Corpos estendidos no espaço em grupos – respostas dos exercícios

Carlos Shine

Não se assuste com o tamanho das soluções a seguir. Eu tentei colocar o máximo de informação relacionada possível nas soluções para tentar torná-las mais instrutivas.

1 Corpos

1.1. Considere o conjunto $\mathbb{Z}/p\mathbb{Z}[i] = \{a+bi, a, b \in \mathbb{Z}/p\mathbb{Z}\}$, em que p é primo e i é a unidade imaginária.

(a) Mostre que se $p \equiv 3 \pmod 4$ então $\mathbb{Z}/p\mathbb{Z}[i]$ é um corpo.

(b) Mostre que se $p \equiv 1 \pmod 4$ então $\mathbb{Z}/p\mathbb{Z}[i]$ não é um corpo.

(c) O que acontece com o item anterior se trocarmos i por uma das "soluções" da congruência $x^2 = -1 \pmod p$? Por "solução" entendemos a solução em $\mathbb{Z}/p\mathbb{Z}$ se $p \equiv 1 \pmod 4$ e um símbolo formal se $p \equiv 3 \pmod 4$.

Solução: O problema se resume a mostrar (ou não) que todo elemento não nulo tem inverso, já que somar, subtrair e multiplicar é trivial, e os elementos neutros são os óbvios 0 e 1.

Também mostramos um resultado preliminar e conhecido, cuja demonstração segue.

Lema 1. *Sendo p primo, $x^2 + 1 \equiv 0 \pmod p$ tem solução se, e somente se, $p = 2$ ou $p \equiv 1 \pmod 4$.*

Demonstração. Se $p \equiv 3 \pmod 4$ então $(p-1)/2$ é inteiro ímpar. Assim,

$$x^2 \equiv -1 \pmod p \implies (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod p \iff x^{p-1} \equiv -1 \pmod p,$$

que contradiz o teorema de Euler-Fermat.

Se $p = 2$, $x = 1$ é solução.

Para $p \equiv 1 \pmod 4$, há várias maneiras de mostrar que $x^2 \equiv -1 \pmod p$ tem solução. Apresentamos duas delas.

- Uma é usar diretamente o teorema de Wilson: $(p-1)! \equiv -1 \pmod p$. Observando que $p - k \equiv -k \pmod p$ e usando que $(p-1)/2$ é par, $(p-1)!$ é "quadrado perfeito" módulo p:

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot (p-2) \cdot (p-1) \\ &\equiv 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdot \ldots \cdot (-2) \cdot (-1) \pmod p \\ &\equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p \\ &\equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p\end{aligned}$$

e temos uma solução explícita para $x^2 \equiv -1 \pmod p$: $x \equiv \left(\frac{p-1}{2}\right)! \pmod p$.

- Outra demonstração tem um pouco a ver com a demonstração do teorema de Wilson: para cada $m \in \mathbb{Z}/p\mathbb{Z}^*$, defina $A_m = \{m, -m, m^{-1}, -m^{-1}\}$. Esses conjuntos particionam $\mathbb{Z}/p\mathbb{Z}$, pois se $n \in A_m$ então $m \in A_n$. Como $m \not\equiv -m \pmod p$ e $m^{-1} \not\equiv -m^{-1} \pmod p$, $|A_m| = 2$ ou $|A_m| = 4$, e $|A_m| = 2$ se, e somente se, $m \equiv m^{-1} \pmod p \iff m \equiv \pm 1 \pmod p$ ou $m \equiv -m^{-1} \pmod p \iff m^2 \equiv -1 \pmod p$.

