Lema 2.
- Sabemos que $p^3 + 0^3$ é soma de dois cubos.
- Sabemos que $p^3 \equiv 6 \pmod{7}$, que implica que p^3 não é soma de duas potências sextas.

Solução 2.

$$1^3 + 2^3 = 9 = 3^2 + 0^2.$$

$$k^6(1^3 + 2^3) = k^6 \cdot 9 = k^6(3^2 + 0^2)$$

$$(k^2)^3 + (2k^2)^3 = k^6 \cdot 9 = (3k^3)^2 + 0^2$$

Note que $k^6 \cdot 9 \equiv 2 \pmod{7}$, logo não é soma de duas potências sextas.
Solução 3.

$$(5 \cdot 5)^3 + (5 \cdot 10)^3 = 25 \cdot 3^2 \cdot 5^4 = (3 \cdot (3^2 \cdot 5^4))^2 + (4 \cdot (3^2 \cdot 5^4))^2$$

Problema 11. Mostre que existem infinitos pares de primos distintos (p, q) tal que

$$p|2^{q-1} - 1 \quad \text{e} \quad q|2^{p-1} - 1.$$

Umas soluções encontradas foram $(p, q) = (11, 31)$ ou $(42, 127)$ ou $(19, 73)$ ou $(17, 257)$.

$$\begin{cases} 11 \mid 2^5 + 1 \\ 31 \mid 2^5 - 1 \end{cases} \qquad \begin{cases} 43 \mid 2^7 + 1 \\ 127 \mid 2^7 - 1 \end{cases} \qquad \begin{cases} 19 \mid 2^9 + 1 \\ 73 \mid 2^9 - 1 \end{cases} \qquad \begin{cases} 257 \mid 2^8 + 1 \\ 17 \mid 2^8 - 1 \end{cases}$$

$$\begin{cases} p \mid 2^n + 1 \\ q \mid 2^n - 1 \\ n \mid p - 1 \\ p - 1 \mid q - 1 \end{cases}$$

Lema 3. Sejam p e q primos e n natural. Se $q \mid 2^n - 1$, $n \mid p - 1$ e $p - 1 \mid q - 1$, então esse par (p, q) satisfaz o enunciado.