  Como há $p - 1 = 4k$ elementos não nulos em $\mathbb{Z}/p\mathbb{Z}$, $A_1 = A_{-1}$ e $|A_1| = 2$, há pelo menos mais um conjunto A_m com dois elementos, que satisfaz $m^2 \equiv -1 \pmod p$, e temos aí uma solução para $m^2 \equiv -1 \pmod p$.[1]

□

(a) Note que $a^2 + b^2 \equiv 0 \pmod p$ só tem a solução $a \equiv b \equiv 0 \pmod p$, pois se $a \not\equiv 0 \pmod p$ então $(ba^{-1})^2 \equiv -1 \pmod p$, e $x^2 \equiv -1 \pmod p$ não tem solução para $p \equiv 3 \pmod 4$. Então todo $a + bi \not\equiv 0 \pmod p$ tem inverso: temos

$$(a + bi)(a - bi) = a^2 + b^2 \implies (a + bi)(a - bi)(a^2 + b^2)^{-1} \equiv 1 \pmod p$$

e o inverso de $a + bi$ é $(a - bi)(a^2 + b^2)^{-1}$.

(b) Seja m uma solução de $x^2 \equiv -1 \pmod p$, que existe pois $p \equiv 1 \pmod 4$. Então $m+i$ não tem inverso: suponha que $a + bi$ é o seu inverso. Então $(m + i)(a + bi) \equiv 1 \pmod p \iff (ma - b) + (a + mb)i \equiv 1 \pmod p \iff a + mb \equiv 0 \pmod p$ e $ma - b \equiv 1 \pmod p \iff a \equiv -mb \pmod p$ e $m(-bm) - b \equiv 1 \pmod p \implies b(1 + m^2) \equiv -1 \pmod p \iff 0b \equiv -1 \pmod p$, absurdo.

(c) Denote por m tal "solução". Então $\mathbb{Z}/p\mathbb{Z}[m]$ é equivalente a $\mathbb{Z}/p\mathbb{Z}[i]$ para $p \equiv 3 \pmod 4$ (todas as contas são exatamente as mesmas que no item a) e a $\mathbb{Z}/p\mathbb{Z}$ para $p \equiv 1 \pmod 4$ (nesse caso, como m é solução, $a + bm \in \mathbb{Z}/p\mathbb{Z}$). De qualquer forma, temos um corpo.

1.2. Seja $f(x)$ um polinômio de coeficientes racionais, irredutível em $\mathbb{Q}$. Sendo F o conjunto dos polinômios com coeficientes racionais vistos módulo $f(x)$ (ou seja, $P(x) \equiv Q(x) \pmod{f(x)} \iff f(x) \mid P(x) - Q(x)$), determine se F é um corpo.

Solução: Novamente, é imediato somar, subtrair e multiplicar. Os elementos neutros são os polinômios constantes 0 e 1. Então basta verificar a existência de inverso.

Se P não é divisível por f então $\mathrm{mdc}(P, f) = 1$. Pelo teorema de Bezóut, existem polinômios A e B com coeficientes racionais tais que

$$AP + Bf = 1 \implies AP \equiv 1 \pmod f,$$

e o inverso de P é A.

1.3. O que acontece se, no exercício anterior, trocarmos os coeficientes de $\mathbb{Q}$ para $\mathbb{Z}/p\mathbb{Z}$? Considere o caso particular $f(x) = x^2 + 1$ e compare com o exercício 1.

Solução: Não muda nada, mas como a demonstração depende do teorema de Bezóut, vale a pena demonstrar o teorema de Bezóut. De fato, vamos fazer a demonstração para polinômios em qualquer corpo K. Fazemos isso definindo divisão euclidiana. Isso é parte do caminho típico divisão euclidiana para fatoração única[2]:

Divisão euclidiana → Bezóut → Irredutível = Primo → Fatoração única

[1] A demonstração do teorema de Wilson envolve definir $B_m = \{m, m^{-1}\}$, e notar que os únicos valores de m para os quais $|B_m| = 1$ são $m \equiv \pm 1 \pmod p$.

[2] Vale ressaltar que nem todo domínio de fatoração única tem divisão euclidiana: por exemplo, $\mathbb{Q}[x, y]$ não tem divisão euclidiana mas tem fatoração única.

Primeiro notamos a existência de divisão euclidiana: de fato, é só emular o algoritmo da chave para polinômios em K, usando a divisão em K. Depois usamos o algoritmo de Euclides para cálculo de mdc: sendo f irredutível e g não divisível por f, se o grau de g é maior ou igual ao de f, ao dividir g por f obtemos um resto r com grau menor do que o de f, e continuamos com f e r; ou seja, podemos supor sem perda que $\partial p < \partial f$. O algoritmo de Euclides gera uma sequência $f = r_0, g = r_1, r_2, \ldots, r_n$ de polinômios tal que

$$\begin{aligned} f &= gq_1 + r_2 \\ g &= r_2q_2 + r_3 \\ r_2 &= r_3q_3 + r_4 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n \\ r_{n-1} &= r_nq_n \end{aligned}$$

Então, substituindo $r_i = r_{i-2} - r_{i-1}q_{i-1}$ sucessivamente de $i = 2$ até $i = k$ nos permite obter polinômios a_k, b_k tais que $a_kf + b_kg = r_k$. Provamos isso por indução em k. Isso é óbvio para $k \geq 2$ pois $f = r_0$, $g = r_1$ e $f - q_1g = r_2$. Para $k > 2$, basta notar que $r_k = r_{k-2} - r_{k-1}q_{k-1}$ e substituir r_{k-2} e r_{k-1}.

Em particular, $r_n = a_nf + b_ng$. Agora, note que r_{n-k} é múltiplo de r_n para todo k, por indução em k: isso é direto para $k = 0$ e para $k = 1$, e para $k > 0$, $r_{n-k} = r_{n-(k-1)}q_{n-(k-1)} + r_{n-(k-2)}$ é múltiplo de r_n porque $r_{n-(k-1)}$ e $r_{n-(k-2)}$ são ambos múltiplos de r_n por hipótese de indução.

(Novamente) em particular, r_n é divisor de f e g. Afirmamos que r_n é um mdc de f e g; sendo d um divisor comum, então d divide $a_nf + b_ng = r_n$, ou seja, $\partial d \leq \partial r_n$, e r_n tem que ter grau máximo. Para provar Bezóut, basta multiplicar por uma constante para obter $af + bg = \text{mdc}(f, g)$.

O caso $f(x) = x^2 + 1$ só faz sentido para $p \equiv 3 \pmod 4$, já que f não é irredutível em $\mathbb{Z}/p\mathbb{Z}$ para $p \equiv 1 \pmod 4$: sendo m a solução de $x^2 \equiv -1 \pmod p$, $x^2 + 1 \equiv x^2 - m^2 \equiv (x + m)(x - m) \pmod p$.

Comentário: Apesar de não ser necessário para o problema, por completude, terminamos o caminho até fatoração única.

- **Bézout → Irredutível = Primo.** Primeiro vamos definir irredutível e primo. Um elemento p é *irredutível* quando não é possível escrever $p = ab$ sendo a e b diferentes de unidades. Bom, agora a gente precisa definir unidade. Um elemento u é uma *unidade* quando existe v tal que $uv = 1$, em que 1 é o elemento neutro da multiplicação. Um elemento p é *primo* quando, para todos a, b, $p \mid ab \iff p \mid a$ ou $p \mid b$.
  Mostremos que não irredutíveis não são primos: se $m = ab$ então $m \mid ab$ mas $m \nmid a$ e $m \nmid b$, pois se $m \mid a$ então $a = mk$ e $m = mkb \iff kb = 1$, mas b não é unidade. Agora, vamos provar que se vale Bezóut, irredutíveis são primos. Suponha que p é irredutível, $p \mid ab$ e $p \nmid a$. Temos que provar que $p \mid b$. Primeiro mostramos que $\text{mdc}(p, a) = 1$. Se $d \mid p$ e $d \mid a$, então $p = dk$, o que só é possível se d ou k é unidade. Se k é unidade, então $k\ell = 1$, e $d = \ell p$, e a é divisível por p. Então d é unidade, e $\text{mdc}(p, a) = 1$. Então, por Bezóut, existem s e t tais que $as + pt = 1 \implies abs + pbt = b \iff b = p(s + bt)$. Assim, $p \mid b$.
- **Irredutível = Primo → Fatoração única.** Basta usar a mesma demonstração do teorema fundamental da aritmética, que é indução na quantidade de primos: suponha que $m = p_1p_2 \ldots p_k = q_1q_2 \ldots q_\ell$. Então $p_1 \mid q_1q_2 \ldots q_\ell \implies p_1 \mid q_i$ para algum i, que implica $q_i = up_1$, em que u é uma unidade. Cortamos p_1 e q_i e continuamos.

2 Espaços vetoriais

2.1. Mostre que $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{R}$. Encontre uma base desse espaço vetorial.

Solução: Esse é só um exercício em definição: se $\alpha, \beta \in \mathbb{R}$ e $u, v \in \mathbb{C}$, é imediato que $\alpha u + \beta v \in \mathbb{C}$. Uma base é $\{1, i\}$, já que i não pode ser escrito como um número real vezes 1 e $\{1, i\}$ gera todos os números $a + bi$, $a, b \in \mathbb{R}$.

2.2. Os polinômios com coeficientes em um corpo K formam um espaço vetorial sobre K? Se sim, determine sua dimensão.

Solução: Sim! A demonstração desse fato é direta: sendo p e q polinômios desse tipo e $\alpha, \beta \in K$, $\alpha p + \beta q$ é também um polinômio.

A dimensão desse espaço vetorial é infinita. Uma base é $\{x^n, n \in \mathbb{Z}_{\geq 0}\}$: de fato, não é possível que x^k seja combinação linear dos outros x^ℓ's e essa base gera todos os polinômios, pela definição de polinômio.

2.3. Mostre que todas as bases de espaços vetoriais têm a mesma quantidade de elementos.

Solução: Vamos fazer só o caso finito (o caso infinito tem várias tecnicalidades que não valem a pena). Suponha que B_1 e B_2 são bases com $|B_1| = m < n = |B_2|$. Escreva cada elemento v_i de B_2 como combinação linear dos elementos u_j de B_1, ou seja, $v_i = a_{i1}u_1 + a_{i2}u_2 + \cdots + a_{im}u_m$. Uma combinação linear de v_i's é

$$x_1v_1 + x_2v_2 + \cdots + x_nv_n = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x_iu_j.$$

Assim, se uma combinação linear dos v_i's é nula, temos

$$\sum_{i=1}^{n} a_{ij}x_n = 0, \quad j = 1, 2, \ldots, m.$$

Como há m equações, n variáveis $x_1, \ldots, x_n$, $m < n$ e o sistema é homogêneo, ele admite uma solução não trivial, e encontramos uma combinação linear não trivial de v_i's que é nula, contradizendo a definição de base para B_2.

3 Extensões de corpos

3.1. Nessa seção mostramos que se $K \subseteq L$ são corpos então L é um espaço vetorial sobre K. Prove que a recíproca não é verdadeira, ou seja, exiba um exemplo de espaço vetorial V sobre um corpo K tal que V não é um corpo.

Solução: Polinômios com coeficientes racionais não formam um corpo. Por exemplo, x não tem inverso.

3.2. Mostre que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ (para obter $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, estendemos colocando $\sqrt{2}$ e $\sqrt{3}$).

Solução: Temos $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$; o inverso de $a + b\sqrt{2}$ é $\frac{a - b\sqrt{2}}{a^2 - 2b^2}$. Como $a, b \in \mathbb{Q}$, $a/b \neq \sqrt{2} \implies a^2 - 2b^2 \neq 0$.

Para obter $\mathbb{Q}(\sqrt{2}\sqrt{3})$, estendemos $\mathbb{Q}(\sqrt{2})$: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\alpha + \beta\sqrt{3}, \alpha, \beta \in \mathbb{Q}(\sqrt{2})\}$. Novamente, o inverso de $\alpha + \beta\sqrt{3}$ é $\frac{\alpha - \beta\sqrt{3}}{\alpha^2 - 3\beta^2}$. $\alpha/\beta = m + n\sqrt{2} \neq \sqrt{3}$ para $m, n \in \mathbb{Q}$, pois $3 = m^2 + 2n^2 + 2mn\sqrt{2}$ não pode acontecer ($m = 0$ não dá e $n = 0$ também não). Descompactando, temos

$$\begin{aligned}
\mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \{\alpha + \beta\sqrt{3}, \alpha, \beta \in \mathbb{Q}(\sqrt{2})\} \\
&= \{a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3}, a, b, c, d \in \mathbb{Q}\} \\
&= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, a, b, c, d \in \mathbb{Q}\}
\end{aligned}$$

Note que $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$.

Agora calculemos $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Como o polinômio minimal de $\sqrt{2}+\sqrt{3}$ é x^4-10x^2+1 (verifique!), sendo $\gamma=\sqrt{2}+\sqrt{3}$, temos

$$\mathbb{Q}(\sqrt{2}+\sqrt{3})=\{a+b\gamma+c\gamma^2+d\gamma^3, a,b,c,d\in\mathbb{Q}\},$$

e temos $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$.

Como γ e γ^3 são da forma $p\sqrt{2}+q\sqrt{3}$ e $\gamma^2=5+2\sqrt{6}$, podemos escrever todo elemento de $\mathbb{Q}$ na forma $a+\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, e como as dimensões sobre $\mathbb{Q}$ são as mesmas, $\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$.

3.3. Seja $p(x)\in\mathbb{Z}[x]$ um polinômio mônico e irredutível tal que $|p(0)|$ não é quadrado perfeito. Prove que $p(x^2)$ é irredutível em $\mathbb{Q}$.

Solução: Seja n o grau de p. Pelo último exemplo, os fatores irredutíveis de $p(x^2)$, que tem grau $2n$, são múltiplos de n. Se $p(x^2)$ não é irredutível, ele só pode ser fatorado como o produto de dois irredutíveis de grau n, ou seja,

$$p(x^2)=f(x)g(x),\quad \partial f=\partial g=n.$$

Seja α uma raiz de f; então α é raiz de $p(x^2)$, e como $p(\alpha^2)=p((-\alpha)^2)$, $-\alpha$ também é raiz de $p(x^2)$ e é, portanto, raiz de f ou g. Como f é irredutível, f é minimal de α, e $\pm f(-x)$ é minimal de $-\alpha$. Se $-\alpha$ é raiz de f, $f(x)=\pm f(x)$, ou seja, f é par ou ímpar. Como f é irredutível, e todo polinômio ímpar tem zero como raiz, f é par, ou seja, $f(x)=q(x^2)$ para algum polinômio q. Mas aí q tem grau $n/2$, e $q(\alpha^2)=0$. Mas $p(\alpha^2)=0$ e p é irredutível de grau n, logo p é minimal de α^2. Isso é uma contradição, pois $\partial q<\partial p$. Logo $-\alpha$ é raiz de g, e $g(x)=\pm f(-x)$. Finalmente, $p(x^2)=\pm f(x)f(-x)$, e temos $p(0)=\pm(f(0))^2$, ou seja, $|p(0)|$ é quadrado perfeito. Provamos então a contrapositiva do enunciado.

4 Grupos

4.1. Seja S a sequência definida por $S_0=4$ e $S_{k+1}=S_k^2-2$ para $k\geq 0$. Para $n>2$, prove que $M_n=2^n-1$ é primo se, e somente se, S_{n-2} é múltiplo de M_n.[3]

Solução: Começamos resolvendo a recursão. Seja $S_k=\alpha_k+\frac{1}{\alpha_k}$. Então $S_{k+1}=S_k^2-2=\alpha_k^2+\frac{1}{\alpha_k^2}$. Assim, podemos tomar $\alpha_{k+1}=\alpha_k^2$, e temos $S_k=\alpha_0^{2^k}+\frac{1}{\alpha_0^{2^k}}$. Resolvendo $\alpha_0+\frac{1}{\alpha_0}=4$ obtemos $\alpha_0=2+\sqrt{3}$, ou seja,

$$S_k=(2+\sqrt{3})^{2^k}+(2-\sqrt{3})^{2^k}.$$

Primeiro suponha que M_n não é primo e que $M_n\mid S_{n-2}$. Seja $p<\sqrt{M_n}$ um de seus fatores primos. Trabalhamos em $\mathbb{Z}/p\mathbb{Z}$ se 3 é resíduo quadrático e em $\mathbb{Z}/p\mathbb{Z}[\sqrt{3}]$ se não é. Temos $2-\sqrt{3}=(2+\sqrt{3})^{-1}$, e

$$\begin{aligned}(2+\sqrt{3})^{2^{n-2}}+(2-\sqrt{3})^{2^{n-2}}\equiv 0 \pmod p &\iff (2+\sqrt{3})^{2^{n-2}}\equiv -(2+\sqrt{3})^{-2^{n-2}} \pmod p\\ &\iff (2+\sqrt{3})^{2^{n-1}}\equiv -1 \pmod p.\end{aligned}$$

Logo a ordem de $2+\sqrt{3}$ é 2^n pois $(2+\sqrt{3})^{2^n}\equiv 1 \pmod p$ e a ordem precisa ser, desse modo, potência de 2. Pelo teorema de Lagrange, $(2+\sqrt{3})^{p^2-1}\equiv 1 \pmod p$ (se estamos em $\mathbb{Z}/p\mathbb{Z}$ eleve a $p+1$). Aí 2^n divide p^2-1, mas $p<\sqrt{2^n-1}\implies p^2-1<2^n$, absurdo. Logo M_n é primo.

[3]Retirado do livro *Primos de Mersenne (e outros primos muito grandes)*, de Carlos Gustavo T. A. Moreira (Gugu), e Nicolau C. Saldanha

Para o outro lado, suponha que M_n é primo. Note que, da reciprocidade quadrática $\left(\frac{3}{M_n}\right) = (-1)^{\frac{3-1}{2}\frac{M_n-1}{2}}\left(\frac{M_n}{3}\right) = -1 \cdot 1 = -1$, pois n é ímpar, o que implica $M_n = 2^n - 1 \equiv 1 \pmod 3$. Logo $\mathbb{Z}/M_n\mathbb{Z}[\sqrt{3}]$ é um corpo de ordem M_n^2.

Queremos mostrar que $(2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}} \equiv 0 \pmod{M_n}$, o que é equivalente a $(2+\sqrt{3})^{2^{n-1}} \equiv -1 \pmod{M_n}$. Isso, por sua vez, é equivalente a mostrar que a ordem de $2+\sqrt{3}$ é 2^n. Agora, $2+\sqrt{3} = \left(\frac{1+\sqrt{3}}{2}\right)^2$. Pelo sonho de todo estudante, e usando o critério de Euler, que diz que $-1 = \left(\frac{3}{M_n}\right) \equiv 3^{\frac{M_n-1}{2}} \pmod{M_n}$,

$$\begin{aligned}(2+\sqrt{3})^{2^{n-1}} &= \left(\frac{1+\sqrt{3}}{2}\right)^{2^n} = \left(\frac{1+\sqrt{3}}{2}\right)^{M_n+1} \equiv \frac{1+3^{\frac{M_n-1}{2}}\sqrt{3}}{2^{M_n}} \cdot \frac{1+\sqrt{3}}{2} \pmod{M_n} \\ &\equiv \frac{1-\sqrt{3}}{2} \cdot \frac{1+\sqrt{3}}{2} \equiv -1 \pmod{M_n}.\end{aligned}$$

Portanto a ordem de $2+\sqrt{3}$ é 2^n, pelo mesmo argumento que a recíproca, e o resultado segue.

4.2. (OBM 2017) Seja a inteiro positivo e p um divisor primo de $a^3 - 3a + 1$ com $p \neq 3$. Prove que p é da forma $9k+1$ ou $9k-1$, sendo k inteiro.

Solução: Seja $a = x + \frac{1}{x}$ em $\mathbb{Z}/p\mathbb{Z}$. Então

$$a^3 - 3a + 1 = x^3 + \frac{1}{x^3} + 3x \cdot \frac{1}{x}\left(x + \frac{1}{x}\right) - 3\left(x + \frac{1}{x}\right) + 1 = \frac{x^6 + x^3 + 1}{x^3} = \frac{x^9 - 1}{x^3(x^3-1)}.$$

Vendo módulo p, temos $p \mid a^3 - 3a + 1 \iff x^9 \equiv 1 \pmod p$. Note que $x^3 \not\equiv 1 \pmod p$ pois isso implicaria $a^3 - 3a + 1 \equiv 1 + 1 + 1 \equiv 3 \pmod p$, e $p \neq 3$. Portanto a ordem de x módulo p é 9.

A questão é que nem sempre existe x módulo p, ou seja, $x + x^{-1} \equiv a \pmod p$ pode não ter solução. Se existe x, o problema acabou pois $9 \mid p-1$. Se não existe, estendemos $\mathbb{Z}/p\mathbb{Z}$ para $\mathbb{Z}/p\mathbb{Z}[x]$. Nesse caso, como $x + x^{-1} \equiv a \pmod p \iff x^2 - ax + 1 \equiv 0 \pmod p$,

$$\mathbb{Z}/p\mathbb{Z}[x] = \{a + bx, a, b \in \mathbb{Z}/p\mathbb{Z}\}.$$

Agora, note que $k + \ell x \equiv m + nx \pmod p \iff k - m \equiv (n-\ell)x \pmod p$. Como $x \notin \mathbb{Z}/p\mathbb{Z}$, $n \equiv \ell \pmod p$ e, consequentemente, $k \equiv m \pmod p$. Como $x^2 - ax + 1$ é irredutível, $a + bx$ tem inverso módulo $x^2 - ax + 1$, e portanto módulo p também. Então $\mathbb{Z}/p\mathbb{Z}[x]$ é um corpo com p^2 elementos, e temos $x^{p^2-1} \equiv 1 \pmod p$, de modo que $9 \mid p^2 - 1$. Como $\text{mdc}(p-1, p+1) = 2$, $9 \mid p-1$ ou $9 \mid p+1$, e o resultado segue.

4.3. (IMO Shortlist 2003) A sequência $a_0, a_1, \ldots$ é definido por $a_0 = 2$, $a_{k+1} = 2a_k^2 - 1$ para $k \geq 0$. Prove que se um primo ímpar p divide a_n então 2^{n+3} divide $p^2 - 1$.

Solução: Esse problema é bem parecido com o do M_n, então só colocarei os "checkpoints" da solução.

- Primeiro encontre
$$a_k = \frac{1}{2}\left((2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}\right).$$
- Depois trabalhe em $\mathbb{Z}/p\mathbb{Z}[\sqrt{3}]$; de fato, a conta é bem fácil:
$$(2+\sqrt{3})^{2^n} \equiv -(2+\sqrt{3})^{-2^n} \pmod p \iff (2+\sqrt{3})^{2^{n+1}} \equiv -1 \pmod p,$$
e a ordem de $2+\sqrt{3}$ é 2^{n+2}, e $2^{n+2} \mid p^2 - 1$ pelo teorema de Lagrange. Quase!

- Para acabar, basta notar que $2+\sqrt{3} = \left(\frac{1+\sqrt{3}}{2}\right)^2$. Qual é a ordem de $\frac{1+\sqrt{3}}{2}$?

4.4. (IMO Shortlist 2004) Seja k um inteiro fixado maior do que 1, e defina $m = 4k^2 - 5$. Prove que existem inteiros positivos a e b tais que a sequência (x_k) definida por

$$x_0 = a, \quad x_1 = b, \quad x_{n+2} = x_{n+1} + x_n, n = 0, 1, 2, \ldots$$

tem todos os seus termos primos com m.

Solução: Nesse caso, $4k^2 \equiv 5 \pmod{m}$, de modo que 5 é resíduo quadrático módulo qualquer primo divisor de m. Sendo $\phi = \frac{1+\sqrt{5}}{2}$ e $\psi = -\phi^{-1}$ as raízes de $x^2 = x + 1$,

$$x_n = \alpha\phi^n + \beta\psi^n,$$

e basta escolher α e β de modo que x_n nunca é zero módulo p. Como $\phi \equiv 0 \pmod{p} \iff \sqrt{5} \equiv -1 \pmod{p} \implies 1 \equiv 5 \pmod{p}$, o que não é possível,

$$x_n \equiv 0 \pmod{p} \iff \alpha\phi^{2n} + \beta(\phi\psi)^n \equiv 0 \pmod{p} \iff \alpha\phi^{2n} + \beta(-1)^n \equiv 0 \pmod{p}.$$

Então basta tomar, digamos, $\alpha \equiv 0 \pmod{p}$ e $\beta \equiv 1 \pmod{p}$. É claro que, ao escolhermos α e β, usamos $\sqrt{5}$. Sendo mais específico: resolvendo $x_0 = a$ e $x_0 = b$ obtemos $a \equiv 1 \pmod{p}$ e $b \equiv \psi \pmod{p}$, sendo ψ uma solução da congruência $x^2 \equiv x + 1 \pmod{p}$. Por exemplo, para $p = 11$, uma solução é $\psi = 8$ ($8^2 = 64 \equiv 9 = 8 + 1 \pmod{11}$), e escolhemos $a = 1$ e $b = 8$.

De fato, a partir da escolha da solução anterior dá para encontrar uma solução bem curta:

Solução: Sendo 5 resíduo quadrático módulo qualquer primo p que divide m, como $p \neq 2$ temos que $\phi = \frac{1+\sqrt{5}}{2}$ existe módulo p e podemos escolher $a = 1$ e $b = \phi \bmod p$, e aí $x_n \equiv \phi^n \pmod{p}$, que nunca é zero.

Comentário: Em tempo: se 5 não é resíduo quadrático, pode ocorrer de existir a sequência ou não. Um programa de computador foi utilizado para testar todos os primos até 2017; entre os que não têm 5 como resíduo quadrático, os resultados são:

- Números que dão certo: 13, 17, 37, 47, 53, 73, 97, 107, 113, 137, 157, 173, 193, 197, 233, 257, 263, 277, 293, 307, 313, 317, 337, 347, 353, 373, 397, 433, 457, 557, 563, 577, 593, 613, 617, 653, 673, 677, 733, 743, 757, 773, 797, 853, 857, 877, 937, 953, 967, 977, 997, 1013, 1033, 1087, 1093, 1097, 1103, 1117, 1153, 1193, 1213, 1217, 1223, 1237, 1277, 1297, 1307, 1373, 1427, 1433, 1453, 1483, 1493, 1523, 1553, 1597, 1613, 1637, 1657, 1693, 1697, 1733, 1753, 1777, 1823, 1873, 1877, 1913, 1933, 1973, 1993, 1997, 2017.
- Números que não dão certo: 3, 7, 23, 43, 67, 83, 103, 127, 163, 167, 223, 227, 283, 367, 383, 443, 463, 467, 487, 503, 523, 547, 587, 607, 643, 647, 683, 727, 787, 823, 827, 863, 883, 887, 907, 947, 983, 1063, 1123, 1163, 1283, 1303, 1327, 1367, 1423, 1447, 1487, 1543, 1567, 1583, 1607, 1627, 1663, 1667, 1723, 1747, 1783, 1787, 1847, 1867, 1907, 1987, 2003.